

# ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
P.IVA 08545970017



---

## Regolamento per la protezione dei dati personali, economici, sensibili e giudiziari 2014

---

ai sensi del Codice in Materia di Protezione dei Dati Personali  
Decreto Legislativo 30 giugno 2003 n. 196

*Privacy*

# Indice

|  |           |
|--|-----------|
| <b>Copertina</b>   | <b>I</b>  |
| <b>Indice</b>  | <b>II</b> |
| <b>1 Regolamento per la protezione dei dati personali, economici, sensibili e giudiziari</b>   | <b>1</b>  |
| 1.1 Scopo . . . . .  | 1         |
| 1.2 Campo di applicazione . . . . .  | 1         |
| 1.3 Riferimenti normativi . . . . .  | 2         |
| 1.4 Definizioni . . . . .  | 3         |
| 1.5 Definizioni ulteriori . . . . .  | 5         |
| <b>2 Ruoli, compiti e nomine</b>   | <b>6</b>  |
| 2.1 Titolare del trattamento dei dati personali . . . . .  | 6         |
| 2.1.1 Compiti del titolare del trattamento dei dati personali . . . . .  | 6         |
| 2.1.2 Nomina del titolare del trattamento dei dati personali . . . . .   | 6         |
| 2.2 Responsabile della sicurezza dei dati personali . . . . .  | 6         |
| 2.2.1 Compiti del responsabile della sicurezza dei dati personali . . . . .  | 6         |
| 2.2.2 Nomina del responsabile della sicurezza dei dati personali . . . . .   | 7         |
| 2.3 Responsabile del trattamento dei dati personali . . . . .  | 8         |
| 2.3.1 Compiti del responsabile del trattamento dei dati personali . . . . .  | 8         |
| 2.3.2 Nomina dei responsabili del trattamento dei dati personali . . . . .   | 8         |
| 2.4 Incaricato del trattamento dei dati personali . . . . .  | 9         |
| 2.4.1 Compiti degli incaricati del trattamento dei dati personali . . . . .  | 9         |
| 2.4.2 Nomina degli incaricati del trattamento dei dati personali . . . . .   | 9         |
| 2.5 Sistema di autorizzazione . . . . .  | 10        |
| <b>3 Disposizioni fondamentali per il trattamento dei dati</b>   | <b>11</b> |
| 3.1 Nomina e istruzioni agli incaricati . . . . .  | 11        |
| 3.2 Copie degli atti e dei documenti . . . . .   | 11        |
| 3.3 Elenco dei trattamenti di dati personali . . . . .   | 12        |
| 3.3.1 Elenco delle sedi e degli uffici in cui vengono trattati i dati . . . . .  | 12        |
| 3.3.2 Elenco degli archivi dei dati oggetto del trattamento . . . . .  | 12        |
| 3.4 Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati . . . . .  | 12        |
| 3.4.1 Elenco dei soggetti autorizzati al trattamento dei dati . . . . .  | 12        |
| 3.4.2 Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni . . . . .   | 12        |
| 3.5 Misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità . . . . .  | 13        |
| 3.5.1 Misure generali . . . . .  | 13        |
| 3.5.2 Procedure per controllare l'accesso ai locali in cui vengono trattati i dati . . . . .   | 13        |
| 3.6 Formazione degli incaricati del trattamento . . . . .  | 13        |
| 3.7 Criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare . . . . . | 14        |
| 3.7.1 Trattamenti di dati personali affidati all'esterno della struttura del titolare . . . . .  | 14        |

|          |          |           |
|----------|----------|-----------|
| 3.7.2    | 3.7.2    | 14        |
| 3.7.3    | 3.7.3    | 14        |
| <b>4</b> | <b>4</b> | <b>16</b> |
| 4.1      | 4.1      | 16        |
| 4.2      | 4.2      | 16        |
| 4.2.1    | 4.2.1    | 16        |
| 4.2.2    | 4.2.2    | 16        |
| 4.2.3    | 4.2.3    | 17        |
| 4.2.4    | 4.2.4    | 17        |
| 4.2.5    | 4.2.5    | 17        |
| 4.3      | 4.3      | 18        |
| 4.3.1    | 4.3.1    | 18        |
| 4.3.2    | 4.3.2    | 18        |
| 4.3.3    | 4.3.3    | 19        |
| 4.4      | 4.4      | 19        |
| 4.5      | 4.5      | 19        |
| 4.5.1    | 4.5.1    | 20        |
| 4.5.2    | 4.5.2    | 21        |
| 4.5.3    | 4.5.3    | 21        |
| 4.5.4    | 4.5.4    | 21        |
| 4.5.5    | 4.5.5    | 21        |
| 4.5.6    | 4.5.6    | 21        |
| 4.5.7    | 4.5.7    | 22        |
| 4.6      | 4.6      | 22        |
| 4.6.1    | 4.6.1    | 22        |
| 4.6.2    | 4.6.2    | 23        |
| 4.7      | 4.7      | 24        |
| 4.8      | 4.8      | 24        |
| 4.8.1    | 4.8.1    | 24        |
| 4.8.2    | 4.8.2    | 24        |
| 4.9      | 4.9      | 25        |
| 4.10     | 4.10     | 26        |
| 4.10.1   | 4.10.1   | 26        |
| 4.10.2   | 4.10.2   | 27        |
| 4.11     | 4.11     | 27        |
| 4.12     | 4.12     | 28        |
| 4.12.1   | 4.12.1   | 28        |
| 4.12.2   | 4.12.2   | 28        |
| 4.12.3   | 4.12.3   | 28        |
| 4.13     | 4.13     | 29        |
| 4.13.1   | 4.13.1   | 29        |
| 4.13.2   | 4.13.2   | 30        |
| <b>5</b> | <b>5</b> | <b>31</b> |
| 5.1      | 5.1      | 31        |
| 5.2      | 5.2      | 31        |
| 5.3      | 5.3      | 31        |
| 5.4      | 5.4      | 32        |
| 5.4.1    | 5.4.1    | 32        |

|          |  |           |
|----------|--|-----------|
| <b>6</b> | <b>Diritti dell'interessato</b>  | <b>33</b> |
| 6.1      | Diritto di accesso ai dati personali . . . . .   | 33        |
| 6.2      | Esercizio dei diritti . . . . .  | 34        |
| 6.3      | Modalità di esercizio . . . . .  | 34        |
| 6.4      | Riscontro all'interessato . . . . .  | 35        |
| <b>7</b> | <b>Trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro</b> | <b>37</b> |
| 7.1      | Premessa . . . . .   | 37        |
| 7.2      | Il rispetto dei principi di protezione dei dati personali . . . . .                                | 38        |
| 7.3      | Titolare e responsabile del trattamento . . . . .  | 38        |
| 7.3.1    | Titolare e responsabile . . . . .  | 38        |
| 7.3.2    | Gruppi di imprese . . . . .  | 39        |
| 7.3.3    | Medico competente . . . . .  | 39        |
| 7.4      | Dati biometrici e accesso ad aree riservate . . . . .  | 40        |
| 7.5      | Comunicazione e diffusione di dati personali . . . . .   | 41        |
| 7.5.1    | Comunicazione . . . . .  | 41        |
| 7.5.2    | Intranet aziendale . . . . .   | 42        |
| 7.5.3    | Diffusione . . . . .   | 42        |
| 7.5.4    | Cartellini identificativi . . . . .  | 42        |
| 7.5.5    | Modalità di comunicazione . . . . .  | 43        |
| 7.6      | Dati idonei a rivelare lo stato di salute di lavoratori . . . . .                                  | 43        |
| 7.6.1    | Dati sanitari . . . . .  | 43        |
| 7.6.2    | Assenze per ragioni di salute . . . . .  | 43        |
| 7.6.3    | Denuncia all'INAIL . . . . .   | 44        |
| 7.6.4    | Altre informazioni relative alla salute . . . . .  | 44        |
| 7.6.5    | Comunicazioni all'INPS . . . . .   | 44        |
| 7.7      | Informativa . . . . .  | 45        |
| 7.8      | Misure di sicurezza . . . . .  | 45        |
| 7.8.1    | Dati sanitari . . . . .  | 45        |
| 7.8.2    | Incaricati . . . . .   | 45        |
| 7.8.3    | Misure fisiche ed organizzative . . . . .  | 45        |
| 7.9      | Esercizio dei diritti dell'interessato e riscontro . . . . .                                       | 46        |
| 7.9.1    | Dati personali e documentazione . . . . .  | 47        |
| <b>8</b> | <b>Regolamentazione del sito web</b>   | <b>48</b> |
| 8.1      | Partita iva obbligatoria su sito web . . . . .   | 48        |
| 8.2      | Informativa presente nella home-page del sito . . . . .  | 48        |
| 8.2.1    | Titolare del trattamento . . . . .   | 48        |
| 8.2.2    | Luogo di trattamento dei dati . . . . .  | 48        |
| 8.2.3    | Tipi di dati trattati . . . . .  | 48        |
| 8.2.4    | Facoltatività del conferimento dei dati . . . . .  | 49        |
| 8.2.5    | Modalità del trattamento . . . . .   | 49        |
| 8.2.6    | Diritti degli interessati . . . . .  | 49        |
| 8.3      | Consenso on-line . . . . .   | 50        |
| <b>9</b> | <b>Norme per posta elettronica e internet</b>  | <b>51</b> |
| 9.1      | Sintesi . . . . .  | 51        |
| 9.2      | Premessa . . . . .   | 52        |
| 9.3      | Principi generali . . . . .  | 52        |
| 9.4      | Correttezza nel trattamento . . . . .  | 53        |
| 9.4.1    | Disciplinare . . . . .   | 53        |
| 9.4.2    | Informativa (art. 13 del Codice) . . . . .   | 54        |
| 9.5      | Apparecchiature preordinate al controllo a distanza . . . . .                                      | 54        |
| 9.6      | Programmi che consentono controlli indiretti . . . . .   | 55        |
| 9.7      | Internet: la navigazione web . . . . .   | 56        |
| 9.8      | Posta elettronica . . . . .  | 56        |
| 9.9      | Controlli . . . . .  | 57        |

|  |            |
|--|------------|
| 9.10 Liceità del trattamento . . . . .   | 58         |
| 9.11 Soggetti preposti . . . . .   | 58         |
| 9.12 Misure da adottare e divieti . . . . .                                    | 59         |
| <b>10 Misure per l'utilizzo di Smartphone e Tablet</b>                         | <b>60</b>  |
| <b>A Elenchi</b>   | <b>78</b>  |
| MOD_ORG . . . . .  | 79         |
| MOD_LOC . . . . .  | 82         |
| MOD_TRT . . . . .  | 87         |
| AGENDA APPUNTAMENTI, VISITE E PRENOTAZIONI . . . . .                           | 87         |
| ANAGRAFICA CONDIVISA E RUBRICA . . . . .                                       | 89         |
| ATTIVITÀ DI RECUPERO CREDITI . . . . .   | 91         |
| BANCA DATI ASSOCIATI . . . . .   | 93         |
| BANCA DATI GESTIONE E ORGANIZZAZIONE EVENTI . . . . .                          | 95         |
| BANCA DATI ISTITUZIONI . . . . .   | 97         |
| BANCA DATI PROMOZIONE . . . . .  | 99         |
| BANCA DATI REGOLAMENTO ED ANAGRAFICA CONTRATTI OPERATORI ESTERNI . . . . .     | 101        |
| BANCA DATI SISTEMA PRENOTAZIONE MUSEI . . . . .                                | 103        |
| BANCA DATI UTENTI CESSIONE TERZI . . . . .                                     | 105        |
| CARTELLE SANITARIE DI RISCHIO DEI LAVORATORI SOGGETTI A SORVEGLIANZA SANITARIA | 107        |
| COMUNICAZIONI TELEFONICHE . . . . .  | 109        |
| CONTABILITÀ PROPRIA . . . . .  | 111        |
| CORRISPONDENZA, COMUNICATI E CIRCOLARI . . . . .                               | 113        |
| ENTRATTEL . . . . .  | 115        |
| GESTIONE ACQUISTI E APPROVVIGIONAMENTI . . . . .                               | 116        |
| GESTIONE DEL RAPPORTO DI LAVORO NEI CONFRONTI DEI PROPRI LAVORATORI . . . . .  | 118        |
| GESTIONE DELLA CLIENTELA . . . . .   | 120        |
| GESTIONE LIBRI SOCIALI . . . . .   | 122        |
| GESTIONE POLIZZE ASSICURATIVE . . . . .  | 124        |
| INCASSI, PAGAMENTI E OPERAZIONI BANCARIE . . . . .                             | 126        |
| POSTA ELETTRONICA . . . . .  | 128        |
| POSTA ELETTRONICA CERTIFICATA . . . . .  | 130        |
| PRATICHE LEGALI E CONTENZIOSI . . . . .  | 132        |
| PREDISPOSIZIONE DICHIARAZIONE DEI REDDITI E BILANCIO . . . . .                 | 134        |
| REGISTRAZIONE E GESTIONE DELLE PRESENZE NEI CONFRONTI DEI PROPRI LAVORATORI    | 136        |
| RELAZIONI PUBBLICHE . . . . .  | 138        |
| REVISIONE DEI CONTI E CERTIFICAZIONE DI BILANCIO . . . . .                     | 140        |
| SELEZIONE DEL PERSONALE . . . . .  | 141        |
| SISTEMA DI GESTIONE DELLA PROTEZIONE DEL TRATTAMENTO DI DATI . . . . .         | 143        |
| SISTEMA DI GESTIONE DELLA SICUREZZA SUL LAVORO . . . . .                       | 145        |
| SISTEMA INFORMATIVO . . . . .  | 147        |
| SITO WEB . . . . .   | 149        |
| SPEDIZIONE E RICEZIONE DI DOCUMENTI E MATERIALE . . . . .                      | 151        |
| TRASMISSIONI DATI IN INTERNET (NAVIGAZIONE WEB, FILE SHARING, ECC.) . . . . .  | 153        |
| MOD_ELAB . . . . .   | 155        |
| MOD_SITI . . . . .   | 159        |
| MOD_EMAIL . . . . .  | 160        |
| <b>B Piano di Formazione</b>   | <b>161</b> |
| MOD_FORMAZ . . . . .   | 162        |
| MOD_RPF . . . . .  | 164        |
| LETTERA D'INCARICO DI LEON FRANCESCA . . . . .                                 | 164        |

|  |  |            |
|--|--|------------|
| <b>C</b>   | <b>Analisi dei Rischi</b>  | <b>165</b> |
| C.1  | Rischi ambientali . . . . .  | 165        |
| C.2  | Rischi sull'integrità dei dati . . . . .   | 166        |
| C.2.1  | Rischi di carattere accidentale . . . . .  | 166        |
| C.2.2  | Rischi di carattere volontario . . . . .   | 166        |
| C.2.3  | Rischi da programmi pericolosi . . . . .   | 167        |
| C.3  | Rischi sulla riservatezza dei dati . . . . .                                     | 167        |
| C.3.1  | Trattamenti non consentiti o non conformi alle finalità della raccolta . . . . . | 167        |
| C.3.2  | Rischi di accessi non autorizzati . . . . .                                      | 168        |
| C.4  | Disponibilità dei dati . . . . .   | 168        |
| C.4.1  | Rischi di natura accidentale . . . . .   | 169        |
| C.4.2  | Rischi di natura intenzionale . . . . .  | 169        |
| C.4.3  | Rischi derivanti da accessi abusivi . . . . .                                    | 169        |
| C.5  | Altri specifici rischi . . . . .   | 171        |
| C.6  | Riepilogo dell'analisi dei rischi . . . . .                                      | 171        |
| MOD_ARCA   | . . . . .  | 173        |
| <b>D</b>   | <b>Lettere di Incarico</b>   | <b>177</b> |
| MOD_TT   | . . . . .  | 178        |
| TITOLARE DEL TRATTAMENTO DI D'ACRI ANTONIO MARCO | . . . . .  | 178        |
| MOD_AUTTIT                                       | . . . . .  | 179        |
| DICHIARAZIONE DI BANCA SELLA                     | . . . . .  | 179        |
| DICHIARAZIONE DI LEGAL MAIL                      | . . . . .  | 180        |
| DICHIARAZIONE DI UNICREDIT BANCA                 | . . . . .  | 181        |
| MOD_RST  | . . . . .  | 182        |
| LETTERA D'INCARICO DI LEON FRANCESCA             | . . . . .  | 182        |
| MOD_ACL  | . . . . .  | 184        |
| LETTERA D'INCARICO DI ARUGA MARCO                | . . . . .  | 184        |
| LETTERA D'INCARICO DI BARAVELLI CRISTINA         | . . . . .  | 185        |
| LETTERA D'INCARICO DI BERTERO LUCA               | . . . . .  | 186        |
| LETTERA D'INCARICO DI BORGARO CHIARA             | . . . . .  | 187        |
| LETTERA D'INCARICO DI CAGNASSO MAGDA             | . . . . .  | 188        |
| LETTERA D'INCARICO DI COCCIARDI STEFANO          | . . . . .  | 189        |
| LETTERA D'INCARICO DI CORREALE AMALIA            | . . . . .  | 190        |
| LETTERA D'INCARICO DI D'ACRI ANTONIO MARCO       | . . . . .  | 191        |
| LETTERA D'INCARICO DI EYNARD SIMONE FLAVIO       | . . . . .  | 192        |
| LETTERA D'INCARICO DI IACOBONE PASQUALE          | . . . . .  | 193        |
| LETTERA D'INCARICO DI LEON FRANCESCA             | . . . . .  | 194        |
| LETTERA D'INCARICO DI MAUTINO ROBERTO            | . . . . .  | 195        |
| LETTERA D'INCARICO DI PEPE ANNARITA              | . . . . .  | 196        |
| LETTERA D'INCARICO DI PINTOR RENATA              | . . . . .  | 197        |
| LETTERA D'INCARICO DI RICCI SIMONA               | . . . . .  | 198        |
| LETTERA D'INCARICO DI SERRA ELEONORA             | . . . . .  | 199        |
| LETTERA D'INCARICO DI VITRANI PAOLO              | . . . . .  | 200        |
| MOD_CAT  | . . . . .  | 201        |
| MOD_IT   | . . . . .  | 201        |
| LETTERA D'INCARICO DI BARAVELLI CRISTINA         | . . . . .  | 201        |
| LETTERA D'INCARICO DI BERTERO LUCA               | . . . . .  | 204        |
| LETTERA D'INCARICO DI BORGARO CHIARA             | . . . . .  | 207        |
| LETTERA D'INCARICO DI COCCIARDI STEFANO          | . . . . .  | 210        |
| LETTERA D'INCARICO DI EYNARD SIMONE FLAVIO       | . . . . .  | 213        |
| LETTERA D'INCARICO DI IACOBONE PASQUALE          | . . . . .  | 216        |
| LETTERA D'INCARICO DI VITRANI PAOLO              | . . . . .  | 219        |
| LETTERA D'INCARICO DI MAUTINO ROBERTO            | . . . . .  | 222        |
| LETTERA D'INCARICO DI PEPE ANNARITA              | . . . . .  | 226        |
| LETTERA D'INCARICO DI PINTOR RENATA              | . . . . .  | 230        |
| LETTERA D'INCARICO DI SERRA ELEONORA             | . . . . .  | 234        |

|  |            |
|--|------------|
| LETTERA D'INCARICO DI ARUGA MARCO . . . . .                          | 238        |
| LETTERA D'INCARICO DI CAGNASSO MAGDA . . . . .                       | 242        |
| LETTERA D'INCARICO DI CORREALE AMALIA . . . . .                      | 246        |
| LETTERA D'INCARICO DI LEON FRANCESCA . . . . .                       | 251        |
| LETTERA D'INCARICO DI D'ACRI ANTONIO MARCO . . . . .                 | 257        |
| LETTERA D'INCARICO DI RICCI SIMONA . . . . .                         | 263        |
| LETTERA D'INCARICO DI BRACCIALARGHE MAURIZIO . . . . .               | 268        |
| LETTERA D'INCARICO DI COPPOLA MICHELE . . . . .                      | 274        |
| LETTERA D'INCARICO DI RINALDI VALERIA . . . . .                      | 280        |
| MOD_EXT . . . . .  | 284        |
| LETTERA D'INCARICO DI BIPOINT . . . . .                              | 284        |
| LETTERA D'INCARICO DI CITTA' DI TORINO . . . . .                     | 286        |
| LETTERA D'INCARICO DI COMITATO ESECUTIVO . . . . .                   | 288        |
| LETTERA D'INCARICO DI CRITICAL CASE . . . . .                        | 291        |
| LETTERA D'INCARICO DI CSI PIEMONTE . . . . .                         | 293        |
| LETTERA D'INCARICO DI DOTT. FRANZO ANGELO . . . . .                  | 295        |
| LETTERA D'INCARICO DI DOTT. MARCO ALBERTO MALAGNINO . . . . .        | 297        |
| LETTERA D'INCARICO DI EVOLUTIVA . . . . .                            | 299        |
| LETTERA D'INCARICO DI FORE . . . . .                                 | 301        |
| LETTERA D'INCARICO DI GLS . . . . .                                  | 303        |
| LETTERA D'INCARICO DI KOINE' SISTEMI . . . . .                       | 305        |
| LETTERA D'INCARICO DI LOTTOMATICA . . . . .                          | 307        |
| LETTERA D'INCARICO DI PLUSERVICE . . . . .                           | 309        |
| LETTERA D'INCARICO DI REALE MUTUA . . . . .                          | 311        |
| LETTERA D'INCARICO DI SEGRE MASSIMO . . . . .                        | 313        |
| LETTERA D'INCARICO DI SPAZIOTTANTOTTO SRL . . . . .                  | 315        |
| LETTERA D'INCARICO DI STUDIO CODA . . . . .                          | 317        |
| LETTERA D'INCARICO DI STUDIO COMOLLO . . . . .                       | 319        |
| LETTERA D'INCARICO DI STUDIO NOTARILE GANELLI MAROCCO . . . . .      | 321        |
| LETTERA D'INCARICO DI STUDIO TOSETTO WEIGMANN . . . . .              | 323        |
| MOD_RGSE . . . . .   | 325        |
| LETTERA D'INCARICO DI MAUTINO ROBERTO . . . . .                      | 325        |
| LETTERA D'INCARICO DI EYNARD SIMONE FLAVIO . . . . .                 | 326        |
| MOD_ADS . . . . .  | 327        |
| LETTERA D'INCARICO DI KOINE' SISTEMI . . . . .                       | 327        |
| MOD_ICCC . . . . .   | 329        |
| LETTERA D'INCARICO DI LEON FRANCESCA . . . . .                       | 329        |
| MOD_ICCBD . . . . .  | 330        |
| LETTERA D'INCARICO DI MAUTINO ROBERTO . . . . .                      | 330        |
| LETTERA D'INCARICO DI ROBERTO MAUTINO . . . . .                      | 332        |
| LETTERA D'INCARICO DI MAUTINO ROBERTO . . . . .                      | 333        |
| <b>E Facsimili per la gestione informatica . . . . .</b>             | <b>334</b> |
| E.1 Elaboratori informatici . . . . .                                | 334        |
| E.2 Credenziali di autenticazione . . . . .                          | 334        |
| E.3 Antivirus . . . . .  | 334        |
| E.4 Firewall . . . . .   | 334        |
| E.5 Back-Up (salvataggio dei dati) . . . . .                         | 335        |
| E.6 Banche Dati Autorizzate . . . . .                                | 335        |
| E.7 Navigazione in Internet e caselle di posta elettronica . . . . . | 335        |
| E.7.1 Siti web correlati con l'attività lavorativa . . . . .         | 335        |
| E.7.2 Caselle di posta elettronica . . . . .                         | 336        |
| E.8 Modelli . . . . .  | 336        |
| MOD_MTZ . . . . .  | 334        |
| MOD_ELAB . . . . .   | 337        |
| MOD_SITI . . . . .   | 338        |
| MOD_EMAIL . . . . .  | 339        |

|  |            |
|--|------------|
| MOD_PWD . . . . .  | 340        |
| MOD_RAEE . . . . .   | 341        |
| MOD_RSK_HW . . . . .   | 342        |
| MOD_RSK_SW . . . . .   | 343        |
| MOD_FW_AV . . . . .  | 344        |
| MOD_AUT_PC . . . . .   | 345        |
| AUTORIZZAZIONE . . . . .   | 345        |
| MOD_MTZ_HWSW . . . . .   | 346        |
| AUTORIZZAZIONE . . . . .   | 346        |
| MOD_VERADS . . . . .   | 347        |
| MOD_TSP . . . . .  | 348        |
| LETTERA DI ASSEGNAZIONE . . . . .                                      | 348        |
| <b>F Facsimili</b>   | <b>349</b> |
| MOD_INF . . . . .  | 350        |
| MOD_INF_F . . . . .  | 350        |
| MOD_INF_C . . . . .  | 351        |
| MOD_INF_WEB . . . . .  | 353        |
| ART.7 D.LGS. 196/03 . . . . .  | 355        |
| MOD_ASNZ_DIP . . . . .   | 356        |
| INFORMATIVA ALL'ATTO DELL'ASSUNZIONE . . . . .                         | 356        |
| MOD_CNTR_AGNZ . . . . .  | 358        |
| CONTRATTO DI AGENZIA . . . . .   | 358        |
| MOD_IT_TMP . . . . .   | 360        |
| LETTERA DI INCARICO TEMPORANEO . . . . .                               | 360        |
| MOD_IT_CES . . . . .   | 361        |
| LETTERA DI CESSAZIONE DELL'INCARICO . . . . .                          | 361        |
| MOD_SEDE . . . . .   | 362        |
| LETTERA PER CAMBIO SEDE . . . . .                                      | 362        |
| MOD_POST . . . . .   | 363        |
| MOD_FAX_MAIL . . . . .   | 364        |
| MOD_PLZ . . . . .  | 365        |
| LETTERA PER IMPRESA DI PULIZIA . . . . .                               | 365        |
| MOD_FRT . . . . .  | 366        |
| SCARICO DI RESPONSABILITÀ . . . . .                                    | 366        |
| <b>G Elenco misure adottate</b>  | <b>367</b> |
| G.1 Misure interne . . . . .   | 367        |
| G.2 Misure atte al trattamento elettronico dell'informazione . . . . . | 367        |
| G.3 Regolamenti e formazione . . . . .                                 | 368        |
| G.4 Ulteriori Misure . . . . .   | 368        |
| G.5 Analisi dei rischi . . . . .                                       | 368        |



# Capitolo 1

## Regolamento per la protezione dei dati personali, economici, sensibili e giudiziari

### 1.1 Scopo

Il presente **Regolamento per la protezione dei dati personali, economici, sensibili e giudiziari** ha valore di ordine di servizio a cui si deve attenere tutto il personale dipendente e non; esso è redatto per soddisfare tutte le misure minime di sicurezza che debbono essere adottate in via preventiva da tutti coloro che trattano dati personali, conformemente a quanto previsto dal CODICE IN MATERIA DI PROTEZIONE DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L).

In esso sono trattati i requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS dall'inglese Information Security Management System), ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa, secondo lo Standard ISO/IEC 27001:2005.

Inoltre costituisce un valido strumento per la adozione delle misure idonee previste dall'articolo 31 dello stesso Codice e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Grazie al presente Regolamento è possibile ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza. Si intende così proteggere l'organizzazione dalla commissione dei reati presupposto per la responsabilità amministrativa dell'ente quali delitti informatici e trattamento illecito di dati ai sensi dell'art. 24-bis del D.Lgs. 231/2001 (articolo aggiunto dalla L. 18 marzo 2008 n. 48, art. 7).

### 1.2 Campo di applicazione

Il Regolamento definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali, economici, sensibili e giudiziari.

Il Regolamento riguarda il trattamento dei dati economici e di tutti i dati personali:

1. Sensibili
2. Giudiziari
3. Comuni

Il Regolamento si applica al trattamento di tutti i dati personali per mezzo di:

1. Strumenti elettronici di elaborazione
2. Altri strumenti di elaborazione (ed esempio: Cartacei, Audio, Visivi e Audiovisivi, ecc..)

Il Regolamento deve essere conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione.

### 1.3 Riferimenti normativi

1. CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L)
2. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Arti. da 33 a 36 del codice)
3. STANDARD ISO/IEC serie 27000

Segue l'elenco dei provvedimenti legislativi di modifica ed integrazione del Codice:

- decreto legge 27 gennaio 2012, n. 3;
- decreto legge 6 dicembre 2011, n. 201 convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214;
- decreto legge 13 maggio 2011, n. 70 convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106;
- legge 4 novembre 2010, n. 183;
- legge 29 luglio 2010, n. 120;
- decreto-legge del 25 settembre 2009, n. 135 convertito, con modificazioni, dalla legge 20 novembre 2009, n. 166;
- legge 4 marzo 2009, n. 15
- decreto-legge del 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14;
- decreto-legge 25 giugno 2008, n. 112 convertito, con modificazioni, dalla legge 6 agosto 2008 n. 133;
- decreto legislativo 30 maggio 2008, n. 109;
- legge 18 marzo 2008, n. 48, ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno
- decreto-legge 28 dicembre 2006, n. 300 convertito, con modificazioni, dalla legge 26 febbraio 2007, n. 17;
- decreto-legge 12 maggio 2006, n. 173 convertito, con modificazioni, dalla legge 12 luglio 2006, n. 228;
- decreto-legge 30 dicembre 2005, n. 273 convertito, con modificazioni, dalla legge 23 febbraio 2006, n. 51;
- decreto legge 30 novembre 2005, n. 245 convertito, con modificazioni, dalla legge 27 gennaio 2006, n. 21;
- decreto legislativo 7 settembre 2005, n. 209;

- decreto-legge 27 luglio 2005, n. 144 convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155;
- decreto-legge 30 dicembre 2004, n. 314 convertito, con modificazioni, dalla legge 1 marzo 2005, n. 26;
- decreto-legge 9 novembre 2004, n. 66 convertito, con modificazioni, dalla legge 27 dicembre 2004, n. 306;
- decreto-legge 24 giugno 2004, n. 158 convertito, con modificazioni, dalla legge 27 luglio 2004, n. 188;
- decreto-legge 29 marzo 2004, n. 81 convertito, con modificazioni, dalla legge 26 maggio 2004, n. 138;
- decreto legislativo 22 gennaio 2004, n. 42;
- decreto-legge 24 dicembre 2003, n. 354 convertito, con modificazioni, dalla legge 26 febbraio 2004, n. 45

Segue l'elenco dei provvedimenti di normazione internazionale:

- ISO/IEC 27000: Principles and vocabulary
- ISO/IEC 27001: Information security management system - Requirements
- ISO/IEC 27002: Information security management system - Best practice
- ISO/IEC 27003: Information security management system - Implementation guidance
- ISO/IEC 27004: Information security management system - metrics and measurement
- ISO/IEC 27005: Information security management system - Risk management

## 1.4 Definizioni

Cfr. Nota <sup>1</sup>

**Trattamento** Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

**Dato personale** Qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

**Dati sensibili** I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

**Dati giudiziari** I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

---

<sup>1</sup>Le definizioni risultano così modificate in base al DECRETO-LEGGE 6 dicembre 2011, n. 201 Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici. (GU n.284 del 6-12-2011 - Suppl. Ordinario n. 251) convertito con modificazioni dalla L. 22 dicembre 2011, n. 214 (in SO n. 276, relativo alla G.U. 27-12-2011, n. 300). In sostanza, dal concetto di dati personali sono stati esclusi quelli riferiti a persona giuridica, ente od associazione, limitandone l'ambito ai soli dati riferiti a persone fisiche.

**Titolare** La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

**Responsabile** La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

**Incaricati** Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

**Interessato** La persona fisica cui si riferiscono i dati personali.

**Comunicazione** Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

**Diffusione** Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

**Dato anonimo** Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

**Blocco** La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

**Banca dati** Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

**Comunicazione elettronica** Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico.

Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

**Misure minime** Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

**Strumenti elettronici** Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

**Autenticazione informatica** L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

**Credenziali di autenticazione** I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

**Parola chiave** Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

**Profilo di autorizzazione** L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

**Sistema di autorizzazione** L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

## 1.5 Definizioni ulteriori

A seguito delle modificazioni normative introdotte nel corso del 2011, risulta utile all'interno di codesto documento, estendere le precedenti definizioni, introducendo

**Dati aziendali o ontologici** Qualunque informazione relativa a persona giuridica, ente od associazione identificati o identificabili, anche indirettamente.

**Azienda o Ente interessato** Persona giuridica, ente od associazione cui si riferiscono i dati.

**Dati Economici** Dati personali o aziendali che riguardano informazioni di carattere economico.

**Dati genetici** Dati sensibili riguardanti le informazioni sul genoma di una persona fisica.

**Trattamenti effettuati per finalità amministrativo-contabili** I trattamenti effettuati per finalità amministrativo-contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro.

## Capitolo 2

# Ruoli, compiti e nomine

### 2.1 Titolare del trattamento dei dati personali

#### 2.1.1 Compiti del titolare del trattamento dei dati personali

Il Titolare del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Il Titolare del trattamento deve assicurare e garantire direttamente che vengano adottate le misure di sicurezza ai sensi del CODICE IN MATERIA DI DATI PERSONALI e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previa idonee istruzioni fornite per iscritto.

Il Titolare del trattamento, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più Responsabili della sicurezza dei dati che assicurino e garantiscano che vengano adottate le misure di sicurezza ai sensi del CODICE IN MATERIA DI DATI PERSONALI e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA. Qualora il Titolare del trattamento ritenga di non nominare alcun Responsabile della sicurezza dei dati, ne assumerà tutte le responsabilità e funzioni.

#### 2.1.2 Nomina del titolare del trattamento dei dati personali

La nomina del titolare del trattamento dei dati personali deve essere effettuata dal legale rappresentante della ditta, società, ente, associazione od organizzazione, mediante una lettera di incarico (MOD\_TT) in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.

Copia della lettera di nomina accettata deve essere conservata a cura del Titolare del trattamento in luogo sicuro.

### 2.2 Responsabile della sicurezza dei dati personali

#### 2.2.1 Compiti del responsabile della sicurezza dei dati personali

Il Responsabile della sicurezza dei dati personali è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo a cui sono affidate le seguenti responsabilità e compiti:

1. Garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.

2. Redigere ed aggiornare ad ogni variazione l'elenco delle sedi in cui vengono trattati i dati.
3. Redigere ed aggiornare ad ogni variazione l'elenco degli uffici in cui vengono trattati i dati.
4. Redigere ed aggiornare ad ogni variazione l'elenco delle banche dati oggetto di trattamento.
5. Se il trattamento è effettuato con mezzi informatici, redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione.
6. Definire e successivamente verificare con cadenza semestrale le modalità di accesso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità come specificato in seguito.
7. Decidere se affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.
8. Qualora il trattamento dei dati sia stato affidato in tutto o in parte all'esterno della struttura del titolare controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
9. Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Responsabili della gestione e della manutenzione degli strumenti elettronici.
10. Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati della custodia delle copie delle credenziali qualora vi sia più di un incaricato del trattamento.
11. Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati delle copie di sicurezza delle banche dati.
12. Custodire e conservare i supporti utilizzati per le copie dei dati .
13. Il Responsabile della sicurezza dei dati personali, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più Responsabili del trattamento con il compito di individuare, nominare e incaricare per iscritto, gli Incaricati del trattamento dei dati personali.
14. Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Responsabile del trattamento, ne assumerà tutte le responsabilità e funzioni.

Qualora il Titolare del trattamento ritenga di non nominare alcun Responsabili della sicurezza dei dati personali, ne assumerà tutte le responsabilità e funzioni.

### 2.2.2 Nomina del responsabile della sicurezza dei dati personali

La nomina di ciascun Responsabile della sicurezza dei dati personali deve essere effettuata dal Titolare del trattamento con una lettera di incarico (MOD\_RST) in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.

Copia della lettera di nomina accettata deve essere conservata a cura del Titolare del trattamento in luogo sicuro.

Il Titolare del trattamento deve informare ciascun Responsabile della sicurezza dei dati personali delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Il Titolare del trattamento deve consegnare a ciascun Responsabile della sicurezza dei dati personali una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina del Responsabile della sicurezza dei dati personali è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina del Responsabile della sicurezza dei dati personali può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

## 2.3 Responsabile del trattamento dei dati personali

### 2.3.1 Compiti del responsabile del trattamento dei dati personali

Il Responsabile del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che ha il compito di individuare, nominare e incaricare per iscritto, gli Incaricati del trattamento dei dati personali.

Il Responsabile del trattamento dei dati personali ha il compito di:

1. Nominare gli incaricati del trattamento per le Banche di dati che gli sono state affidate.
2. Di sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice in materia di dati personali.
3. Di dare le istruzioni adeguate agli incaricati del trattamento effettuato con strumenti elettronici e non.
4. Periodicamente, e comunque almeno annualmente, verifica la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati del trattamento dei dati personali.

Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Responsabile del trattamento, ne assumerà tutte le responsabilità e funzioni.

### 2.3.2 Nomina dei responsabili del trattamento dei dati personali

La nomina di ciascun Responsabile del trattamento deve essere effettuata dal Responsabile della sicurezza dei dati personali con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.

Copia della lettera di nomina (MOD\_RT) accettata deve essere conservata a cura del Responsabile della sicurezza dei dati personali in luogo sicuro.

Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Responsabile del trattamento, ne assumerà tutte le responsabilità e funzioni.

Il Responsabile della sicurezza dei dati personali deve informare ciascun Responsabile del trattamento delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Il Responsabile della sicurezza dei dati personali deve consegnare a ciascun Responsabile del trattamento una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.



La nomina del Responsabile del trattamento è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina del Responsabile del trattamento può essere revocata in qualsiasi momento dal Responsabile della sicurezza dei dati personali senza preavviso, ed eventualmente affidata ad altro soggetto.

## 2.4 Incaricato del trattamento dei dati personali

### 2.4.1 Compiti degli incaricati del trattamento dei dati personali

Gli Incaricati del trattamento sono le persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali da un Responsabile del trattamento.

In particolare gli incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

1. Gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo.
2. La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
3. La parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato.
4. L'incaricato del trattamento deve modificarla al primo utilizzo e, successivamente, almeno ogni sei mesi.
5. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi.
6. Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.
7. Gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
8. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

### 2.4.2 Nomina degli incaricati del trattamento dei dati personali

La nomina di ciascun Incaricato del trattamento dei dati personali deve essere effettuata dal Responsabile del trattamento con una lettera di incarico in cui sono specificati i compiti che gli sono stati affidati che deve essere controfirmata dall'interessato per presa visione.

Copia della lettera di nomina (MOD\_IT) firmata deve essere conservata a cura del Responsabile del trattamento in luogo sicuro.

Il Responsabile del trattamento deve informare ciascun Incaricato del trattamento dei dati personali delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta

Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Il Responsabile del trattamento deve consegnare a ciascun Incaricato del trattamento dei dati personali una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

Gli Incaricati del trattamento dei dati personali devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

Agli Incaricati del trattamento dei dati personali deve essere assegnata una parola chiave e un codice di autenticazione informatica.

Agli Incaricati del trattamento dei dati personali è prescritto di adottare le necessarie cautele per assicurare la segretezza della parola chiave e la diligente custodia dei dispositivi in possesso e ad uso esclusivo dell'incaricato.

La nomina del Incaricato del trattamento dei dati personali è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina dell'Incaricato del trattamento dei dati personali può essere revocata in qualsiasi momento dal Responsabile del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

## 2.5 Sistema di autorizzazione

I Responsabili del trattamento hanno il compito di individuare gli Incaricati del trattamento per ogni tipologia di banca di dati personali trattata.

Il tipo di trattamento effettuato da ogni singolo Incaricato del trattamento può essere differenziato.

In particolare ad ogni Incaricato del trattamento può essere data dal Responsabile del trattamento la possibilità di:

1. Inserire nuove informazioni nella banca di dati personali
2. Consultare le informazioni, accedendovi in visualizzazione e stampa
3. Modificare le informazioni esistenti nella banca di dati personali
4. Annullare e cancellare le informazioni esistenti nella banca di dati personali
5. Trasportare e trasferire i supporti su cui sono memorizzati i dati (dossier, faldoni, documenti cartacei, hard disk, nastri magnetici, cd, dvd, ecc.
6. Esclusivamente conservare i supporti, senza accedere ai contenuti
7. Procedere con operazioni di diffusione dei dati
8. Manutenere e amministrare la banca di dati personali

## Capitolo 3

# Disposizioni fondamentali per il trattamento dei dati

### 3.1 Nomina e istruzioni agli incaricati

Per ogni archivio i Responsabili della sicurezza dei dati personali debbono definire l'elenco degli incaricati autorizzati ad accedervi e impartire istruzioni tese a garantire un controllo costante nell'accesso negli archivi.

Gli incaricati che trattano atti e documenti contenenti dati personali sono tenuti a conservarli e restituirli al termine delle operazioni.

Qualora i documenti contengano dati sensibili o giudiziari ai sensi dell'art. 4 del CODICE IN MATERIA DI DATI PERSONALI, gli incaricati del trattamento sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura.

L'accesso agli archivi contenenti documenti ove sono presenti dati sensibili o giudiziari è consentito, dopo l'orario di chiusura, previa identificazione e registrazione dei soggetti

### 3.2 Copie degli atti e dei documenti

In base a quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA, è fatto divieto a chiunque di:

- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Responsabile della sicurezza dei dati personali, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del Responsabile della sicurezza dei dati personali, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal Responsabile della sicurezza dei dati personali, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

## 3.3 Elenco dei trattamenti di dati personali

### 3.3.1 Elenco delle sedi e degli uffici in cui vengono trattati i dati

Al Responsabile della sicurezza dei dati personali è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle sedi in cui viene effettuato il trattamento dei dati.

Per redigere l'Elenco delle sedi in cui vengono trattati i dati deve essere utilizzato il modulo MOD\_LOC che deve essere aggiornato e conservato in luogo sicuro a cura del Responsabile della sicurezza dei dati personali.

### 3.3.2 Elenco degli archivi dei dati oggetto del trattamento

Al Responsabile della sicurezza dei dati personali è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati.

Ogni banca di dati o archivio deve essere classificato in relazione alle informazioni contenute indicando se si tratta di:

1. Dati personali
2. Dati sensibili
3. Dati giudiziari

ed eventualmente di

1. Dati aziendali o ontologici
2. Dati economici
3. Dati genetici

Per l'individuazione degli archivi dei dati oggetto del trattamento deve essere utilizzato il modulo MOD\_TRT\_XX (dove XX rappresenta un codice identificativo dell'archivio), che deve essere compilato e conservato dal Responsabile della sicurezza dei dati personali in luogo sicuro.

## 3.4 Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

### 3.4.1 Elenco dei soggetti autorizzati al trattamento dei dati

Il Responsabile della sicurezza dei dati personali ha il compito di assegnare le credenziali di autenticazione e di aggiornare l'elenco del personale autorizzato al trattamento dei dati utilizzando il già citato modulo MOD\_IT, che deve essere conservato a cura del Responsabile della sicurezza dei dati personali, in luogo sicuro e deve essere trasmesso in copia controllata all'Incaricato della custodia delle copie delle credenziali di competenza.

### 3.4.2 Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni

Il Responsabile della sicurezza dei dati personali ha il compito di verificare ogni anno, entro il 31 dicembre, le credenziali di autenticazione e di aggiornare l'elenco dei soggetti autorizzati al trattamento dei dati utilizzando il modulo MOD\_IT che deve essere conservato a cura del Responsabile della sicurezza dei dati personali, in luogo sicuro e deve essere trasmesso in copia controllata agli Incaricati della custodia delle copie delle credenziali di competenza.

## **3.5 Misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità**

### **3.5.1 Misure generali**

In considerazione di quanto disposto dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA, è fatto divieto a chiunque di:

1. Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Responsabile della sicurezza dei dati personali di dati oggetto del trattamento.
2. Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Responsabile della sicurezza dei dati personali, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
3. Sottrarre, cancellare, distruggere senza l'autorizzazione del Responsabile della sicurezza dei dati personali, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
4. Consegnare a persone non autorizzate dal Responsabile della sicurezza dei dati personali, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

### **3.5.2 Procedure per controllare l'accesso ai locali in cui vengono trattati i dati**

Al Responsabile della sicurezza dei dati personali è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati, e di nominare per ciascun ufficio un incaricato con il compito di controllare direttamente i sistemi, le apparecchiature, o i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.

Il Responsabile della sicurezza dei dati personali deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.

Il Responsabile della sicurezza dei dati personali deve informare con una comunicazione scritta l'incaricato dell'ufficio dei compiti che gli sono stati affidati utilizzando il modello MOD\_ACL.

## **3.6 Formazione degli incaricati del trattamento**

Il Responsabile del trattamento dei dati personali valuta, per ogni incaricato a cui ha affidato il trattamento, sulla base dell'esperienza, delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessario pianificare interventi di formazione, che devono essere riportati nel modello MOD\_FORMAZ.

La previsione di interventi formativi degli incaricati del trattamento, ha lo scopo principale di renderli edotti sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano e sulle modalità per aggiornarsi sulle misure minime adottate dal titolare.

La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

Al Responsabile della sicurezza dei dati personali è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di ulteriore formazione del personale incaricato di effettuare periodicamente le operazioni di copia di sicurezza delle banche di dati trattate.

## **3.7 Criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare**

### **3.7.1 Trattamenti di dati personali affidati all'esterno della struttura del titolare**

Il Responsabile della sicurezza dei dati personali può decidere di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.

Il Responsabile della sicurezza dei dati personali, deve redigere e aggiornare ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, ed indicare per ognuno di essi il tipo di trattamento effettuato specificando:

1. i soggetti interessati
2. i luoghi dove fisicamente avviene il trattamento dei dati stessi
3. i responsabili del trattamento di dati personali

Per l'inventario dei soggetti a cui affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, deve essere utilizzato il modulo MOD\_EXT, che deve essere conservato a cura del Responsabile della sicurezza dei dati personali, in luogo sicuro.

Nel caso in cui, per il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, i responsabili del trattamento di dati personali non vengano espressamente nominati Responsabili del trattamento di dati personali affidati all'esterno della struttura del titolare (out-sourcing), ai sensi dell'art. 29 del CODICE IN MATERIA DI DATI PERSONALI, devono intendersi autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.

### **3.7.2 Criteri per la scelta degli enti terzi per il trattamento di dati personali affidati all'esterno della struttura del titolare**

Il Responsabile della sicurezza dei dati personali, può affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare a quei soggetti terzi che abbiano i requisiti individuati all'art. 29 del CODICE IN MATERIA DI DATI PERSONALI (esperienza, capacità ed affidabilità).

Il Titolare a cui è stato affidato il trattamento dei dati all'esterno deve rilasciare una dichiarazione scritta da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento ai sensi del CODICE IN MATERIA DI DATI PERSONALI e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

### **3.7.3 Nomina dell'incaricato del trattamento in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare**

Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, il Responsabile della sicurezza dei dati personali deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.

Il Responsabile della sicurezza dei dati personali deve informare l'incaricato del trattamento dei dati affidato all'esterno alla struttura del titolare, dei compiti che gli sono assegnati in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

L'incaricato del trattamento dei dati affidato all'esterno alla struttura del titolare deve accettare la nomina, secondo il modello MOD\_EXT.

La nomina dell'Incaricato del trattamento dei dati affidato all'esterno alla struttura del titolare deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Responsabile della sicurezza dei dati personali in luogo sicuro.

## Capitolo 4

# Trattamento con l'ausilio di strumenti elettronici

### 4.1 Elenco dei sistemi di elaborazione per il trattamento

Al Responsabile della sicurezza dei dati personali è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione con cui viene effettuato il trattamento dei dati.

Per ogni sistema deve essere specificato:

1. Il Responsabile della gestione e della manutenzione
2. Il nome dell'incaricato o degli incaricati che lo utilizzano
3. Il nome di uno o più Incaricati della custodia delle copie delle credenziali

Per l'Elenco dei sistemi di elaborazione deve essere utilizzato il modulo MOD\_ELAB che deve essere conservato a cura del Responsabile della sicurezza dei dati personali in luogo sicuro.

### 4.2 Sistema di autenticazione informatica

#### 4.2.1 Procedura di identificazione

Nel caso in cui il trattamento di dati personali sia effettuato con strumenti elettronici, il Responsabile della sicurezza dei dati personali deve assicurarsi che il trattamento sia consentito solamente agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

#### 4.2.2 Identificazione dell'incaricato

Il Responsabile della sicurezza dei dati personali deve assicurare che il trattamento di dati personali, effettuato con strumenti elettronici, sia consentito solamente agli incaricati dotati di una o più credenziali di autenticazione tra le seguenti:

Un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo

Un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave



Una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

Il Responsabile della sicurezza dei dati personali deve assicurarsi che il codice per l'identificazione, laddove utilizzato, non potrà essere assegnato ad altri incaricati, neppure in tempi diversi.

Il Responsabile della sicurezza dei dati personali deve assicurarsi che le credenziali di autenticazione non utilizzate da almeno sei mesi debbono essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Il Responsabile della sicurezza dei dati personali deve assicurarsi che le credenziali siano disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Ad ogni Incaricato del trattamento possono essere assegnate o associate individualmente una o più credenziali per l'autenticazione.

### 4.2.3 Caratteristiche della parola chiave

La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.

1. La parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato.
2. La parola chiave deve essere modificata dall'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi.
3. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi.

### 4.2.4 Cautele per assicurare la segretezza della componente riservata della credenziale

Gli incaricati debbono adottare le necessarie cautele per assicurare la segretezza della parola chiave e custodire diligentemente ogni altro dispositivo che gli è stato affidato per i sistemi di autenticazione informatica (badge magnetici, tessere magnetiche, ecc..).

In particolare è fatto divieto comunicare a chiunque altro incaricato le proprie credenziali di accesso al sistema informatico.

### 4.2.5 Istruzioni per non lasciare incustodito e accessibile lo strumento elettronico

Gli incaricati hanno l'obbligo di:

1. Non lasciare incustodito il proprio posto di lavoro.
2. Di chiudere tutte le applicazioni aperte o meglio ancora di spegnere il sistema informatico in caso di assenza prolungata.
3. Di attivare la configurazione del sistema informatico di lavoro in modo che automaticamente si attivi il blocco della stessa dopo un certo tempo di inattività dell'operatore, con richiesta di autenticazione per la riattivazione

## 4.3 Incaricato della custodia delle copie delle credenziali

### 4.3.1 Compiti degli incaricati della custodia delle copie delle credenziali

È onere del Responsabile della sicurezza dei dati personali, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Incaricati della custodia delle copie delle credenziali.

È compito degli Incaricati della custodia delle copie delle credenziali:

1. Gestire e custodire le credenziali per l'accesso ai dati degli Incaricati del trattamento.
2. Predisporre, per ogni incaricato del trattamento, una busta sulla quale è indicato il nome dell'incaricato e all'interno della busta deve essere indicata la credenziale usata. Le buste con le credenziali debbono essere conservate in luogo chiuso e protetto. Nel caso si utilizzi un sistema centralizzato di autenticazione, non è necessario predisporre le buste per gli incaricati, in quanto si utilizzano le funzioni del sistema stesso.
3. Istruire gli incaricati del trattamento sull'uso delle parole chiave, e sulle caratteristiche che debbono avere, e sulle modalità per la loro modifica in autonomia.
4. Revocare tutte le credenziali non utilizzate in caso di perdita della qualità che consentiva all'incaricato l'accesso ai dati personali.
5. Revocare le credenziali per l'accesso ai dati degli Incaricati del trattamento nel caso di mancato utilizzo per oltre 6 (sei) mesi.

Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Incaricato della custodia delle copie delle credenziali, ne assumerà tutte le responsabilità e funzioni.

### 4.3.2 Nomina degli incaricati della custodia delle copie delle credenziali

Il Responsabile della sicurezza dei dati personali nomina uno o più soggetti Incaricati della custodia delle copie delle credenziali a cui è conferito il compito di custodire le Parole chiave per l'accesso ai dati archiviati nei sistemi di elaborazione dei dati.

La nomina di uno o più Incaricati della custodia delle copie delle credenziali deve essere effettuata con una lettera di incarico (MOD\_ICCC) e deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Responsabile della sicurezza dei dati personali in luogo sicuro.

Il responsabile della sicurezza dei dati personali deve informare gli Incaricati della custodia delle copie delle credenziali della responsabilità che è stata loro affidata in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Il Responsabile della sicurezza dei dati personali deve consegnare a ciascun Incaricato della custodia delle copie delle credenziali, una copia di tutte le norme che riguardano la Sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina di uno o più Incaricati della custodia delle copie delle credenziali è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina di uno o più Incaricati della custodia delle copie delle credenziali può essere revocata in qualsiasi momento dal Responsabile della sicurezza dei dati personali senza preavviso, ed essere affidata ad altro soggetto.

### 4.3.3 Accesso straordinario

Gli Incaricati della custodia delle copie delle credenziali, hanno il compito di assicurare la disponibilità dei dati e degli strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

La custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza.

Gli Incaricati della custodia delle copie delle credenziali devono informare tempestivamente l'Incaricato del trattamento ogni qualvolta sia stato effettuato un tale tipo di intervento.

Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

## 4.4 Riferimenti normativi

Con i provvedimenti del 25 giugno 2009 (G.U. n. 149 del 30 giugno 2009) e del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008) recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema e alla proroga dei termini per il loro adempimento, il Garante per la protezione dei dati personali ha deciso di richiamare l'attenzione di enti, amministrazioni, società private sulla figura professionale dell'amministratore di sistema e ha prescritto l'adozione di specifiche misure tecniche ed organizzative che agevolino la verifica sulla sua attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici.

Gli amministratori di sistema sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici di un'azienda o di una pubblica amministrazione.

Le ispezioni effettuate in questi anni dall'Autorità hanno permesso di mettere in luce in diversi casi una scarsa consapevolezza da parte di organizzazioni grandi e piccole del ruolo svolto dagli amministratori di sistema. I gravi casi verificatisi negli ultimi anni hanno evidenziato una preoccupante sottovalutazione dei rischi che possono derivare quando l'attività di questi esperti sia svolta senza il necessario controllo.

Le misure e le cautele dovranno essere messe in atto da parte di tutte le aziende private e da tutti i soggetti pubblici, compresi gli uffici giudiziari, le forze di polizia, i servizi di sicurezza. Sono esclusi invece i trattamenti di dati, sia in ambito pubblico che privato, effettuati a fini amministrativo contabile, che pongono minori rischi per gli interessati.

## 4.5 Amministratori di sistema

Con la definizione di Amministratore di Sistema si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del provvedimento del Garante sono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei

dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente responsabili di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup e recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti in chiaro le informazioni medesime.

La rilevanza, la specificità e la particolare criticità del ruolo dell'amministratore di sistema sono state considerate anche dal legislatore il quale ha individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una circostanza aggravante. Ci si riferisce, in particolare, all'abuso della qualità di operatore di sistema prevista dal codice penale per le fattispecie di accesso abusivo a sistema informatico o telematico (art. 615 ter) e di frode informatica (art. 640 ter), nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (artt. 635 bis e ter) e di danneggiamento di sistemi informatici e telematici (artt. 635 quater e quinquies).

Le funzioni tipiche dell'amministrazione di un sistema sono richiamate nel menzionato Allegato B, nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione. Gran parte dei compiti previsti nel medesimo Allegato B spettano tipicamente all'amministratore di sistema: dalla realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati) alla custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione. Nel loro complesso, le norme predette mettono in rilievo la particolare capacità di azione propria degli amministratori di sistema e la natura fiduciaria delle relative mansioni, analoga a quella che, in un contesto del tutto differente, caratterizza determinati incarichi di custodia e altre attività per il cui svolgimento è previsto il possesso di particolari requisiti tecnico-organizzativi, di onorabilità, professionali, morali o di condotta, a oggi non contemplati per lo svolgimento di uno dei ruoli più delicati della società dell'informazione.

Il Responsabile della sicurezza dei dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici, vista la particolare criticità del ruolo degli amministratori di sistema, deve adottare idonee cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, in specie quelli realizzati con abuso della qualità di amministratore di sistema; deve inoltre valutare con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema, laddove queste siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali. Ciò, tenendo in considerazione l'opportunità o meno di tale attribuzione e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato, da vagliare anche in considerazione delle responsabilità, specie di ordine penale e civile (artt. 15 e 169 del Codice), che possono derivare in caso di incauta o inadeguata designazione.

#### 4.5.1 Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

### 4.5.2 Designazioni individuali

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

### 4.5.3 Elenco degli amministratori di sistema

Gli estremi identificativi delle persone fisiche o giuridiche designate quali amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel Regolamento per la protezione dei dati personali, economici, sensibili e giudiziari, valevole come Documento programmatico sulla sicurezza, oppure, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico la cui adozione è prevista dal provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58); in alternativa si possono anche utilizzare strumenti di comunicazione interna (a es., intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tale forma di pubblicità o di conoscibilità non sia esclusa in forza di un'eventuale disposizione di legge che disciplini in modo difforme uno specifico settore.

Nel caso di servizi di amministrazione di sistema affidati in outsourcing, il responsabile esterno deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

### 4.5.4 Verifica delle attività

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

### 4.5.5 Registrazione degli accessi

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

### 4.5.6 Compiti degli Amministratori di sistema

L'Amministratore di sistema è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che sovrintende al buon funzionamento di banche di dati e di sistemi software complessi

È compito degli Amministratori di sistema:

1. sovrintendere al buon funzionamento di banche di dati e di sistemi software complessi
2. proteggere le banche dati e i sistemi software complessi dal rischio di intrusione o di accesso non autorizzato
3. registrare gli accessi alle banche di dati ed ai sistemi software complessi
4. Informare il Responsabile della sicurezza dei dati personali nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Amministratore di sistema, ne assumerà tutte le responsabilità e funzioni.

#### 4.5.7 Nomina degli amministratori di sistema

È onere del Responsabile della sicurezza dei dati personali, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Amministratori di sistema.

Anche se non espressamente previsto dalla norma, è opportuno che il Responsabile della sicurezza dei dati personali nomini uno o più Amministratori di sistema, specificando le banche di dati e i sistemi software complessi che è chiamato a sovrintendere.

Il Responsabile della sicurezza dei dati personali deve informare ciascun Amministratore di sistema delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

La nomina di uno o più Amministratori di sistema deve essere effettuata con una lettera di incarico (MOD\_ADS) e deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Responsabile della sicurezza dei dati personali in luogo sicuro.

La nomina dell'Amministratore di sistema è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina dell'Amministratore di sistema può essere revocata in qualsiasi momento dal Responsabile della sicurezza dei dati personali senza preavviso, ed eventualmente affidata ad altro soggetto.

## 4.6 Responsabili della gestione e della manutenzione degli strumenti elettronici

La figura di Responsabile della gestione e della manutenzione degli strumenti elettronici corrisponde ad un sotto tipo di Amministratore di sistema, che si occupa specificatamente dei sistemi di elaborazione e dei relativi sistemi operativi.

### 4.6.1 Compiti dei responsabili della gestione e della manutenzione degli strumenti elettronici

Il Responsabile della gestione e della manutenzione degli strumenti elettronici è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che sovrintende agli strumenti di un sistema informativo, con finalità atte alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

È compito dei Responsabili della gestione e della manutenzione degli strumenti elettronici:

1. sovrintendere agli strumenti di un sistema informativo, con finalità atte alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti
2. Attivare le credenziali di autenticazione e attivare ove possibile e previsto le politiche di autorizzazione agli Incaricati del trattamento, su indicazione del Responsabile del trattamento, per tutti i trattamenti effettuati con strumenti informatici.
3. Definire quali politiche adottare per la protezione dei sistemi contro i virus informatici e verificarne l'efficacia con cadenza almeno semestrale.
4. Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di hackers).
5. Informare il Responsabile della sicurezza dei dati personali nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Responsabile della gestione e della manutenzione degli strumenti elettronici, ne assumerà tutte le responsabilità e funzioni.

#### **4.6.2 Nomina dei responsabili della gestione e della manutenzione degli strumenti elettronici**

È onere del Responsabile della sicurezza dei dati personali, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Responsabili della gestione e della manutenzione degli strumenti elettronici a cui è conferito il compito di sovrintendere al buon funzionamento delle risorse del sistema informativo.

Anche se non espressamente previsto dalla norma, è opportuno che il Responsabile della sicurezza dei dati personali nomini uno o più Responsabili della gestione e della manutenzione degli strumenti elettronici, specificando gli elaboratori che è chiamato a sovrintendere.

Il Responsabile della sicurezza dei dati personali deve informare ciascun Responsabile della gestione e della manutenzione degli strumenti elettronici delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

La nomina di uno o più Responsabili della gestione e della manutenzione degli strumenti elettronici deve essere effettuata con una lettera di incarico (MOD\_RGSE) e deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Responsabile della sicurezza dei dati personali in luogo sicuro.

Il Responsabile della sicurezza dei dati personali deve consegnare a ciascun Responsabile della gestione e della manutenzione degli strumenti elettronici una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina del Responsabile della gestione e della manutenzione degli strumenti elettronici è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina del Responsabile della gestione e della manutenzione degli strumenti elettronici può essere revocata in qualsiasi momento dal Responsabile della sicurezza dei dati personali dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

## 4.7 Sistema di autorizzazione

La politica di autorizzazioni, definita dal Responsabile del trattamento per ciascun Incaricato deve essere applicata anche per le banche di dati personali gestite elettronicamente, utilizzando gli strumenti elettronici presenti sui sistemi di elaborazione per verificarne l'applicazione, negando eventualmente l'accesso ai dati o impedendo le operazioni non consentite. È compito del Responsabile della gestione e della manutenzione degli strumenti elettronici, ove tali strumenti lo consentano, di definire, aggiornare e mantenere tali politiche.

## 4.8 Analisi dei rischi che incombono sui dati

### 4.8.1 Manutenzione dei sistemi di elaborazione dei dati

Il Responsabile della gestione e della manutenzione degli strumenti elettronici, anche avvalendosi di consulenti interni o esterni, deve verificare ogni anno:

1. la situazione delle apparecchiature hardware installate con cui vengono trattati i dati
2. la situazione delle apparecchiature periferiche
3. la situazione dei dispositivi di collegamento con le reti pubbliche

La verifica ha lo scopo di controllare l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica, per quanto riguarda:

1. la sicurezza dei dati trattati.
2. il rischio di distruzione o di perdita.
3. il rischio di accesso non autorizzato o non consentito

Il Responsabile della gestione e della manutenzione degli strumenti elettronici deve, se necessario, aggiornare la relazione annuale dei rischi hardware conformemente al modulo MOD\_RSK\_HW

Il Responsabile della gestione e della manutenzione degli strumenti elettronici nel caso in cui esistano rischi evidenti debbono informare il Responsabile della sicurezza dei dati personali perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

### 4.8.2 Manutenzione dei sistemi operativi e dei software installati

Al Responsabile della gestione e della manutenzione degli strumenti elettronici è affidato il compito di verificare ogni anno, la situazione dei Sistemi Operativi e delle applicazioni software installate sulle apparecchiature con cui vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi e delle applicazioni software, per quanto riguarda:

1. La sicurezza dei dati trattati.
2. Il rischio di distruzione o di perdita.
3. Il rischio di accesso non autorizzato o non consentito.

Tenendo conto in particolare di:



1. Disponibilità di nuove versioni migliorative dei software utilizzati.
2. Segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti.
3. Segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici deve, se necessario, aggiornare la relazione annuale dei rischi sui software installati conformemente al modulo MOD\_RSK\_SW.

I Responsabili della gestione e della manutenzione degli strumenti elettronici, nel caso in cui esistano rischi evidenti, debbono informare il Responsabile della sicurezza dei dati personali affinché siano presi gli opportuni provvedimenti per assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

## 4.9 Misure da adottare per garantire l'integrità e la disponibilità dei dati

Il Responsabile della gestione e della manutenzione degli strumenti elettronici al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati.

I criteri debbono essere definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici, eventualmente per ogni banca di dati, deve predisporre le istruzioni di copia, verifica e ripristino dei dati, utilizzando il modulo MOD\_BCKP.

Il Documento con le istruzioni di copia deve essere conservato a cura del Responsabile della sicurezza dei dati personali in luogo sicuro e deve essere trasmesso in copia controllata a ciascun incaricato delle copie di sicurezza delle banche dati.

In particolare per ogni banca di dati debbono essere definite le seguenti specifiche:

1. Il Tipo di supporto da utilizzare per le Copie di sicurezza dei dati.
2. Il numero di Copie di sicurezza dei dati effettuate ogni volta
3. Se i supporti utilizzati per le Copie di sicurezza dei dati sono riutilizzati e in questo caso con quale periodicità.
4. Se per effettuare le Copie di sicurezza dei dati si utilizzano procedure automatizzate e programmate.
5. Le modalità di controllo delle Copie di sicurezza dei dati.
6. La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
7. Il nome dell'incaricato a cui è stato assegnato il compito di effettuare le Copie di sicurezza dei dati.
8. Le istruzioni e i comandi necessari per effettuare le Copie di sicurezza dei dati.
9. Le istruzioni e i comandi necessari per effettuare il ripristino delle Copie di sicurezza dei dati.

Al Responsabile della sicurezza dei dati personali è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di formazione del personale incaricato di effettuare periodicamente le Copie di sicurezza delle banche di dati trattate, in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica.

## 4.10 Incaricato delle copie di sicurezza delle banche dati

### 4.10.1 Compiti degli incaricati delle copie di sicurezza delle banche dati

L'incaricato delle copie di sicurezza delle banche dati è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che ha il compito di effettuare periodicamente le copie di sicurezza delle Banche di dati gestite.

È onere del Responsabile della sicurezza dei dati personali, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Incaricati delle copie di sicurezza delle banche dati.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce, con il supporto tecnico del Responsabile della gestione e della manutenzione degli strumenti elettronici la periodicità con cui debbono essere effettuate le copie di sicurezza delle Banche di Dati trattate.

I criteri debbono essere concordati con il Responsabile della gestione e della manutenzione degli strumenti elettronici in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In particolare per ogni Banca di dati debbono essere definite le seguenti specifiche:

1. Il Tipo di supporto da utilizzare per le Copie di Back-Up .
2. Il numero di Copie di Back-Up effettuate ogni volta.
3. Se i supporti utilizzati per le Copie di Back-Up sono riutilizzati e in questo caso con quale periodicità.
4. Se per effettuare le Copie di Back-Up si utilizzano procedure automatizzate e programmate.
5. Le modalità di controllo delle Copie di Back-Up .
6. La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
7. L'incaricato del trattamento a cui è stato assegnato il compito di effettuare le Copie di Back-Up .
8. Le istruzioni e i comandi necessari per effettuare le Copie di Back-Up .

È compito degli Incaricati delle copie di sicurezza delle banche dati:

1. Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal Responsabile della sicurezza dei dati personali.
2. Assicurarisi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro.
3. Assicurarisi della conservazione delle copie di sicurezza in luogo adatto e sicuro e ad accesso controllato.
4. Di provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato.
5. Di segnalare tempestivamente al Responsabile della gestione e della manutenzione degli strumenti elettronici, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Incaricato delle copie di sicurezza delle banche dati, ne assumerà tutte le responsabilità e funzioni.

### 4.10.2 Nomina degli incaricati delle copie di sicurezza delle banche dati

Il Responsabile della sicurezza dei dati personali nomina uno o più soggetti Incaricati delle copie di sicurezza delle banche dati a cui è conferito il compito di effettuare periodicamente le copie di sicurezza delle Banche di dati gestite.

Anche se non espressamente previsto dalla norma, è opportuno che il Responsabile della sicurezza dei dati personali nomini uno o più Incaricati delle copie di sicurezza delle banche dati, specificando gli elaboratori o le banche dati che è chiamato a sovrintendere.

Il Responsabile della sicurezza dei dati personali deve informare ciascun Incaricato delle copie di sicurezza delle banche dati delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

La nomina di uno o più Incaricati delle copie di sicurezza delle banche dati deve essere effettuata con una lettera di incarico (MOD\_ICCBD) e deve essere controfirmata per accettazione.

Copia della lettera di nomina accettata deve essere conservata a cura del Responsabile della sicurezza dei dati personali in luogo sicuro.

Il Responsabile della sicurezza dei dati personali deve consegnare a ciascun Incaricato delle copie di sicurezza delle banche dati una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

## 4.11 Istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili

Il Responsabile della sicurezza dei dati personali è responsabile della custodia e della conservazione dei supporti utilizzati per le copie dei dati.

Per ogni banca di dati deve essere individuato il luogo di conservazione copie dei dati in modo che sia convenientemente protetto dai potenziali rischi di:

1. Agenti chimici
2. Fonti di calore
3. Campi magnetici
4. Intrusioni e atti vandalici
5. Incendio
6. Allagamento
7. Furto

Nel modulo MOD\_BCKP deve essere specificato il luogo di conservazione supporti utilizzati per le copie dei dati.

L'accesso ai supporti utilizzati per le copie dei dati è limitato per ogni banca di dati a:

1. Incaricati delle copie di sicurezza delle banche dati
2. Responsabile della sicurezza dei dati personali

## 4.12 Misure in caso di trattamento di dati sensibili o giudiziari

### 4.12.1 Protezione contro l'accesso abusivo

Al fine di garantire la sicurezza dei dati sensibili o giudiziari contro l'accesso abusivo, il Responsabile della sicurezza dei dati personali, stabilisce, con il supporto tecnico dei Responsabili della gestione e della manutenzione degli strumenti elettronici, le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione o di hacker su ogni sistema collegato in rete pubblica.

I criteri debbono essere definiti dal Responsabile della sicurezza dei dati personali in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In particolare per ogni sistema interessato debbono essere definite le seguenti specifiche:

1. Le misure applicate per evitare intrusioni.
2. Le misure applicate per evitare contagi da Virus Informatici.

Deve essere utilizzato il modulo MOD\_FW\_AV che va conservato a cura del Responsabile della gestione e della manutenzione degli strumenti elettronici in luogo sicuro e deve essere trasmesso in copia al Responsabile della sicurezza dei dati personali.

### 4.12.2 Riutilizzo dei supporti rimovibili

Se il Responsabile della gestione e della manutenzione degli strumenti elettronici decide che i supporti magnetici contenenti dati sensibili o giudiziari non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto annullando e rendendo intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso contenute.

È compito del Responsabile della gestione e della manutenzione degli strumenti elettronici assicurarsi che in nessun caso vengano lasciate copie di Banche di dati contenenti dati sensibili o giudiziari, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso registrate.

### 4.12.3 Ripristino dell'accesso ai dati in caso di danneggiamento

La decisione di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento è compito esclusivo del Responsabile della sicurezza dei dati personali.

La decisione di ripristinare la disponibilità dei dati deve essere presa rapidamente e in ogni caso la disponibilità dei dati deve essere ripristinata al massimo entro sette giorni.

Una volta valutata la assoluta necessità di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento il Responsabile della sicurezza dei dati personali deve provvedere tramite l'Incaricato delle copie di sicurezza delle banche dati e tramite il Responsabile della gestione e della manutenzione degli strumenti elettronici all'operazione di ripristino dei dati.

La decisione di ripristinare la funzionalità degli elaboratori elettronici guasti, è compito esclusivo del Responsabile della sicurezza dei dati personali che si può avvalere del parere del Responsabile della gestione e della manutenzione degli strumenti elettronici.

La decisione di ripristinare la funzionalità degli elaboratori elettronici guasti deve essere presa rapidamente e in ogni caso la funzionalità deve essere ripristinata al massimo entro sette giorni.

## 4.13 Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali

Se nello svolgimento delle proprie attività, in particolare quelle industriali, commerciali, professionali o istituzionali, si è fatto uso di supporti che contengono dati personali, quando tali supporti giungono al termine del loro ciclo di impiego, il Responsabile della sicurezza dei dati personali, in collaborazione con il Responsabile della gestione e manutenzione degli strumenti elettronici deve provvedere alla distruzione o dismissione adottando idonei accorgimenti e misure, anche con l'ausilio di terzi tecnicamente qualificati, volti a prevenire accessi non consentiti ai dati personali memorizzati nelle apparecchiature elettriche ed elettroniche destinate a essere reimpiegate, riciclate o smaltite, compilando il registro MOD\_RAEE

Tali misure e accorgimenti possono essere attuate anche con l'ausilio o conferendo incarico a terzi tecnicamente qualificati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

Chi procede al reimpiego o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti è comunque tenuto ad assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo, ove possibile, l'autorizzazione a cancellarli o a renderli non intelligibili.

### 4.13.1 Reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche

In caso di reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche le misure e gli accorgimenti volti a prevenire accessi non consentiti ai dati personali in esse contenuti, adottati nel rispetto delle normative di settore, devono consentire l'effettiva cancellazione dei dati o garantire la loro non intelligibilità. Tali misure, anche in combinazione tra loro, devono tenere conto degli standard tecnici esistenti e possono consistere, tra l'altro, in:

#### Misure tecniche preventive per la memorizzazione sicura dei dati, applicabili a dispositivi elettronici o informatici

1. Cifratura di singoli file o gruppi di file, di volta in volta protetti con parole-chiave riservate, note al solo utente proprietario dei dati, che può con queste procedere alla successiva decifratura. Questa modalità richiede l'applicazione della procedura di cifratura ogni volta che sia necessario proteggere un dato o una porzione di dati (file o collezioni di file), e comporta la necessità per l'utente di tenere traccia separatamente delle parole-chiave utilizzate.
2. Memorizzazione dei dati sui dischi rigidi (hard-disk) dei personal computer o su altro genere di supporto magnetico od ottico (cd-rom, dvd-r) in forma automaticamente cifrata al momento della loro scrittura, tramite l'uso di parole-chiave riservate note al solo utente. Può effettuarsi su interi volumi di dati registrati su uno o più dispositivi di tipo disco rigido o su porzioni di essi (partizioni, drive logici, file-system) realizzando le funzionalità di un c.d. file-system crittografico (disponibili sui principali sistemi operativi per elaboratori elettronici, anche di tipo personal computer, e dispositivi elettronici) in grado di proteggere, con un'unica parola-chiave riservata, contro i rischi di acquisizione indebita delle informazioni registrate. L'unica parola-chiave di volume verrà automaticamente utilizzata per le operazioni di cifratura e decifratura, senza modificare in alcun modo il comportamento e l'uso dei programmi software con cui i dati vengono trattati.

#### Misure tecniche per la cancellazione sicura dei dati, applicabili a dispositivi elettronici o informatici

1. Cancellazione sicura delle informazioni, ottenibile con programmi informatici (quali wiping program o file shredder) che provvedono, una volta che l'utente abbia eliminato dei file da un'unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti

dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre binarie (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati. Il numero di ripetizioni del procedimento considerato sufficiente a raggiungere una ragionevole sicurezza (da rapportarsi alla delicatezza o all'importanza delle informazioni di cui si vuole impedire l'indebita acquisizione) varia da sette a trentacinque e incide proporzionalmente sui tempi di applicazione delle procedure, che su dischi rigidi ad alta capacità (oltre i 100 gigabyte) possono impiegare diverse ore o alcuni giorni), a secondo della velocità del computer utilizzato.

2. Formattazione a basso livello dei dispositivi di tipo hard disk (low-level formatting), laddove effettuabile, attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;
3. Demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, floppy-disk, nastri magnetici su bobine aperte o in cassette), in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione software (che richiedono l'accessibilità del dispositivo da parte del sistema a cui è interconnesso).

#### 4.13.2 Smaltimento di rifiuti elettrici ed elettronici

In caso di smaltimento di rifiuti elettrici ed elettronici, l'effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche può anche risultare da procedure che, nel rispetto delle normative di settore, comportino la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l'acquisizione indebita di dati personali.

La distruzione dei supporti prevede il ricorso a procedure o strumenti diversi a secondo del loro tipo, quali:

- sistemi di punzonatura o deformazione meccanica;
- distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd);
- demagnetizzazione ad alta intensità.

## Capitolo 5

# Ulteriori disposizioni per il trattamento

### 5.1 Periodicità di revisione del Regolamento

Entro il 31 marzo di ogni anno, il Titolare del trattamento di dati sensibili o di dati giudiziari deve verificare ed eventualmente predisporre una nuova versione del Regolamento in quanto valevole come Documento programmatico sulla sicurezza contenente idonee informazioni riguardo ai punti 19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L).

### 5.2 Descrizione degli interventi effettuati da soggetti esterni

Nel caso in cui ci si avvale di soggetti esterni alla propria struttura, per provvedere alla riparazione il Responsabile della sicurezza dei dati personali, deve richiedere al tecnico che ha effettuato la riparazione, una descrizione scritta dell'intervento effettuato che ne attesti la conformità a quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

### 5.3 Regolamento per l'attività di recupero crediti

La struttura nelle vesti del suo titolare del trattamento richiede agli incaricati che si occuperanno per suo conto di recupero crediti, finanziarie e concessionarie di pubblici servizi di attenersi alle seguenti normative nel rispetto delle prescrizioni del Garante per non incorrere in illeciti e per rispettare i principi posti a tutela dei diritti dei cittadini.

Non sono ammesse prassi invasive o lesive della dignità personale. Per sollecitare ed ottenere il pagamento di somme dovute non è lecito comunicare ingiustificatamente informazioni relative ai mancati pagamenti ad altri soggetti che non siano l'interessato (es. familiari, colleghi di lavoro o vicini di casa) ed esercitare indebite pressioni su quest'ultimo.

Non si deve far ricorso a telefonate preregistrate perché con questa modalità persone diverse dal debitore possono venire a conoscenza di una sua eventuale condizione di inadempienza.

Illecita è pure l'affissione da parte degli incaricati del recupero crediti di avvisi di mora sulla porta di casa, modalità questa che rende possibile la diffusione dei dati personali dell'interessato ad una serie indeterminata di soggetti.

Non si deve inoltre rendere visibile a persone estranee il contenuto di una comunicazione, come può accadere con l'utilizzo di cartoline postali o con l'invio di plichi recanti all'esterno la scritta "recupero crediti" o formule simili. È necessario, invece, che le sollecitazioni di pagamento vengano portate a conoscenza del solo debitore, usando plichi chiusi e senza scritte specifiche.

Gli incaricati delle società non possono usare altri dati se non quelli assolutamente necessari all'esecuzione del mandato (dati anagrafici, codice fiscale, ammontare del credito, recapiti telefonici).

Una volta assolto l'incarico e acquisite le somme, i dati devono essere cancellati.

## 5.4 Trattamenti in contitolarità

Qualunque trattamento di dati personali può essere svolto in contitolarità con altri soggetti. In alcuni casi la contitolarità deriva da una volontà esplicita, comune ed organizzata dei singoli soggetti titolari, che distribuiscono tra loro compiti, incarichi e misure di protezione, ma che detengono collegialmente la responsabilità delle decisioni in ordine alle finalità ed alle modalità del trattamento.

In altri casi, non esiste una reale volontà, quanto piuttosto l'adozione di una norma giuridica che impone ed attribuisce lo status di contitolare a soggetti che normalmente non operano nell'ambito del trattamento, ma che potrebbero esservi interessati e a cui va garantito il diritto di parteciparvi, trovandosi di norma in una posizione svantaggiata. Tale partecipazione si concretizza di solito con l'accesso alle informazioni, piuttosto che con l'attribuzione di un incarico di trattamento.

Nel seguito è presentata la casistica di trattamenti che sottostanno ad obblighi di legge e che determinano l'implicita contitolarità del trattamento tra diversi soggetti.

### 5.4.1 Libro soci

I provvedimenti del Garante del 19 dicembre 2000 e del 26 marzo 2009 resi in merito al diritto di ispezione al libro soci nelle società e cooperative, ribadiscono che la comunicazione dei dati personali può avvenire senza il consenso delle persone cui si riferiscono i dati, quando si tratta di adempiere ad un obbligo normativo. Nella fattispecie, l'art. 2422 cod. civ. riconosce ai soci il diritto di accedere alle informazioni obbligatoriamente annotate nel libro dei soci ai sensi dell'art. 2421 del Codice Civile (il numero delle azioni, il cognome e il nome dei titolari delle azioni nominative, i trasferimenti e i vincoli ad esse relativi e i versamenti eseguiti). Altre norme (art. 4 R.D. 29 marzo 1942, n. 239; art. 5, Legge 29 dicembre 1962, n. 1745) integrano i dati da annotarsi nel libro soci: in particolare, domicilio per le persone fisiche e sede principale per le persone giuridiche. Alla luce di tali dispositivi di Legge, il Garante ha confermato la liceità della richiesta dei dati anagrafici completi presenti nel libro soci da parte del socio che ne faccia richiesta ai sensi dell'art. 2422 cod. civ., eventualmente ottenendone estratti a proprie spese, senza che sia previamente necessario chiedere il consenso ai consoci interessati.

Per quanto riguarda ulteriori dati (e-mail, telefono, codice fiscale, ecc.) eventualmente raccolti e trattati, non essendovi al riguardo disposizioni di legge, risultano di completa ed esclusiva responsabilità del titolare del trattamento, il quale non è tenuto a condividere tali informazioni né potrebbe farlo senza aver prima acquisito il consenso di tutti gli interessati.



## Capitolo 6

# Diritti dell'interessato

### 6.1 Diritto di accesso ai dati personali

L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

L'interessato ha diritto di ottenere l'indicazione:

1. dell'origine dei dati personali;
2. delle finalità e modalità del trattamento;
3. della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
4. dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

L'interessato ha diritto di ottenere:

1. l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
2. l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

L'interessato ha diritto di opporsi, in tutto o in parte:

1. per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
2. al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

## 6.2 Esercizio dei diritti

I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.

I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati:

1. in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio;
2. in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;
3. da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione; d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
4. ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;
5. da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n.397;
6. per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;
7. ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1° aprile 1981, n. 121.

Il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere a), b), d), e) ed f), provvede nei modi di cui agli articoli 157, 158 e 159 e, nei casi di cui alle lettere c), g) ed h) del medesimo comma, provvede nei modi di cui all'articolo 160.

L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché "indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

## 6.3 Modalità di esercizio

La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.

Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.

I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.

La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

## 6.4 Riscontro all'interessato

Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:

1. ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
2. a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1.

Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.

Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.

Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.

Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro.

## Capitolo 7

# Trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro

### 7.1 Premessa

Con riguardo alle operazioni di trattamento effettuate con dati personali (anche sensibili) di lavoratori operanti alle dipendenze di datori di lavoro privati, il Garante ha introdotto un insieme di linee guida, comprendenti precedenti decisioni dell'Autorità stessa.

Le indicazioni fornite non pregiudicano l'applicazione delle disposizioni di legge o di regolamento che stabiliscono divieti o limiti più restrittivi in relazione a taluni settori o a specifici casi di trattamento di dati (artt. 113, 114 e 184, comma 3, del Codice).

Le tematiche prese in considerazione si riferiscono prevalentemente alla comunicazione e alla diffusione dei dati, all'informativa che il datore di lavoro deve rendere ai lavoratori (art. 13 del Codice), ai dati idonei a rivelare lo stato di salute e il diritto d'accesso.

Le operazioni di trattamento riguardano per lo più:

- dati anagrafici di lavoratori (assunti o cessati dal servizio), dati biometrici, fotografie e dati sensibili riferiti anche a terzi, idonei in particolare a rivelare il credo religioso o l'adesione a sindacati; dati idonei a rivelare lo stato di salute, di regola contenuti in certificati medici o in altra documentazione prodotta per giustificare le assenze dal lavoro o per fruire di particolari permessi e benefici previsti anche nei contratti collettivi;
- informazioni più strettamente connesse allo svolgimento dell'attività lavorativa, quali la tipologia del contratto (a tempo determinato o indeterminato, a tempo pieno o parziale, etc.); la qualifica e il livello professionale, la retribuzione individuale corrisposta anche in virtù di provvedimenti ad personam; l'ammontare di premi; il tempo di lavoro anche straordinario; ferie e permessi individuali (fruiti o residui); l'assenza dal servizio nei casi previsti dalla legge o dai contratti anche collettivi di lavoro; trasferimenti ad altra sede di lavoro; procedimenti e provvedimenti disciplinari.

I medesimi dati sono:

- contenuti in atti e documenti prodotti dai lavoratori in sede di assunzione (rispetto ai quali, con riferimento alle informazioni raccolte mediante annunci contenenti offerte di lavoro, questa Autorità si è già pronunciata o nel corso del rapporto di lavoro;
- contenuti in documenti e/o file elaborati dal (o per conto del) datore di lavoro in pendenza del rapporto di lavoro per finalità di esecuzione del contratto e successivamente raccolti e conservati in fascicoli personali, archivi cartacei o elettronici aziendali;

- resi disponibili in albi e bacheche o, ancora, nelle intranet aziendali.

## 7.2 Il rispetto dei principi di protezione dei dati personali

Le predette informazioni di carattere personale possono essere trattate dal datore di lavoro nella misura in cui siano necessarie per dare corretta esecuzione al rapporto di lavoro; talvolta, sono anche indispensabili per attuare previsioni contenute in leggi, regolamenti, contratti e accordi collettivi.

In ogni caso, deve trattarsi di informazioni pertinenti e non eccedenti e devono essere osservate tutte le disposizioni della vigente disciplina in materia di protezione dei dati personali che trae origine anche da direttive comunitarie.

In particolare, il Codice in materia di protezione dei dati personali (Codice), in attuazione delle direttive 95/46/CE e 2002/58/CE, prescrive che il trattamento di dati personali avvenga:

- nel rispetto di principi di necessità e liceità e che riguardano la qualità dei dati (artt. 3 e 11);
- informando preventivamente e adeguatamente gli interessati (art. 13);
- chiedendo preventivamente il consenso solo quando, anche a seconda della natura dei dati, non sia corretto avvalersi di uno degli altri presupposti equipollenti al consenso (artt. 23, 24, 26 e 43 del Codice);
- rispettando, se si trattano dati sensibili o giudiziari, le prescrizioni impartite dal Garante nelle autorizzazioni anche di carattere generale rilasciate (artt. 26 e 27 del Codice; cfr., in particolare, l'autorizzazione generale n. 1/2005);
- adottando le misure di sicurezza idonee a preservare i dati da alcuni eventi tra i quali accessi ed utilizzazioni indebite, rispetto ai quali può essere chiamato a rispondere anche civilmente e penalmente (artt. 15, 31 e ss., 167 e 169 del Codice).

Il trattamento di dati personali riferibili a singoli lavoratori, anche sensibili, è lecito, se finalizzato ad assolvere obblighi derivanti dal contratto individuale (ad esempio, per verificare l'esatto adempimento della prestazione o commisurare l'importo della retribuzione, anche per lavoro straordinario, o dei premi da corrispondere, per quantificare le ferie e i permessi, per appurare la sussistenza di una causa legittima di assenza).

Alcuni scopi sono altresì previsti dalla contrattazione collettiva per la determinazione di circostanze relative al rapporto di lavoro individuale (ad esempio, per la fruizione di permessi o aspettative sindacali e periodi di comporto o rispetto alle percentuali di lavoratori da assumere con particolari tipologie di contratto) o, ancora, dalla legge (quali, ad esempio, le comunicazioni ad enti previdenziali e assistenziali).

Se queste finalità sono in termini generali lecite, occorre però rispettare il principio della compatibilità tra gli scopi perseguiti (art. 11, comma 1, lett. b), del Codice): lo scopo perseguito in concreto dal datore di lavoro sulla base del trattamento di dati personali non deve essere infatti incompatibile con le finalità per le quali i medesimi sono stati raccolti.

## 7.3 Titolare e responsabile del trattamento

### 7.3.1 Titolare e responsabile

Ai fini della protezione dei dati personali assume un ruolo rilevante identificare le figure soggettive che a diverso titolo possono trattare i dati, definendo chiaramente le rispettive attribuzioni, in particolare, quelle del titolare e del responsabile del trattamento (artt. 4, comma 1, lett. f) e g), 28 e

29 del Codice). In linea di principio, per individuare il titolare del trattamento rileva l'effettivo centro di imputazione del rapporto di lavoro, al di là dello schema societario formalmente adottato. Peraltro, specie nelle realtà imprenditoriali più articolate, questa identificazione può risultare non sempre agevole e tale circostanza costituisce in qualche caso un ostacolo anche per l'esercizio dei diritti di cui all'art. 7

### 7.3.2 Gruppi di imprese

Le società che appartengono a gruppi di imprese individuati in conformità alla legge (art. 2359 cod. civ.; d.lg. 2 aprile 2002, n. 74) hanno di regola una distinta ed autonoma titolarità del trattamento in relazione ai dati personali dei propri dipendenti e collaboratori (artt. 4, comma 1, lett. f) e 28 del Codice).

Tuttavia, nell'ambito dei gruppi, le società controllate e collegate possono delegare la società capogruppo a svolgere adempimenti in materia di lavoro, previdenza ed assistenza sociale per i lavoratori indicati dalla legge (Cfr. art. 1 della legge 11 gennaio 1979, n. 12; cfr. art. 31, comma 1, d.lg. 10 settembre 2003, n. 276; l. 14 febbraio 2003, n. 30): tale attività implica la designazione della società capogruppo quale responsabile del trattamento ai sensi dell'art. 29 del Codice.

Analoga soluzione (art. 31, comma 2, d.lg. n. 276/2003) deve essere adottata per i trattamenti di dati personali, aventi identica natura, effettuati nell'ambito dei consorzi di società cooperative (nei quali a tal fine può essere altresì designata una delle società consorziate).

### 7.3.3 Medico competente

Considerazioni ulteriori devono essere svolte in relazione a taluni specifici trattamenti che possono o devono essere effettuati all'interno dell'impresa in conformità alla disciplina in materia di sicurezza e igiene del lavoro (Nuovo T.U. 81/2008 Sicurezza sul Lavoro).

Tale disciplina, che attua anche alcune direttive comunitarie e si colloca nell'ambito del più generale quadro di misure necessarie a tutelare l'integrità psico-fisica dei lavoratori (art. 2087 cod. civ.), pone direttamente in capo al medico competente in materia di igiene e sicurezza dei luoghi di lavoro la sorveglianza sanitaria obbligatoria (e per quanto previsto dal Nuovo T.U. 81/2008 la modalità di gestione, trattamento e conservazione dei dati contenuti in cartelle cliniche).

In quest'ambito, il medico competente effettua accertamenti preventivi e periodici sui lavoratori e istituisce (curandone l'aggiornamento) una cartella sanitaria e di rischio.

Detta cartella è custodita presso l'azienda o l'unità produttiva, o presso lo studio del medico competente con salvaguardia del segreto professionale, e (consegnata in) copia al lavoratore stesso al momento della risoluzione del rapporto di lavoro, ovvero quando lo stesso ne fa richiesta; in caso di cessazione del rapporto di lavoro le cartelle sono trasmesse all'Istituto superiore prevenzione e sicurezza sul lavoro-Ispesl, in originale e in busta chiusa.

In relazione a tali disposizioni, il medico competente è deputato a trattare i dati sanitari dei lavoratori, procedendo alle dovute annotazioni nelle cartelle sanitarie e di rischio, e curando le opportune misure di sicurezza per salvaguardare la segretezza delle informazioni trattate in rapporto alle finalità e modalità del trattamento stabilite. Ciò, quale che sia il titolare del trattamento effettuato dal medico (il medico opera quale libero professionista, o quale dipendente del datore di lavoro o di aziende sanitarie locali).

Alle predette cartelle il datore di lavoro non può accedere, dovendo soltanto concorrere ad assicurarne un'efficace custodia nei locali aziendali (anche in vista di possibili accertamenti ispettivi da parte dei soggetti istituzionalmente competenti), ma, come detto, con salvaguardia del

segreto professionale.

Il datore di lavoro, sebbene sia tenuto, su parere del medico competente (o qualora il medico lo informi di anomalie imputabili all'esposizione a rischio), ad adottare le misure preventive e protettive per i lavoratori interessati, non può conoscere le eventuali patologie accertate, ma solo la valutazione finale circa l'idoneità del dipendente (dal punto di vista sanitario) allo svolgimento di date mansioni.

In tal senso, peraltro, depongono anche le previsioni legislative che dispongono la comunicazione all'Ispesl della cartella sanitaria e di rischio in caso di cessione o cessazione del rapporto di lavoro, precludendosi anche in tali occasioni ogni loro conoscibilità da parte del datore di lavoro.

## 7.4 Dati biometrici e accesso ad aree riservate

In più circostanze, anche ricorrendo al procedimento previsto dall'art. 17 del Codice, è stato prospettato al Garante l'utilizzo di dati biometrici sul luogo di lavoro, con particolare riferimento all'impiego di tali informazioni per accedere ad aree specifiche dell'impresa.

Si tratta di dati ricavati dalle caratteristiche fisiche o comportamentali della persona a seguito di un apposito procedimento (in parte automatizzato) e poi risultanti in un modello di riferimento. Quest'ultimo consiste in un insieme di valori numerici ricavati, attraverso funzioni matematiche, dalle caratteristiche individuali sopra indicate, preordinati all'identificazione personale attraverso opportune operazioni di confronto tra il codice numerico ricavato ad ogni accesso e quello originariamente raccolto.

L'uso generalizzato e incontrollato di dati biometrici, specie se ricavati dalle impronte digitali, non è lecito. Tali dati, per la loro peculiare natura, richiedono l'adozione di elevate cautele per prevenire possibili pregiudizi a danno degli interessati, con particolare riguardo a condotte illecite che determinino l'abusiva ricostruzione dell'impronta, partendo dal modello di riferimento, e la sua ulteriore utilizzazione a loro insaputa.

L'utilizzo di dati biometrici può essere giustificato solo in casi particolari, tenuto conto delle finalità e del contesto in cui essi sono trattati e, in relazione ai luoghi di lavoro, per presidiare accessi ad aree sensibili, considerata la natura delle attività ivi svolte: si pensi, ad esempio, a processi produttivi pericolosi o sottoposti a segreti di varia natura o al fatto che particolari locali siano destinati alla custodia di beni, documenti segreti o riservati o oggetti di valore

Inoltre, nei casi in cui l'uso dei dati biometrici è consentito, la centralizzazione in una banca dati delle informazioni personali (nella forma del predetto modello) trattate nell'ambito del descritto procedimento di riconoscimento biometrico risulta di regola sproporzionata e non necessaria. I sistemi informativi devono essere infatti configurati in modo da ridurre al minimo l'utilizzazione di dati personali e da escluderne il trattamento, quando le finalità perseguite possono essere realizzate con modalità tali da permettere di identificare l'interessato solo in caso di necessità (artt. 3 e 11 del Codice).

In luogo, quindi, di modalità centralizzate di trattamento dei dati biometrici, deve ritenersi adeguato e sufficiente avvalersi di sistemi efficaci di verifica e di identificazione biometrica basati sulla lettura delle impronte digitali memorizzate, tramite il predetto modello cifrato, su un supporto posto nell'esclusiva disponibilità dell'interessato (una smart card o un dispositivo analogo) e privo di indicazioni nominative riferibili a quest'ultimo (essendo sufficiente attribuire a ciascun dipendente un codice individuale).

Tale modalità di riconoscimento, infatti, è idonea ad assicurare che possano accedere all'area riservata solo coloro che, autorizzati preventivamente, decidano su base volontaria di avvalersi della predetta carta o del dispositivo analogo. Il confronto delle impronte digitali con il modello



memorizzato sulla carta o sul dispositivo può essere realizzato ricorrendo a comuni procedure di confronto sulla carta o dispositivo stesso, evitando così la costituzione di un archivio di delicati dati biometrici. Del resto, in caso di smarrimento della carta o dispositivo, sono allo stato circoscritte le possibilità di abuso rispetto ai dati biometrici ivi memorizzati.

I dati personali necessari per realizzare il modello possono essere trattati esclusivamente durante la fase di registrazione; per il loro utilizzo, il titolare del trattamento deve raccogliere il preventivo consenso informato degli interessati.

In aggiunta alle misure di sicurezza minime prescritte dal Codice, devono essere adottati ulteriori accorgimenti a protezione dei dati, impartendo agli incaricati apposite istruzioni scritte alle quali attenersi, con particolare riguardo al caso di perdita o sottrazione delle carte o dispositivi loro affidati.

I dati memorizzati devono essere accessibili al personale preposto al rispetto delle misure di sicurezza all'interno dell'impresa, per l'esclusiva finalità della verifica della loro osservanza (rispettando peraltro la disciplina sul controllo a distanza dei lavoratori: art. 4, comma 2, l. 20 maggio 1970, n. 300, richiamato dall'art. 114 del Codice).

I dati raccolti non possono essere di regola conservati per un arco di tempo superiore a sette giorni e vanno assicurati, anche quando tale arco temporale possa essere lecitamente protratto, idonei meccanismi di cancellazione automatica dei dati.

Resta salva, per fattispecie particolari o in ragione di situazioni eccezionali non considerate in questa sede, la presentazione da parte di titolari del trattamento che intendano discostarsi dalle presenti prescrizioni, di apposito interpello al Garante, ai sensi dell'art. 17 del Codice.

## 7.5 Comunicazione e diffusione di dati personali

### 7.5.1 Comunicazione

La conoscenza dei dati personali relativi ad un lavoratore da parte di terzi è ammessa se l'interessato vi acconsente.

Se il datore di lavoro non può avvalersi correttamente di uno degli altri presupposti del trattamento equipollenti al consenso (art. 24 del Codice), non può prescindere dal consenso stesso per comunicare dati personali (ad esempio, inerenti alla circostanza di un'avvenuta assunzione, allo status o alla qualifica ricoperta, all'irrogazione di sanzioni disciplinari o a trasferimenti del lavoratore) a terzi quali:

- associazioni (anche di categoria) di datori di lavoro, o di ex dipendenti (anche della medesima istituzione);
- conoscenti, familiari e parenti.

Fermo restando il rispetto dei principi generali sopra richiamati in materia di trattamento di dati personali, rimane impregiudicata la facoltà del datore di lavoro di disciplinare le modalità del proprio trattamento designando i soggetti, interni o esterni, incaricati o responsabili del trattamento, che possono acquisire conoscenza dei dati inerenti alla gestione del rapporto di lavoro, in relazione alle funzioni svolte e a idonee istruzioni scritte alle quali attenersi (artt. 4, comma 1, lett. g) e h), 29 e 30). Ciò, ove necessario, anche mediante consegna di copia di documenti all'uopo predisposti.

È altresì impregiudicata la facoltà del datore di lavoro di comunicare a terzi in forma realmente anonima dati ricavati dalle informazioni relative a singoli o gruppi di lavoratori: si pensi al numero

complessivo di ore di lavoro straordinario prestate o di ore non lavorate a livello aziendale o all'interno di singole unità produttive, agli importi di premi aziendali di risultato individuati per fasce, o qualifiche/livelli professionali, anche nell'ambito di singole funzioni o unità organizzative).

### 7.5.2 Intranet aziendale

Allo stesso modo, il consenso del lavoratore è necessario per pubblicare informazioni personali allo stesso riferite (quali fotografia, informazioni anagrafiche o curricula) nella intranet aziendale (e a maggior ragione in Internet), non risultando tale ampia circolazione di dati personali di regola necessaria per eseguire obblighi derivanti dal contratto di lavoro (art. 24, comma 1, lett. b), del Codice). Tali obblighi possono trovare esecuzione indipendentemente da tale particolare forma di divulgazione che comunque, potendo a volte risultare pertinente (specie in realtà produttive di grandi dimensioni o ramificate sul territorio), richiede il preventivo consenso del singolo dipendente, salva specifica disposizione di legge.

### 7.5.3 Diffusione

In assenza di specifiche disposizioni normative che impongano al datore di lavoro la diffusione di dati personali riferiti ai lavoratori (art. 24, comma 1, lett. a) o la autorizzino, o comunque di altro presupposto ai sensi dell'art. 24 del Codice, la diffusione stessa può avvenire solo se necessaria per dare esecuzione a obblighi derivanti dal contratto di lavoro (art. 24, comma 1, lett. b) del Codice). È il caso, ad esempio, dell'affissione nella bacheca aziendale di ordini di servizio, di turni lavorativi o feriali, oltre che di disposizioni riguardanti l'organizzazione del lavoro e l'individuazione delle mansioni cui sono deputati i singoli dipendenti.

Salvo che ricorra una di queste ipotesi, non è invece di regola lecito dare diffusione a informazioni personali riferite a singoli lavoratori, anche attraverso la loro pubblicazione in bacheche aziendali o in comunicazioni interne destinate alla collettività dei lavoratori, specie se non correlate all'esecuzione di obblighi lavorativi. In tali casi la diffusione si pone anche in violazione dei principi di finalità e pertinenza (art. 11 del Codice), come nelle ipotesi di:

- affissione relativa ad emolumenti percepiti o che fanno riferimento a particolari condizioni personali;
- sanzioni disciplinari irrogate o informazioni relative a controversie giudiziarie;
- assenze dal lavoro per malattia;
- iscrizione e/o adesione dei singoli lavoratori ad associazioni.

### 7.5.4 Cartellini identificativi

Analogamente, si possono determinare altre forme di diffusione di dati personali quando dette informazioni debbano essere riportate ed esibite su cartellini identificativi appuntati ad esempio sull'abito o sulla divisa del lavoratore (di solito, con lo scopo di migliorare il rapporto fra operatori ed utenti o clienti).

In relazione allo svolgimento del rapporto di lavoro alle dipendenze di soggetti privati, l'obbligo di portare in modo visibile un cartellino identificativo può trovare fondamento in alcune prescrizioni contenute in accordi sindacali aziendali, il cui rispetto può essere ricondotto alle prescrizioni del contratto di lavoro. Tuttavia, in relazione al rapporto con il pubblico, si è ravvisata la sproporzione dell'indicazione sul cartellino di dati personali identificativi (generalità o dati anagrafici), ben potendo spesso risultare sufficienti altre informazioni (quali codici identificativi, il solo nome o il ruolo professionale svolto), per sé sole in grado di essere d'ausilio all'utenza.

### 7.5.5 Modalità di comunicazione

Salvi i casi in cui forme e modalità di divulgazione di dati personali discendano da specifiche previsioni (cfr. art. 174, comma 12, del Codice) 19, il datore di lavoro deve utilizzare forme di comunicazione individualizzata con il lavoratore, adottando le misure più opportune per prevenire un'indebita comunicazione di dati personali, in particolare se sensibili, a soggetti diversi dal destinatario, ancorché incaricati di talune operazioni di trattamento (ad esempio, inoltrando le comunicazioni in plico chiuso o spillato; invitando l'interessato a ritirare personalmente la documentazione presso l'ufficio competente; ricorrendo a comunicazioni telematiche individuali).

Analoghe cautele, tenendo conto delle circostanze di fatto, devono essere adottate in relazione ad altre forme di comunicazione indirizzate al lavoratore dalle quali possano desumersi vicende personali.

## 7.6 Dati idonei a rivelare lo stato di salute di lavoratori

### 7.6.1 Dati sanitari

Devono essere osservate cautele particolari anche nel trattamento dei dati sensibili del lavoratore (art. 4, comma 1, lett. d), del Codice) e, segnatamente, di quelli dati idonei a rivelarne lo stato di salute. Tra questi ultimi, può rientrare l'informazione relativa all'assenza dal servizio per malattia, indipendentemente dalla circostanza della contestuale enunciazione della diagnosi 21. Per tali informazioni, l'ordinamento appresta anche fuori della disciplina di protezione dei dati personali particolari accorgimenti per contenere, nei limiti dell'indispensabile, i dati dei quali il datore di lavoro può venire a conoscenza per dare esecuzione al contratto (cfr. già l'art. 8 della legge n. 300/1970).

In questo contesto, la disciplina generale contenuta nel Codice deve essere coordinata ed integrata, come si è visto (cfr. punto 3.3.), con altre regole settoriali o speciali. Resta comunque vietata la diffusione di dati sanitari (art. 26, comma 5, del Codice).

### 7.6.2 Assenze per ragioni di salute

Con specifico riguardo al trattamento di dati idonei a rivelare lo stato di salute dei lavoratori, la normativa di settore e le disposizioni contenute nei contratti collettivi giustificano il trattamento dei dati relativi ai casi di infermità (e talora a quelli inerenti all'esecuzione di visite specialistiche o di accertamenti clinici) che determini un'incapacità lavorativa (temporanea o definitiva, con la conseguente sospensione o risoluzione del contratto). Non diversamente, il datore di lavoro può trattare dati relativi a invalidità o all'appartenenza a categorie protette, nei modi e per le finalità prescritte dalla vigente normativa in materia.

A tale riguardo, infatti, sussiste un quadro normativo articolato che prevede anche obblighi di comunicazione in capo al lavoratore e di successiva certificazione nei confronti del datore di lavoro e dell'ente previdenziale della condizione di malattia: obblighi funzionali non solo a giustificare i trattamenti normativi ed economici spettanti al lavoratore, ma anche a consentire al datore di lavoro, nelle forme di legge, di verificare le reali condizioni di salute del lavoratore.

Per attuare tali obblighi viene utilizzata un'apposita modulistica, consistente in un attestato di malattia da consegnare al datore di lavoro - con la sola indicazione dell'inizio e della durata presunta dell'infermità: c.d. prognosi - e in un certificato di diagnosi da consegnare, a cura del lavoratore stesso, all'Istituto nazionale della previdenza sociale (INPS) o alla struttura pubblica indicata dallo stesso Istituto d'intesa con la regione, se il lavoratore ha diritto a ricevere l'indennità di malattia a carico dell'ente previdenziale.

Tuttavia, qualora dovessero essere presentati dai lavoratori certificati medici redatti su moduli diversa da quella sopra descritta, nella quale i dati di prognosi e di diagnosi non siano separati, i datori di lavoro restano obbligati, ove possibile, ad adottare idonee misure e accorgimenti volti a prevenirne la ricezione o, in ogni caso, ad oscurarli.

### 7.6.3 Denuncia all'INAIL

Diversamente, per dare esecuzione ad obblighi di comunicazione relativi a dati sanitari, in taluni casi il datore di lavoro può anche venire a conoscenza delle condizioni di salute del lavoratore.

Tra le fattispecie più ricorrenti deve essere annoverata la denuncia all'Istituto assicuratore (INAIL) avente ad oggetto infortuni e malattie professionali occorsi ai lavoratori; essa, infatti, per espressa previsione normativa, deve essere corredata da specifica certificazione medica (artt. 13 e 53 d.P.R. n. 1124/1965).

In tali casi, pur essendo legittima la conoscenza della diagnosi da parte del datore di lavoro, resta fermo a suo carico l'obbligo di limitarsi a comunicare all'ente assistenziale esclusivamente le informazioni sanitarie relative o collegate alla patologia denunciata e non anche dati sulla salute relativi ad altre assenze che si siano verificate nel corso del rapporto di lavoro, la cui eventuale comunicazione sarebbe eccedente e non pertinente, trattandosi di dati non rilevanti nel caso oggetto di denuncia (art. 11, commi 1 e 2 del Codice)

### 7.6.4 Altre informazioni relative alla salute

A tali fattispecie devono essere aggiunti altri casi nei quali può, parimenti, effettuarsi un trattamento di dati relativi alla salute del lavoratore (e finanche di suoi congiunti), anche al fine di permettergli di godere dei benefici di legge (quali, ad esempio, permessi o periodi prolungati di aspettativa con conservazione del posto di lavoro): si pensi, ad esempio, a informazioni relative a condizioni di handicap.

Allo stesso modo, il datore di lavoro può venire a conoscenza dello stato di tossicodipendenza del dipendente, ove questi richieda di accedere a programmi riabilitativi o terapeutici con conservazione del posto di lavoro (senza retribuzione), atteso l'onere di presentare (nei termini prescritti dai contratti collettivi) specifica documentazione medica al datore di lavoro (ai sensi dell'art. 124, commi 1 e 2, d.P.R. n. 309/1990).

### 7.6.5 Comunicazioni all'INPS

È altresì legittima la comunicazione di dati idonei a rivelare lo stato di salute dei lavoratori che il datore di lavoro faccia ai soggetti pubblici (enti previdenziali e assistenziali) tenuti a erogare le prescritte indennità in adempimento a specifici obblighi derivanti dalla legge, da altre norme o regolamenti o da previsioni contrattuali, nei limiti delle sole informazioni indispensabili.

In particolare, il datore di lavoro può comunicare all'Istituto nazionale della previdenza sociale (INPS) i dati del dipendente assente, anche per un solo giorno, al fine di farne controllare lo stato di malattia (art. 5, commi 1 e 2, l. 20 maggio 1970, n. 300) 29; a tal fine deve tenere a disposizione e produrre, a richiesta, all'Inps, la documentazione in suo possesso. Le eventuali visite di controllo sullo stato di infermità del lavoratore, ai sensi dell'art. 5 della legge 20 maggio 1970, n. 300, o su richiesta dell'Inps o della struttura sanitaria pubblica da esso indicata, sono effettuate dai medici dei servizi sanitari indicati dalle regioni (art. 2, l. n. 33/1980 cit.).

## 7.7 Informativa

Il datore di lavoro è tenuto a rendere al lavoratore, prima di procedere al trattamento dei dati personali che lo riguardano (anche in relazione alle ipotesi nelle quali la legge non richieda il suo consenso), un'informativa individualizzata completa degli elementi indicati dall'art. 13 del Codice: i lavoratori devono conoscere quali dati il datore di lavoro stia raccogliendo sul loro conto (direttamente o da altre fonti), quali siano gli scopi delle operazioni di trattamento previste o effettuate per tali dati sia per il presente che per il futuro.

Con particolare riferimento a realtà produttive nelle quali, per ragioni organizzative (ad esempio, per l'articolata dislocazione sul territorio o per il ricorso consistente a forme di out-sourcing) o dimensionali, può risultare difficoltoso per il singolo lavoratore esercitare i propri diritti ai sensi dell'art. 7 del Codice, è opportuna la designazione di un responsabile del trattamento appositamente deputato alla trattazione di tali profili (o di responsabili esterni alla società, che effettuino, ad esempio, l'attività di gestione degli archivi amministrativi dei dipendenti), indicandolo chiaramente nell'informativa fornita.

## 7.8 Misure di sicurezza

### 7.8.1 Dati sanitari

Il datore di lavoro titolare del trattamento è tenuto ad adottare ogni misura di sicurezza, anche minima, prescritta dal Codice a protezione dei dati personali dei dipendenti comunque trattati nell'ambito del rapporto di lavoro, ponendo particolare attenzione all'eventuale natura sensibile dei medesimi (art. 31 ss. e Allegato B) al Codice).

Dette informazioni devono essere conservate separatamente da ogni altro dato personale dell'interessato; ciò, deve trovare attuazione anche con riferimento ai fascicoli personali cartacei dei dipendenti (ad esempio, utilizzando sezioni appositamente dedicate alla custodia dei dati sensibili, inclusi quelli idonei a rivelare lo stato di salute del lavoratore, da conservare separatamente o in modo da non consentirne una indistinta consultazione nel corso delle ordinarie attività amministrative).

Del pari, nei casi in cui i lavoratori producano spontaneamente certificati medici su modulistica diversa da quella prevista, il datore di lavoro non può, comunque, utilizzare ulteriormente tali informazioni (art. 11, comma 2, del Codice) e deve adottare gli opportuni accorgimenti per non rendere visibili le diagnosi contenute nei certificati (ad esempio, prescrivendone la circolazione in busta chiusa previo oscuramento di tali informazioni); ciò, al fine di impedire ogni accesso abusivo a tali dati da parte di soggetti non previamente designati come incaricati o responsabili (art. 31 e ss. del Codice).

### 7.8.2 Incaricati

Resta fermo l'obbligo del datore di lavoro di preporre alla custodia dei dati personali dei lavoratori apposito personale, specificamente incaricato del trattamento, che deve avere cognizioni in materia di protezione dei dati personali e ricevere una formazione adeguata. In assenza di un'adeguata formazione degli addetti al trattamento dei dati personali il rispetto della riservatezza dei lavoratori sul luogo di lavoro non potrà mai essere garantito.

### 7.8.3 Misure fisiche ed organizzative

Il datore di lavoro deve adottare, tra l'altro (cfr. artt. 31 ss. del Codice), misure organizzative e fisiche idonee a garantire che:

- i luoghi ove si svolge il trattamento di dati personali dei lavoratori siano opportunamente protetti da indebite intrusioni;
- le comunicazioni personali riferibili esclusivamente a singoli lavoratori avvengano con modalità tali da escluderne l'indebita presa di conoscenza da parte di terzi o di soggetti non designati quali incaricati;
- siano impartite chiare istruzioni agli incaricati in ordine alla scrupolosa osservanza del segreto d'ufficio, anche con riguardo a dipendenti del medesimo datore di lavoro che non abbiano titolo per venire a conoscenza di particolari informazioni personali;
- sia prevenuta l'acquisizione e riproduzione di dati personali trattati elettronicamente, in assenza di adeguati sistemi di autenticazione o autorizzazione e/o di documenti contenenti informazioni personali da parte di soggetti non autorizzati 33;
- sia prevenuta l'involontaria acquisizione di informazioni personali da parte di terzi o di altri dipendenti: opportuni accorgimenti, ad esempio, devono essere presi in presenza di una particolare conformazione o dislocazione degli uffici, in assenza di misure idonee volte a prevenire la diffusione delle informazioni (si pensi al mancato rispetto di distanze di sicurezza o alla trattazione di informazioni riservate in spazi aperti, anziché all'interno di locali chiusi).

## 7.9 Esercizio dei diritti dell'interessato e riscontro

I lavoratori interessati possono esercitare nei confronti del datore di lavoro i diritti previsti dall'art. 7 del Codice (nei modi di cui agli artt. 8 e ss.), tra cui il diritto di accedere ai dati che li riguardano (anziché, in quanto tale, all'intera documentazione che li contiene), di ottenerne l'aggiornamento, la rettificazione, l'integrazione, la cancellazione, la trasformazione in forma anonima o il blocco se trattati in violazione di legge, di opporsi al trattamento per motivi legittimi.

La richiesta di accesso che non faccia riferimento ad un particolare trattamento o a specifici dati o categorie di dati, deve ritenersi riferita a tutti i dati personali che riguardano il lavoratore comunque trattati dall'amministrazione (art. 10) e può riguardare anche informazioni di tipo valutativo, alle condizioni e nei limiti di cui all'art. 8, comma 5.

Tra essi non rientrano notizie di carattere contrattuale o professionale che non hanno natura di dati personali in qualche modo riferibili a persone identificate o identificabili.

Il datore di lavoro destinatario della richiesta è tenuto a fornire un riscontro completo alla richiesta del lavoratore interessato, senza limitarsi alla sola elencazione delle tipologie di dati detenuti, ma comunicando in modo chiaro e intelligibile tutte le informazioni in suo possesso.

Il riscontro deve essere fornito nel termine di 15 giorni dal ricevimento dell'istanza dell'interessato (ritualmente presentata); il termine più lungo, pari a 30 giorni, può essere osservato, dandone comunicazione all'interessato, solo se le operazioni necessarie per un integrale riscontro sono di particolare complessità o se ricorre altro giustificato motivo (art. 146 del Codice).

Pertanto il datore di lavoro, specie nelle realtà produttive di grande dimensione, deve pertanto predisporre procedure organizzative adeguate per dare piena attuazione alle disposizioni del Codice in materia di accesso ai dati e all'esercizio degli altri diritti, anche attraverso l'impiego di appositi programmi finalizzati ad una accurata selezione dei dati relativi a singoli lavoratori, nonché alla semplificazione delle modalità e alla compressione dei tempi per il riscontro.

Il riscontro può essere fornito anche oralmente; tuttavia, in presenza di una specifica istanza, il datore di lavoro è tenuto a trasporre i dati su supporto cartaceo o informatico o a trasmetterli all'interessato per via telematica (art. 10).

Muovendo dalla previsione dell'art. 10, comma 1, del Codice, secondo cui il titolare deve predisporre accorgimenti idonei a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, può risultare legittima la richiesta dell'interessato di ricevere la comunicazione dei dati in questione presso la propria sede lavorativa o la propria abitazione.

### 7.9.1 Dati personali e documentazione

Come più volte dichiarato dal Garante, l'esercizio del diritto di accesso consente di ottenere, ai sensi dell'art. 10 del Codice, solo la comunicazione dei dati personali relativi al richiedente detenuti dal titolare del trattamento e da estrarre da atti e documenti; non permette invece di richiedere a quest'ultimo il diretto e illimitato accesso a documenti e ad intere tipologie di atti, o la creazione di documenti allo stato inesistenti negli archivi, o la loro innovativa aggregazione secondo specifiche modalità prospettate dall'interessato o, ancora, di ottenere, sempre e necessariamente, copia dei documenti detenuti, ovvero di pretendere particolari modalità di riscontro (salvo quanto previsto per la trasposizione dei dati su supporto cartaceo: cfr. art. 10, comma 2, del Codice).

Specie nei casi in cui è elevata la mole di informazioni personali detenute dal titolare del trattamento, il diritto di accesso ai dati può essere soddisfatto mettendo a disposizione dell'interessato il fascicolo personale, dal quale successivamente possono essere estratte le informazioni personali.

La scelta circa l'eventuale esibizione o consegna in copia di atti e documenti contenenti i dati personali richiesti può essere effettuata dal titolare del trattamento nel solo caso in cui l'extrapolazione dei dati personali da tali documenti risulti particolarmente difficoltosa per il titolare medesimo; devono essere poi omessi eventuali dati personali riferiti a terzi (art. 10, comma 4, del Codice). L'adozione di tale modalità di riscontro non comporta l'obbligo in capo al titolare di fornire copia di tutti i documenti che contengano i medesimi dati personali dell'interessato, quando gli stessi dati siano conservati in più atti, lettere o note.

Nel fornire riscontro ad una richiesta di accesso formulata ai sensi degli artt. 7 e 8 del Codice, il titolare del trattamento deve, poi, comunicare i dati richiesti ed effettivamente detenuti, e non è tenuto a ricercare o raccogliere altri dati che non siano nella propria disponibilità e non siano oggetto, in alcuna forma, di attuale trattamento da parte dello stesso (o perché originariamente trattati e non più disponibili, ovvero perché, come nel caso di dati contenuti nella corrispondenza intercorsa, in qualunque forma, tra dipendenti di un determinato datore di lavoro, non siano mai stati nell'effettiva e libera disponibilità di quest'ultimo (si pensi al caso di dati contenuti nella corrispondenza intercorsa tra dipendenti), al di là dei profili di tutela della segretezza della corrispondenza che pur vengono in rilievo, non competerebbero le decisioni in ordine alle loro finalità e modalità di trattamento (cfr. art. 4, comma 1, lett. f), del Codice).

Infine, il lavoratore può ottenere l'aggiornamento dei dati personali a sé riferiti. In ordine, poi, all'eventuale richiesta di rettifica dei dati personali indicati nel profilo professionale del lavoratore, la medesima può avvenire solo in presenza della prova dell'effettiva e legittima attribuibilità delle qualifiche rivendicate dall'interessato, ad esempio in base a decisioni o documenti del datore di lavoro o di terzi, obblighi derivanti dal contratto di lavoro, provvedimenti di organi giurisdizionali relativi all'interessato o altri titoli o atti che permettano di ritenere provata, agli effetti e sul piano dell'applicazione della (disciplina di protezione dei dati personali), la richiesta dell'interessato (che può comunque far valere in altra sede, sulla base di idoneo materiale probatorio, la propria pretesa al riconoscimento della qualifica o mansione rivendicata).

## Capitolo 8

# Regolamentazione del sito web

### 8.1 Partita iva obbligatoria su sito web

Il numero di partita Iva deve essere indicato nella pagina dell'eventuale sito web utilizzato, anche qualora attraverso di esso non venga esercitata attività di commercio elettronico e, dunque, anche se il sito venga utilizzato per finalità meramente pubblicitarie o propagandistiche.

L'Agenzia delle entrate, con risoluzione n. 60/E del 16 maggio 2006, ha in tal modo chiarito l'ambito di applicazione dell'articolo 35, comma 1, del Dpr n. 633 del 1972 in materia di dichiarazioni di inizio, variazione e cessazione attività ai fini Iva, disposizione integralmente modificata dall'articolo 2, comma 1, Dpr 5 ottobre 2001, n. 404, in vigore dal 1° dicembre 2001.

### 8.2 Informativa presente nella home-page del sito

L'informativa si ispira alla Raccomandazione n. 2/2001 che le autorità europee per la protezione dei dati personali, riunite nel Gruppo istituito dall'art. 29 della direttiva n. 95/46/CE adottata il 17 maggio 2001 per individuare alcuni requisiti minimi per la raccolta di dati personali on-line, e, in particolare, le modalità, i tempi e la natura delle informazioni che i titolari del trattamento devono fornire agli utenti quando questi si collegano a pagine web, indipendentemente dagli scopi del collegamento.

Di seguito sono descritte le nozioni da riportare all'interno dell'informativa.

#### 8.2.1 Titolare del trattamento

All'interno dell'informativa deve essere chiaramente indicato il titolare del trattamento dei dati del sito web. Infatti, a seguito della consultazione del sito esiste la possibilità di trattare dati relativi a persone identificate o identificabili.

#### 8.2.2 Luogo di trattamento dei dati

Indicare le sedi dove avvengono i trattamenti connessi ai servizi web del sito e dichiarare se il personale addetto autorizzato al trattamento è interno e/o esterno. Indicare se i dati vengono diffusi, modalità e finalità della diffusione.

#### 8.2.3 Tipi di dati trattati

##### Dati di navigazione

I sistemi informatici e le procedure software preposte al funzionamento dei siti web acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei



protocolli di comunicazione di Internet.

Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti.

In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente. Indicare la metodologia di gestione, conservazione e cancellazione di tali dati.

### **Contatti al sito web attraverso la posta elettronica**

L'invio facoltativo, esplicito e volontario di posta elettronica agli indirizzi indicati sul sito comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti nella missiva. Specificare nell'informativa finalità e modalità della gestione ed eventuale conservazione delle informazioni acquisite

### **Cookies**

Dare garanzie sul fatto che nessun dato personale degli utenti viene in proposito acquisito dal sito. Dichiarare inoltre che non viene fatto uso di cookies per la trasmissione di informazioni di carattere personale, né vengono utilizzati c.d. cookies persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti.

### **8.2.4 Facoltatività del conferimento dei dati**

A parte quanto specificato per i dati di navigazione, l'utente è libero di fornire i dati personali attraverso e-mail o form in quanto il loro mancato conferimento può comportare l'impossibilità di ottenere i servizi richiesti. Qualora venissero costruite attraverso le informazioni acquisite banche dati deve essere redatto un regolamento interno per la gestione delle banche dati e l'utente deve essere informato su un loro eventuale utilizzo per finalità commerciali e/o promozionali.

### **8.2.5 Modalità del trattamento**

Indicare la tipologia di strumenti automatizzati adottati per il trattamento, la conservazione e il salvataggio dei dati. Si dovranno inoltre dare adeguate garanzie sui metodi di raccolta, conservazione e protezione da eventuali intercettazioni delle informazioni acquisite.

### **8.2.6 Diritti degli interessati**

I soggetti cui si riferiscono i dati personali hanno il diritto in qualunque momento di ottenere la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento, oppure la rettificazione (art. 7 del d.lgs. n. 196/2003).

Ai sensi del medesimo articolo si ha il diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento. Indicare chiaramente sul sito web l'indirizzo a cui rivolgersi per richiedere la cancellazione dei dati acquisiti attraverso il sito web.

## 8.3 Consenso on-line

Per le modalità di raccolta on-line del consenso della clientela si ha la necessità che i sistemi informativi dei siti web vengano configurati in modo da consentire agli interessati di esplicitare pienamente il proprio diritto all'autodeterminazione informativa, prevedendo opzioni di tipo "positivo" (mediante l'inserimento di caselle di scelta, anziché di campi pre-selezionati su una tra le possibili scelte), così da permettere ad essi di esprimere liberamente le proprie scelte in ordine alle finalità legittimamente perseguibili da parte del titolare del trattamento.

Ad esempio è constatata la non conformità alle norme in materia di protezione dei dati della scelta di raccogliere in un unico contesto (condizioni generali di contratto), sia il consenso del cliente per accedere on-line ad alcuni servizi, sia il consenso per trattare i dati conferiti per la fruizione di quest'ultimi allo scopo di perseguire una finalità diversa, quale quella dell'invio di comunicazioni commerciali in forma elettronica intese a promuovere iniziative proprie o a veicolare iniziative promozionali nell'interesse di terzi. Un consenso manifestato nei termini appena descritti non può ritenersi valido, atteso che i clienti devono essere messi in condizione di esprimere consapevolmente e liberamente le proprie scelte in ordine al trattamento dei dati che li riguardano, manifestando il proprio consenso, quando questo è necessario, per ciascuna distinta finalità perseguita dal titolare.

Qualora ricorrano le condizioni di cui all'art. 130, comma 4, del Codice, norma in base alla quale il titolare del trattamento che utilizzi le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio ai fini di vendita diretta di propri prodotti o servizi (e sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato), può non richiedere il consenso qualora l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. Affinché in tale ipotesi il trattamento si configuri come legittimo, occorre quindi accordare al cliente la possibilità di opporsi in maniera agevole e gratuitamente all'utilizzo delle coordinate di posta elettronica per finalità di vendita diretta, sin dalla fase di raccolta dei dati, come pure in occasione dell'invio di ogni comunicazione successiva.

## Capitolo 9

# Norme per posta elettronica e internet

### 9.1 Sintesi

I datori di lavoro pubblici e privati non possono controllare la posta elettronica e la navigazione in Internet dei dipendenti, se non in casi eccezionali. Spetta al datore di lavoro definire le modalità d'uso di tali strumenti ma tenendo conto dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali.

Il Garante prescrive innanzitutto ai datori di lavoro di informare con chiarezza e in modo dettagliato i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica e sulla possibilità che vengano effettuati controlli. Il Garante vieta poi la lettura e la registrazione sistematica delle e-mail così come il monitoraggio sistematico delle pagine web visualizzate dal lavoratore, perché ciò realizzerebbe un controllo a distanza dell'attività lavorativa vietato dallo Statuto dei lavoratori. Viene inoltre indicata tutta una serie di misure tecnologiche e organizzative per prevenire la possibilità, prevista solo in casi limitatissimi, dell'analisi del contenuto della navigazione in Internet e dell'apertura di alcuni messaggi di posta elettronica contenenti dati necessari all'azienda.

Il provvedimento raccomanda l'adozione da parte delle aziende di un disciplinare interno, definito coinvolgendo anche le rappresentanze sindacali, nel quale siano chiaramente indicate le regole per l'uso di Internet e della posta elettronica.

Il datore di lavoro è inoltre chiamato ad adottare ogni misura in grado di prevenire il rischio di utilizzi impropri, così da ridurre controlli successivi sui lavoratori. Per quanto riguarda Internet è opportuno ad esempio:

- individuare preventivamente i siti considerati correlati o meno con la prestazione lavorativa;
- utilizzare filtri che prevenivano determinate operazioni, quali l'accesso a siti inseriti in una sorta di black list o il download di file musicali o multimediali.

Per quanto riguarda la posta elettronica, è opportuno che l'azienda:

- renda disponibili anche indirizzi condivisi tra più lavoratori (info@ente.it; urp@ente.it; ufficio-reclami@ente.it), rendendo così chiara la natura non privata della corrispondenza;
- valuti la possibilità di attribuire al lavoratore un altro indirizzo (oltre quello di lavoro), destinato ad un uso personale;
- preveda, in caso di assenza del lavoratore, messaggi di risposta automatica con le coordinate di altri lavoratori cui rivolgersi;
- metta in grado il dipendente di delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al titolare quelli ritenuti rilevanti per l'ufficio, ciò in caso di assenza prolungata o non prevista del lavoratore interessato e di improrogabili necessità legate all'attività lavorativa.

Qualora queste misure preventive non fossero sufficienti a evitare comportamenti anomali, gli eventuali controlli da parte del datore di lavoro devono essere effettuati con gradualità. In prima battuta si dovranno effettuare verifiche di reparto, di ufficio, di gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole. Solo successivamente, ripetendosi l'anomalia, si potrebbe passare a controlli su base individuale.

## 9.2 Premessa

Per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet, occorre muovere da alcune premesse:

1. compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
2. spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità (artt. 15, 31 ss., 167 e 169 del Codice);
3. emerge l'esigenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;
4. l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di log file di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;
5. le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

Le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, può essere tracciata a volte solo con difficoltà.

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.; cfr. altresì l'art. 2, comma 5, Codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato).

Non a caso, nell'organizzare l'attività lavorativa e gli strumenti utilizzati, diversi datori di lavoro hanno prefigurato modalità d'uso che, tenendo conto del crescente lavoro in rete e di nuove tariffe di traffico forfettarie, assegnano aree di lavoro riservate per appunti strettamente personali, ovvero consentono usi moderati di strumenti per finalità private.

## 9.3 Principi generali

Si tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (artt. 1 e 2 del Codice). Alcune disposizioni di settore, fatte

salve dal Codice, prevedono specifici divieti o limiti, come quelli posti dallo Statuto dei lavoratori sul controllo a distanza (artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n. 300). La disciplina di protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie.

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti principi:

- il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice; par. 5.2 );
- il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, comma 1, lett. a), del Codice). Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati (v. par. 3 );
- i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice: par. 4 e 5), osservando il principio di pertinenza e non eccedenza (par. 6). Il datore di lavoro deve trattare i dati nella misura meno invasiva possibile; le attività di monitoraggio devono essere svolte solo da soggetti preposti (par. 8) ed essere mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza

## 9.4 Correttezza nel trattamento

In base al richiamato principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore (art. 4, secondo comma, Statuto dei lavoratori; allegato VII, par. 3 d.lg. n. 626/1994 e successive integrazioni e modificazioni in materia di uso di attrezzature munite di videoterminali, il quale esclude la possibilità del controllo informatico all'insaputa dei lavoratori).

Grava quindi sul datore di lavoro o titolare del trattamento l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.

Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative.

### 9.4.1 Disciplinare

In questo quadro, può risultare opportuno adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico.

A seconda dei casi andrebbe ad esempio specificato:

- se determinati comportamenti non sono tollerati rispetto alla navigazione in Internet (ad es., il download di software o di file musicali), oppure alla tenuta di file nella rete interna;

- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di webmail, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- quali informazioni sono memorizzate temporaneamente (ad es., le componenti di file di log eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di back up, della gestione tecnica della rete o di file di log );
- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime, specifiche e non generiche, per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constatati che la posta elettronica e la rete Internet sono utilizzate indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;
- se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;
- quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi (art. 34 del Codice, nonché Allegato B), in particolare regole 4, 9, 10 ).

#### 9.4.2 Informativa (art. 13 del Codice)

All'onere del datore di lavoro di prefigurare e pubblicizzare una policy interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare comunque gli interessati ai sensi dell'art. 13 del Codice, anche unitamente agli elementi indicati ai punti 3.1. e 3.2.. Rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli.

Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, quando comportano un trattamento lecito di dati (art. 4, secondo comma, l. n. 300/1970 ); possono anche riguardare l'esercizio di un diritto in sede giudiziaria. Devono essere tra l'altro indicate le principali caratteristiche dei trattamenti, nonché il soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti.

## 9.5 Apparecchiature preordinate al controllo a distanza

Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice), il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 cod. civ. ). Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese

strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica. Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa. Ciò, anche quando i singoli lavoratori ne siano consapevoli.

In particolare non può ritenersi consentito il trattamento effettuato mediante sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire l'attività di lavoratori. È il caso, ad esempio:

- della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- della riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- dell'analisi occulta di computer portatili affidati in uso.

Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro. A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili (art. 11, comma 2, del Codice).

## 9.6 Programmi che consentono controlli indiretti

Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Ciò, anche in presenza di attività di controllo discontinue. Il trattamento di dati che ne consegue può risultare lecito. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

In applicazione del menzionato principio di necessità il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (da preferire rispetto all'adozione di misure repressive) e, comunque, a minimizzare l'uso di dati riferibili ai lavoratori (artt. 3, 11, comma 1, lett. d) e 22, commi 3 e 5, del Codice; aut. gen. al trattamento dei dati sensibili n. 1/2005, punto 4). Dal punto di vista organizzativo è quindi opportuno che:

- si valuti attentamente l'impatto sui diritti dei lavoratori (prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento);
- si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e l'accesso a Internet;
- si determini quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.

Il datore di lavoro ha inoltre l'onere di adottare tutte le misure tecnologiche volte a minimizzare l'uso di dati identificativi (c.d. Privacy Enhancing Technologies ovvero PET). Le misure possono essere differenziate a seconda della tecnologia impiegata (ad es., posta elettronica o navigazione in Internet).

## 9.7 Internet: la navigazione web

Il datore di lavoro, per ridurre il rischio di usi impropri della navigazione in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (art. 8 l. n. 300/1970; artt. 26 e 113 del Codice; Prov. 2 febbraio 2006, cit. ).

In particolare, il datore di lavoro può adottare una o più delle seguenti misure opportune, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva e dei diversi profili professionali:

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevenano determinate operazioni quali l'upload o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

## 9.8 Posta elettronica

Il contenuto dei messaggi di posta elettronica, come pure i dati esteriori delle comunicazioni e i file allegati, riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale). Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.

La mancata esplicitazione di una policy al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione. Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta in entrata) o di quelli inviati da quest'ultimo (posta in uscita).

È quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.

In questo quadro è opportuno che:



- il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@società.com, urp@ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it, rossi@società.com, mario.rossi@società.it);
- il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore;
- il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le coordinate (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. È parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta policy datoriale.

## 9.9 Controlli

Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali. Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria. In assenza di particolari esigenze tecniche o di sicurezza,

la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario a raggiungerla (v. art. 11, comma 1, lett. e), del Codice). Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali (tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nelle autorizzazioni generali nn. 1/2005 e 5/2005 adottate dal Garante) deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

## 9.10 Liceità del trattamento

I datori di lavoro privati e gli enti pubblici economici possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili:

- se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria (art. 24, comma 1, lett. f) del Codice);
- in caso di valida manifestazione di un libero consenso;
- anche in assenza del consenso, ma per effetto del presente provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul c.d. bilanciamento di interessi (art. 24, comma 1, lett. g), del Codice).

Per tale bilanciamento si è tenuto conto delle garanzie che lo Statuto prevede per il controllo indiretto a distanza presupponendo non il consenso degli interessati, ma un accordo con le rappresentanze sindacali (o, in difetto, l'autorizzazione di un organo periferico dell'amministrazione del lavoro).

L'eventuale trattamento di dati sensibili è consentito con il consenso degli interessati o, senza il consenso, nei casi previsti dal Codice (in particolare, esercizio di un diritto in sede giudiziaria, salvaguardia della vita o incolumità fisica; specifici obblighi di legge anche in caso di indagine giudiziaria: art. 26).

Per quanto riguarda i soggetti pubblici restano fermi i differenti presupposti previsti dal Codice a seconda della natura dei dati, sensibili o meno (artt. 18-22 e 112).

In tutti i casi predetti resta impregiudicata la facoltà del lavoratore di opporsi al trattamento per motivi legittimi (art. 7, comma 4, lett. a), del Codice).

## 9.11 Soggetti preposti

Nel caso di eventuali interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti. Resta fermo l'obbligo dei soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa. Resta parimenti ferma la necessità che, nell'individuare regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sia svolta un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

## 9.12 Misure da adottare e divieti

Le misure prescritte e da adottare da parte del titolare del trattamento sono:

1. la predisposizione di un'informativa per specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori, indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;
2. l'adozione e la pubblicizzazione di un disciplinare interno;
3. l'adozione di misure di tipo organizzativo affinché; si proceda ad un'attenta valutazione dell'impatto sui diritti dei lavoratori; si individuino preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet; si individuino quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi;
4. l'adozione di misure di tipo tecnologico, rispetto alla navigazione in Internet;
5. l'adozione di misure di tipo tecnologico, rispetto all'utilizzo della posta elettronica.

Vige inoltre il divieto per i datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. d), del Codice, di effettuare trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori, svolti in particolare mediante:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- l'analisi occulta di computer portatili affidati in uso;

Tuttavia si individuano, ai sensi dell'art. 24, comma 1, lett. g), del Codice, i casi nei quali il trattamento dei dati personali di natura non sensibile possono essere effettuati per perseguire un legittimo interesse del datore di lavoro anche senza il consenso degli interessati: esercizio di un diritto in sede giudiziaria, salvaguardia della vita o incolumità fisica; specifici obblighi di legge anche in caso di indagini giudiziarie.

## Capitolo 10

# Misure per l'utilizzo di *Smartphone* e *Tablet*

Con riferimento al documento (allegato di seguito) che il Garante ha elaborato in merito alle indicazioni per il corretto e consapevole trattamento dei dati personali con riferimento all'impiego di nuovi strumenti di comunicazione, come gli smartphone e i tablet, il Titolare del trattamento o il Responsabile della sicurezza del trattamento:

- censisce tali attrezzature all'interno dell'elenco della strumentazione elettronica, sul modello MOD\_ELAB) dell'Appendice A di codesto documento
- predispone le lettere di assegnazione di tali strumenti agli utilizzatori, sulla base del modello MOD\_TSP



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

Smartphone e tablet

# *Smartphone e tablet: scenari attuali e prospettive operative*

Schede di documentazione

*Smartphone e tablet:*  
scenari attuali e  
prospettive operative

# INDICE

|   |         |
|---|---------|
| <b><i>1. Il contesto delle mobile apps</i></b>                        | pag. 5  |
| <i>1.1. Smartphone e tablet</i>                                       | pag. 5  |
| <i>1.2. Le mobile apps e i market</i>                                 | pag. 6  |
| <i>1.3. Smartphone e sistemi tradizionali: cosa cambia</i>            | pag. 7  |
| <b><i>2. L'indagine conoscitiva</i></b>                               | pag. 9  |
| <i>2.1. L'attività istruttoria</i>                                    | pag. 9  |
| <i>2.2. Riscontri pervenuti</i>                                       | pag. 9  |
| <b><i>3. Aspetti critici legati all'utilizzo degli smartphone</i></b> | pag. 11 |
| <i>3.1. Rischi e minacce specifici</i>                                | pag. 13 |
| <b><i>4. Come aumentare le garanzie per gli utenti</i></b>            | pag. 15 |

## 1. IL CONTESTO DELLE MOBILE APPS

### 1.1. Smartphone e tablet

Uno *smartphone* (o cellulare intelligente o telefono *touch*, cioè sensibile al tocco) è un dispositivo portatile, alimentato a batteria, che coniuga le funzionalità di telefono cellulare con quelle di elaborazione e trasmissione dati tipiche del mondo dei personal computer; esso, inoltre, impiega sensori per la determinazione della posizione (GPS) e per l'acquisizione di altri elementi dell'ambiente circostante l'utente. Le componenti *hardware* generalmente presenti in dispositivi di questo tipo sono riassunte in *Tabella 1*, le caratteristiche funzionali e la tipologia di destinazione d'uso sono rappresentate in *Tabella 2*:

| Componenti trasmissive             | Sensori e dispositivi                              |
|------------------------------------|--|
| Modulo telefonico                  | Schermo <i>touch</i> inferiore ai 5" <sup>33</sup> |
| <i>Wifi</i> (rete senza fili)      | Altoparlante e microfono integrati                 |
| <i>Bluetooth</i> (rete senza fili) | Fotocamera/videocamera digitale                    |
| Radio FM                           | Dispositivo di localizzazione (GPS)                |
|                                    | Bussola digitale e altri sensori                   |
|                                    | Moduli di pagamento                                |

*Tabella 1. Smartphone: caratteristiche + hardware di massima*

| Nuove caratteristiche   |
|---|
| Applicazioni con funzionalità di localizzazione   |
| Riconoscimento vocale, facciale e di immagini   |
| <i>Social network</i> con possibilità di rendere nota la posizione geografica degli utenti  |
| L'utente generalmente acquisisce applicazioni utilizzando lo specifico <i>market</i> dedicato ( <i>OviStore</i> per <i>Nokia</i> , <i>Apple Store</i> per <i>Apple</i> , <i>Android Market</i> per <i>Google</i> , <i>Windows Market Place</i> per <i>Microsoft</i> ) |
| Possibilità di confusione tra dati di origine diversa (es. quelli contenuti nella rubrica per uso personale e quelli relativi ai contatti di lavoro.)   |

*Tabella 2. Smartphone: applicazioni innovative e nuove funzionalità delle applicazioni tradizionali*



I *tablet* o *tablet computer* sono dispositivi assimilabili per componenti *hardware* e *software* agli *smartphone*, dai quali si distinguono per:

- dimensioni dello schermo
- possibile assenza del modulo telefonico
- destinazione d'uso

Gli *smartphone* e i *tablet computer* per lo più condividono la stessa infrastruttura tecnologica ovvero le stesse componenti *hardware* e lo stesso sistema operativo. I *tablet* sono però caratterizzati da uno schermo di dimensioni maggiori, il che li rende più idonei al consumo di prodotti multimediali ed editoriali (es. *gaming on-line*, *film on-demand*, abbonamenti a riviste e quotidiani) e meno pratici per essere utilizzati come telefoni e come PIM (*Personal Information Management*); per questa ragione alcuni esemplari non sono dotati di modulo telefonico. La maggior parte dei modelli si avvale, tuttavia, di schede SIM per la connessione dati con le tecnologie cellulari (GPRS e UMTS).

È opportuno osservare che, per le finalità connesse alle problematiche relative alla protezione dei dati personali, sia i dispositivi *tablet* che *smartphone* possono essere considerati unitariamente, dal momento che le modalità di funzionamento delle applicazioni sono pressoché identiche. Va altresì evidenziato che non costituisce oggetto di indagine l'impiego di questi dispositivi come apparecchi telefonici per le comunicazioni interpersonali.

### *1.2. Le mobile apps e i market*

Per *mobile apps* o applicazioni per *smartphone* si intende il *software* che è possibile installare sugli *smartphone* e sui *tablet* per fornire funzionalità aggiuntive. Le applicazioni per *smartphone* estendono, cioè, le funzionalità rese disponibili dal sistema operativo dello specifico produttore e sono reperibili tramite *download* da una speciale applicazione che acquisisce il marchio (*brand*) del produttore del telefono o del sistema operativo installato sul telefono. Tale particolare applicazione viene

detta *market* ed è denominata diversamente dai vari produttori. I principali *market* attualmente sono:

- *Android Market* (*Google*)
- *Apple Store* (*Apple*)
- *Windows MarketPlace* (*Microsoft*)
- *Nokia OviStore* (*Nokia*)

Tutti i *market* sono una speciale applicazione per *smartphone* che visualizza una vetrina virtuale dalla quale è possibile acquisire ulteriori applicazioni.

### 1.3. *Smartphone e sistemi tradizionali: cosa cambia*

*Tablet* e *smartphone* si differenziano dai *netbook* e dai *notebook* più tradizionali non soltanto per la specificità dell'*hardware* e del *software* di base, ma anche e soprattutto per i meccanismi e le modalità di acquisizione e distribuzione del *software* (*software acquisition & distribution*), che sono centralizzati e normalmente controllati dal fornitore del dispositivo, dall'operatore telefonico, dal produttore del sistema operativo o, infine, dal "gestore del market" che opera da intermediario tra il produttore/sviluppatore dei software e dei servizi (nella maggior parte dei casi esterno alla società e, dunque, terzo rispetto ad essa) e l'utente finale. Infatti, con specifico riguardo a *smartphone* e *tablet*, l'utente acquista *software* aggiuntivi (es. un videogame) e servizi (es. un cruscotto dell'andamento titoli, un servizio di condizioni meteo, un film in *streaming*, un *videogame* in *multiplayer*) avvalendosi di un'applicazione fornita dal gestore denominata *market* e preinstallata sul dispositivo.

Come sopra accennato, si tratta di una sorta di vetrina dei *software* e dei servizi disponibili resa accessibile all'utente per ampliare le funzionalità *software* del proprio *smartphone*. Il relativo utilizzo richiede la preventiva registrazione dell'utente e l'accettazione, da parte di quest'ultimo, delle condizioni contrattuali prefissate dal gestore del *market*, cristallizzate in un documento denominato *terms of service* (*ToS*).

In linea di massima non è possibile acquisire un'applicazione tramite canali tradizionali (es. CD acquistato in negozio), né avvalersi di modalità alternative a quelle

rigidamente previste dal gestore dello specifico *market* di riferimento, che va considerato lo strumento privilegiato e più diffuso per la distribuzione e l'acquisizione delle applicazioni per *smartphone*. L'eventuale installazione di applicazioni al di fuori del *market* è da ritenersi, dunque, una possibilità residuale.

Parallelamente, anche uno sviluppatore terzo che intenda creare un'applicazione in ambito *mobile* sarà tenuto ad accettare i *ToS* definiti dal detentore della piattaforma da lui scelta, ovvero dal gestore del *market*, e potrà vendere il suo prodotto solo attraverso il canale previsto da quest'ultimo.

Va sottolineato che il panorama delle *mobile apps* è molto vivace e in rapida evoluzione, anche in considerazione del fatto che le tecnologie alla base delle *mobile apps* (quali l'introduzione dei citati sensori sugli *smartphone*, la nuova modalità *touch* di interfacciamento con lo strumento), la facilità di accesso e di utilizzo di questi dispositivi e le innovative modalità di distribuzione dei relativi servizi hanno aperto la via a nuove, concrete opportunità di *business*, all'implementazione tecnologica ed alla diffusione di servizi ed applicazioni del tutto impensabili solo fino a qualche tempo fa. Attualmente esistono numerosissimi sviluppatori in ogni parte del mondo, caratterizzati da dimensioni imprenditoriali anche molto limitate, a volte semplici appassionati individuali senza particolari ambizioni commerciali, i quali con bassissimi investimenti e puntando su un'idea o un'intuizione creano e, attraverso la vetrina resa disponibile dal gestore (il *market*), mettono a disposizione di un mercato potenzialmente mondiale soluzioni talvolta molto innovative, in genere dal costo anche molto contenuto, che l'utente può acquistare in tutta semplicità, autonomia ed immediatezza. È tuttavia presumibile che questa dimensione artigianale con il tempo tenderà ad evolversi, convergendo verso una contrazione del numero degli sviluppatori che assumeranno connotazioni di maggior strutturazione e di più ampie dimensioni: è, infatti, verosimile che le aspettative dei consumatori siano destinate a crescere, con l'effetto che i prodotti, per essere competitivi, dovranno essere progressivamente più complessi e diversificati, con conseguente aumento dei costi di ideazione e sviluppo.

## 2. L'INDAGINE CONOSCITIVA

### 2.1. L'attività istruttoria

Agli inizi del 2011 l'Autorità ha avviato un'indagine che ha avuto come interlocutori privilegiati i principali produttori di sistemi operativi per *smartphone* (nello specifico, *Nokia*, *Microsoft*, *Apple*, *Google*), al fine di verificare gli accorgimenti adottati da queste società per garantire la sicurezza nell'utilizzo delle *mobile apps* sviluppate per i loro sistemi.

In particolare, le società sono state invitate ad indicare:

1. i meccanismi adottati o i requisiti richiesti (in termini, ad esempio, di affidabilità o di adeguato rispetto di misure di sicurezza) per selezionare preventivamente gli sviluppatori terzi (quelli, cioè, non direttamente dipendenti dalla società) autorizzati a distribuire le *application* di propria creazione sulle piattaforme di *market* di quest'ultima e quali condizioni e procedure siano previste per un'eventuale revoca dell'autorizzazione;

2. i meccanismi adottati per valutare le diverse funzionalità delle *application* e per verificare se la raccolta di dati personali effettuata dallo sviluppatore, per il tramite dell'applicazione, sia effettivamente pertinente rispetto alle predette funzionalità e alle finalità della raccolta;

3. le *policies* interne per assicurare il rispetto della normativa in materia di protezione dei dati personali e quali meccanismi siano adottati per verificare la conformità delle *application* già distribuite alla predetta normativa, nel caso in cui pervengano segnalazioni da parte degli utenti.

### 2.2. Riscontri pervenuti

Le risposte rese dai soggetti interpellati hanno evidenziato l'adozione di politiche aziendali solo in parte comuni.

In tutti e quattro i casi oggetto di indagine, ad esempio, lo sviluppatore terzo può proporre le applicazioni di propria creazione per la distribuzione sulla piattaforma di *market* dell'intermediario prescelto soltanto a seguito del perfezionamento di una

procedura di registrazione ed all'accettazione di specifici accordi contrattuali predisposti, proprio, da quest'ultimo; ne consegue una marcata eterogeneità delle clausole contrattuali cui gli sviluppatori sono vincolati, a seconda che decidano di proporre le proprie creazioni all'una o all'altra delle quattro diverse società.

Le indicazioni fornite, segnate naturalmente dal carattere della confidenzialità, hanno evidenziato differenze più o meno sensibili anche in ordine alle attività di controllo, alle assunzioni di responsabilità, ai rimedi esperibili in caso di inconvenienti, sia di carattere tecnico, nel funzionamento dell'applicazione, sia di carattere giuridico e dunque maggiormente attinenti agli aspetti contrattuali.

Ulteriori diversità sono state osservate anche con specifico riguardo al profilo che più direttamente interessa questa Autorità, quello cioè della protezione dei dati personali degli utenti. In quest'ambito è stato possibile, tuttavia, identificare due diversi e contrapposti modelli di condotta, che si distinguono per il modo in cui viene garantita la sicurezza delle applicazioni messe in vendita tramite il *market* e possono essere definiti nel modo seguente:

- *privacy by process*
- *privacy by platform*

Nel modello *privacy by process*, il processo di accreditamento dei potenziali sviluppatori e di inserimento delle loro applicazioni nel *market* viene sottoposto ad un rigido controllo, tipicamente formalizzato in un accordo *ToS* (*Terms of Service* - condizioni di contratto) tra il soggetto interessato a pubblicare il suo *software* sul *market* e il gestore del *market* stesso. Inoltre, l'applicazione viene controllata allo scopo di garantirne la sicurezza sotto il profilo tecnico prima dell'immissione nel mercato.

Nel modello *privacy by platform* il gestore del *market* non effettua un controllo preventivo sull'applicazione, ma affida la tutela dei diritti dell'utente alla solidità della piattaforma di sistema operativo, alle sue funzionalità che permettono all'utente di avere coscienza di quali dati saranno oggetto di trattamento da parte dell'applicazione disponibile sul *market*, facendo ricorso a meccanismi di *ranking* gestiti dagli

stessi utenti. In termini più concreti, chi utilizza il *market* può verificare per ogni applicazione disponibile le opinioni di coloro che prima di lui ne hanno già fatto uso, espresse sotto forma di punteggi sintetici e commenti. Inoltre, all'atto dell'installazione di un'applicazione la piattaforma *software* presente sul suo *smartphone* provvede ad informare l'utente su quali funzionalità l'applicazione utilizzerà e quindi a quali dati può potenzialmente accedere.

### 3. ASPETTI CRITICI LEGATI ALL'UTILIZZO DEGLI *SMARTPHONE*

La diffusione dei moderni *smartphone* determina una crescita sostenuta nell'utilizzo delle applicazioni per questo tipo di dispositivi: i principali *market* hanno ormai un *portfolio* che può superare le decine di migliaia di *apps*.

Gli utenti tendono a delegare la gestione di molti aspetti della propria vita sia personale che professionale alle nuove tecnologie, le quali fanno sempre più spesso impiego di informazioni relative alla geolocalizzazione degli interessati. Questi dati non sempre restano archiviati esclusivamente sul dispositivo, ma vengono frequentemente conservati in aree remote potenzialmente accessibili anche da altri utenti. Uno stesso *smartphone* può essere utilizzato per le finalità più disparate, ad esempio per la gestione del *portfolio* clienti, del catalogo e del calendario aziendali, ma anche per la condivisione di foto, informazioni, video etc. con i propri amici o familiari, per il confronto dei prezzi dei prodotti al supermercato con quelli del negozio *on-line*, per monitorare i propri movimenti bancari, per localizzare la propria autovettura in caso si dimentichi dove è stata posteggiata, per sapere, in quel determinato momento, chi dei propri amici si trovi in zona, per redigere programmi di benessere alla stregua delle proprie abitudini alimentari, per impostare il monitoraggio ormonale del ciclo femminile, e magari, in una prospettiva di prossima, futura realizzazione, persino come telecomando per aprire il cancello automatico del proprio box

auto o per sbloccare la serratura della propria abitazione. Il ventaglio delle applicazioni possibili è, allora, realmente impressionante e destinato ad accrescersi ulteriormente. Tuttavia, l'utilizzo di tali applicazioni implica l'elaborazione e quindi il trattamento di dati, anche personali, riservati e persino sensibili. In molti casi i dati verranno archiviati e conservati sul dispositivo, ma sempre più spesso ci si avvale di *mobile apps* che consistono in realtà in servizi erogati in modalità *web*, il cui utilizzo implica, cioè, che le informazioni personali siano spostate o copiate nella *cloud* del fornitore del servizio. Il fornitore, ovvero lo sviluppatore delle *mobile apps*, può essere lo stesso gestore del *market* o uno sviluppatore indipendente. In altri termini, molte delle applicazioni per *smartphone* sono servizi erogati in modalità *cloud* (“*SaaS*” - *Software as a service*) che trasportano tutti o parte dei dati dell'utente nella *cloud*.

La transizione dal modello applicativo tradizionale a quello in cui il *software* è un servizio della *cloud* è condivisa sia dal fornitore sia dal consumatore, in quanto la modalità *cloud* costituisce apparentemente un'esclusiva facilitazione per l'utente. In realtà questi non è, spesso, neppure consapevole del fatto che sta utilizzando un servizio *cloud*; è, tuttavia, perfettamente al corrente della possibilità di accedere agli stessi dati da dispositivi differenti (*es. smartphone* e *pc* da scrivania) ovvero che se acquista uno *smartphone* nuovo può ritrovare, “*come per magia*”, tutti i propri dati sul nuovo dispositivo senza dover ricorrere a tediose transizioni dal vecchio al nuovo telefonino (si pensi allo spostamento dei contatti della rubrica).

Un ulteriore aspetto che viene proposto e percepito come facilitazione a valore aggiunto è l'integrazione di *set* di dati che hanno origini differenti. Ad esempio con i telefoni basati sul *software* di *Google* (*Android*) è possibile trasferire nella rubrica dello *smartphone* i contatti, compresi quelli di posta elettronica, prelevati dall'*account* *Google*. Inoltre alcuni produttori di telefoni danno la possibilità all'utente di integrare tale rubrica con ulteriori dati prelevati dal proprio *account Facebook*, aggiungendo ad esempio le foto e gli indirizzi di residenza.

Questi, in sintesi, gli aspetti critici di carattere generale in merito all'utilizzo della nuova generazione dei dispositivi *smartphone*:

- sono dispositivi pervasivi, utilizzabili in tutti gli aspetti della vita personale e professionale;
- è presumibile che vi si farà sempre più frequentemente ricorso per gestire anche dati "riservati";
- le facilitazioni d'uso favoriscono l'esternalizzazione dei dati;
- le facilitazioni d'uso favoriscono l'integrazione di dati tra aspetti distinti della propria vita (es. rubrica lavorativa e amici su *Facebook*).

### 3.1. *Rischi e minacce specifici*

Le precedenti osservazioni consentono, allora, di definire, elencandoli, i principali fattori connessi all'utilizzo dei sistemi *mobile* idonei a determinare rischi e minacce specifici per la protezione dei dati personali degli utenti. Segnatamente:

- la linea di demarcazione che permette di distinguere l'*Identità digitale* dall'*Identità reale* tende progressivamente ad affievolirsi sino a scomparire. L'utilizzatore di *applications* per *smartphone* è, infatti, identificabile abbastanza facilmente attraverso informazioni obiettive e concrete, non autonomamente modificabili (ad esempio il numero di telefonino, il codice IMEI, i dati anagrafici dei contatti registrati nella rubrica archiviata sul proprio dispositivo etc.);
- il *social networking* tende ad essere sempre più pervasivo e si integra e arricchisce con nuove informazioni personali (ad esempio la posizione geografica dell'utente);
- in generale, a causa dell'integrazione dei servizi informatici e dello scambio di dati tra applicazioni, telefono e servizi, è sempre più difficile - e spesso impossibile - controllare il flusso dei propri dati personali;
- a causa della progressiva diminuzione del controllo sui propri dati e della correlata fusione tra l'identità digitale e quella reale, emergono maggiori pericoli dal punto di vista della sicurezza informatica e si creano nuovi rischi e minacce



(es. *stalking* sociale, intercettazioni, furto di *account* di pagamento);

- possibilità di accedere da parte delle applicazioni a dati e strumenti in un modo ancor più invasivo che in passato (numero di telefono, rubrica, messaggi);
- possibilità da parte delle applicazioni di intrecciare aspetti differenti della vita degli utenti (es. vita privata e vita professionale) in modi non sempre chiari, conoscibili, prevedibili, controllabili e desiderati da parte dell'utente stesso;
- tracciamento e profilazione dell'utente a sua insaputa e disponibilità di dati univoci (IMEI, numero di telefono) da utilizzare ad esempio per la pubblicità comportamentale, per l'enforcement di un accordo di servizio o per la tutela del diritto d'autore;
- alcuni produttori, per ragioni di mercato, tendono a non distribuire tempestivamente gli aggiornamenti *software* che risolvono accertate vulnerabilità di sicurezza informatica.

In un tentativo di ulteriore schematizzazione, i rischi e le minacce in cui un utente può incorrere per un uso non accorto o non regolamentato delle *mobile apps* derivano da:

- mancanza di TRASPARENZA nelle modalità e nelle finalità di raccolta dei dati;
- incapacità o impossibilità da parte degli interessati di esercitare o recuperare il CONTROLLO sui propri dati e sul modo in cui essi vengono comunicati a terzi;
- elementi tecnici di SICUREZZA INFORMATICA

|             |           |                       |
|-------------|-----------|-----------------------|
| Trasparenza | Controllo | Sicurezza informatica |
|-------------|-----------|-----------------------|

*Tabella 3: Le tre dimensioni della protezione dei dati personali nelle apps*

#### 4. COME AUMENTARE LE GARANZIE PER GLI UTENTI

In questa sede si intendono formulare proposte di carattere operativo tese a favorire sia l'utilizzo consapevole, da parte dell'utente, degli strumenti e dei dispositivi dei quali si tratta, sia un più efficace esercizio dei propri diritti in merito alla gestione dei dati personali.

È opportuno muovere da una duplice considerazione:

- i produttori di dispositivi e dei relativi *software*, così come gli operatori di telefonia che commercializzano tali dispositivi previa apposizione del proprio marchio (*brand*), rivestono un ruolo importante sul livello di sicurezza dei dispositivi *mobile* che distribuiscono; coerentemente, sono loro i soggetti deputati a garantire anche la messa a disposizione di aggiornamenti tempestivi qualora siano rilevate nuove minacce per la sicurezza informatica. A questo riguardo, giova specificare che le caratteristiche del sistema operativo associato ad uno specifico dispositivo mutano a seconda che l'operatore di telefonia vi abbia apposto il proprio *brand* oppure no e sono, dunque, soggette ad una sorta di "personalizzazione" legata, proprio, al *brand*. In termini più concreti, la configurazione del *software* di un dispositivo destinato ad essere commercializzato previa apposizione di un marchio (per esempio *Telecom Italia*, *Vodafone*, *Wind*, *H3G* etc.) è almeno in parte determinata dall'operatore di telefonia stesso, con l'obiettivo di renderne l'utilizzo il più possibile idoneo alla fruizione dei servizi che esso stesso mette a disposizione dei propri clienti. Ne consegue che due telefonini originariamente ed apparentemente identici, poiché dello stesso modello e della stessa marca, potranno in realtà differenziarsi in maniera anche significativa sotto il profilo delle caratteristiche del *software* a seconda del gestore che ne curi la personalizzazione e vi apponga il proprio *brand*. In questa ipotesi, le mutate caratteristiche del *software* di un dispositivo cui sia stato apposto il marchio dell'operatore di telefonia potrebbero, in alcuni casi, influire sul processo di aggiornamento del *software* reso disponibile dal produttore del telefonino (ad

esempio *Nokia, Sony Ericsson, Samsung, LG* etc.), rendendolo non direttamente ed immediatamente fruibile;

- nel caso delle *mobile apps*, a differenza del tradizionale modello di acquisizione del *software* su PC, c'è generalmente - lo si ribadisce - un intermediario univoco che si frappone tra lo sviluppatore / fornitore del servizio e l'utente finale; in altri termini, l'indeterminata molteplicità degli sviluppatori da un lato e l'altrettanto enorme massa degli utenti dall'altro trovano il loro punto di contatto e di raccordo proprio per il tramite di pochi soggetti, appunto gli intermediari, sulle cui attività imprenditoriali e commerciali si concentra il funzionamento del peculiare mercato di riferimento.

Il panorama prevalente consente, allora, di ipotizzare interventi mirati che, sfruttando la posizione di centralità degli intermediari all'interno della richiamata dialettica contrattuale e di *business*, possano efficacemente raggiungere la maggior parte dei soggetti coinvolti, con il dichiarato intento di porre le basi di una disciplina chiara ed efficace di tutela degli utenti in materia di protezione dei dati personali che non costituisca, tuttavia, un limite né dal punto di vista della logica concorrenziale propria del mercato né tantomeno abbia l'effetto di imbrigliare le potenzialità creative degli sviluppatori delle più moderne tecnologie.

In questa prospettiva, giova sottolineare che proprio all'intermediario, cioè al gestore del *market* che è spesso anche il produttore del sistema operativo dello *smartphone*, compete sempre un potere definitivo segnato dal massimo carattere della deterrenza, e cioè quello di interdizione nei confronti del *software* prodotto da terze parti con le quali sussista un vincolo di carattere contrattuale.

Una prima conclusione: è indispensabile, perché gli utenti siano posti nella condizione di decidere con responsabilità in ordine all'utilizzo dei propri dati, agire in modo da accrescerne la consapevolezza sulle opportunità, ma anche sui potenziali rischi riconducibili al mondo degli *smartphone* e delle *mobile apps*.

È altrettanto fondamentale che gli utenti, dopo aver conferito e, in senso lato, affidato i propri dati, ne mantengano comunque il controllo.

Ed è proprio da queste considerazioni ed in questa direzione che l'Autorità intende muovere per affrontare la sfida offerta dal sempre più diffuso impiego di applicazioni per *smartphone*, adoperandosi concretamente - se del caso, anche mediante mirate campagne informative - per diffondere tra gli utenti una nuova cultura che tenga conto, oltre che delle affascinanti ed innovative possibilità rese accessibili dalle nuove tecnologie, anche di alcuni punti di particolare rilievo e delicatezza. Tra questi:

- il rischio cagionato dalla carenza di consapevolezza dell'utente in ordine a profili di assoluta rilevanza che lo riguardano in maniera diretta e possiedono potenziali attitudini lesive dei suoi diritti in materia di protezione dei dati personali;
- le specificità legate all'utilizzo di applicazioni, specie quelle ad opera di sviluppatori terzi, che raccolgono dati sulla vita privata (dai contatti alla posizione geografica, sino alle abitudini di consumi e comportamenti, a dati relativi alla salute ed alla vita di relazione);
- la possibilità che i soggetti che trattano le informazioni personali degli utenti, anche eventualmente di carattere sensibile, possano renderle "pubbliche" ovvero comunicarle ad altri soggetti determinati, sia per finalità commerciali che di altro genere, non specificamente correlate alla raccolta e, più in generale, non conformi ai desideri dell'utente medesimo, innanzitutto per l'indubbia attitudine dei dati a favorire attività di profilazione dell'utente;
- la possibilità che, in assenza di regole specifiche, i dati così raccolti possano essere archiviati sui sistemi del fornitore del servizio applicativo per periodi di tempo ultronei rispetto alla fornitura del servizio stesso, potenzialmente indeterminati; che, addirittura, possano continuare a costituire oggetto di trattamento perfino successivamente al momento in cui l'utente ha cessato di far ricorso ad una determinata applicazione ovvero di utilizzare uno specifico dispositivo.

Il duplice obiettivo di implementare sia la trasparenza nelle modalità di funzionamento delle applicazioni, con specifico riguardo al trattamento delle informazioni personali degli utenti, sia il controllo esercitabile, nonchè la dimensione

sovranazionale dei produttori e, in termini ancor più generali, il respiro globale del mercato delle *mobile apps*, suggeriscono di pensare alla possibile trasposizione degli interventi in un contesto più ampio di quello nazionale. Si potrebbe, cioè, ipotizzare un'azione sinergica con interlocutori, anche istituzionali, che operino in ambito comunitario.

Una prospettiva, questa, concretamente realizzabile, specie se si valuta lo specifico ruolo di mediazione assunto dai citati produttori di sistemi operativi che, essendo anche i gestori dei *market* ovvero dei cataloghi di applicazioni, hanno tra l'altro una capacità di interdizione nei confronti degli sviluppatori eventualmente inadempienti alle prescrizioni previste dalle disposizioni contrattuali (*Terms of Service*).

In tale quadro, più pregnanti garanzie per l'utente potranno essere ottenute attraverso una combinazione di accorgimenti tecnici - sufficientemente generali da non modificare le strategie di mercato ma comunque ragionevolmente efficaci - e di norme contrattualistiche da inserire negli accordi proposti dai gestori dei *market* e rivolti sia agli sviluppatori delle applicazioni che agli utenti finali.

Il futuro, insomma, è già incominciato.

# Appendice A

## Elenchi

Seguono gli elenchi per

- Responsabili, Incaricati e Addetti (organigramma);
- Locali;
- Trattamenti;

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Titolare del trattamento**

siccome l'attività compete a persona giuridica, il Titolare del trattamento è l'entità nel suo complesso nella persona di:  
D'ACRI ANTONIO MARCO

**Responsabile della sicurezza  
dei dati personali**

LEON FRANCESCA

**Addetti al controllo dei locali**

ARUGA MARCO  
BARAVELLI CRISTINA  
BERTERO LUCA  
BORGARO CHIARA  
CAGNASSO MAGDA  
COCCIARDI STEFANO  
CORREALE AMALIA  
D'ACRI ANTONIO MARCO  
EYNARD SIMONE FLAVIO  
IACOBONE PASQUALE  
LEON FRANCESCA  
MAUTINO ROBERTO  
PEPE ANNARITA  
PINTOR RENATA  
RICCI SIMONA  
SERRA ELEONORA  
VITRANI PAOLO

**Incaricati del trattamento**

ARUGA MARCO  
BARAVELLI CRISTINA  
BERTERO LUCA  
BORGARO CHIARA  
BRACCIALARGHE MAURIZIO

(continua...)

**Incaricati del trattamento (...segue)**

CAGNASSO MAGDA  
COCCIARDI STEFANO  
COPPOLA MICHELE  
CORREALE AMALIA  
D'ACRI ANTONIO MARCO  
EYNARD SIMONE FLAVIO  
IACOBONE PASQUALE  
LEON FRANCESCA  
MAUTINO ROBERTO  
PEPE ANNARITA  
PINTOR RENATA  
RICCI SIMONA  
RINALDI VALERIA (legge 104)  
SERRA ELEONORA  
VITRANI PAOLO

**Responsabili esterni del trattamento**

BIPOINT  
CITTA' DI TORINO  
COMITATO ESECUTIVO  
CRITICAL CASE  
CSI PIEMONTE  
DOTT. FRANZO ANGELO  
DOTT. MARCO ALBERTO MALAGNINO  
EVOLUTIVA  
FORE  
GLS  
KOINE' SISTEMI  
LOTTOMATICA  
PLUSERVICE  
REALE MUTUA  
SEGRE MASSIMO  
SPAZIOTTANTOTTO SRL  
STUDIO CODA  
STUDIO COMOLLO  
STUDIO NOTARILE GANELLI MAROCCO  
STUDIO TOSETTO WEIGMANN

(continua...)



**Responsabili esterni del trattamento**  
(...segue)**Responsabili della gestione e della manutenzione degli strumenti elettronici**EYNARD SIMONE FLAVIO  
KOINE' SISTEMI  
MAUTINO ROBERTO**Amministratori di sistema**

KOINE' SISTEMI

**Incaricato della custodia delle copie delle credenziali di autenticazione**

LEON FRANCESCA

**Incaricato delle copie di sicurezza delle banche dati elettroniche**KOINE' SISTEMI  
MAUTINO ROBERTO  
ROBERTO MAUTINO**Responsabile dei processi formativi in materia di protezione dei dati**

LEON FRANCESCA di COADIUVATA DA ING. MARTINI FABRIZIO

Addetti non direttamente coinvolti nel trattamento dei dati che, tuttavia, operano a contatto con strumenti o supporti contenenti dati:

**Addetti alla manutenzione o sostituzione del hardware degli elaboratori** - KOINE' SISTEMI

Autonomi titolari del trattamento che forniscono determinati servizi e/o prodotti coinvolti nel trattamento dei dati che, tuttavia, operano autonomamente senza nessun rapporto di responsabilità nei confronti del titolare del trattamento

**Autonomi titolari del trattamento**BANCA SELLA  
LEGAL MAIL  
UNICREDIT BANCA

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

Segue l'elenco delle sedi e dei locali sotto la diretta responsabilità del titolare del trattamento.

|                  |   |
|------------------|---|
| <b>Sede</b>      | C/O PALAZZO DELLA REGIONE                                 |
| <b>Indirizzo</b> | VIA GARIBALDI ANG. PIAZZA CASTELLO<br>10122 - TORINO (TO) |

Descrizione dei locali:

|  |   |
|--|---|
| C/O INFOPIEMONTE<br>- FRONT OFFICE -<br>AREA OPERATIVA | <p>Accesso pubblico, controllato<br/>Il locale è dotato di sistema antifurto<br/>Il locale è provvisto di porte, armadi e/o cassette con serratura<br/>Il locale contiene dati personali, sensibili<br/>Il locale contiene 5 elaboratori informatici<br/>Gli addetti al controllo del locale sono BARAVELLI CRISTINA, BERTERO LUCA,<br/>BORGARO CHIARA, COCCIARDI STEFANO, EYNARD SIMONE FLAVIO,<br/>IACOBONE PASQUALE, VITRANI PAOLO</p> |
|--|---|

|                  |  |
|------------------|--|
| <b>Sede</b>      | MAGAZZINO / ARCHIVIO                             |
| <b>Indirizzo</b> | VIA BUTTIGLIERA 6<br>10100 - RIVA DI CHIERI (TO) |

Descrizione dei locali:

|                    |  |
|--------------------|--|
| MAGAZZINO/ARCHIVIO | <p>Accesso controllato<br/>Il locale è dotato di sistema antifurto<br/>Il locale è provvisto di porte, armadi e/o cassette con serratura<br/>Il locale contiene dati personali, sensibili<br/>Gli addetti al controllo del locale sono MAUTINO ROBERTO, PEPE ANNARITA,<br/>PINTOR RENATA, SERRA ELEONORA</p> |
|--------------------|--|

|                  |   |
|------------------|---|
| <b>Sede</b>      | SEDE LEGALE C/O COMUNE PALAZZO CIVICO             |
| <b>Indirizzo</b> | PIAZZA PALAZZO DI CITTA' 1<br>10122 - TORINO (TO) |

|                  |  |
|------------------|--|
| <b>Sede</b>      | SEDE OPERATIVA                         |
| <b>Indirizzo</b> | VIA ASSAROTTI 9<br>10122 - TORINO (TO) |

Descrizione dei locali:

|                             |  |
|-----------------------------|--|
| ABBONAMENTO<br>MUSEI + CARD | <p>Accesso pubblico, controllato<br/>Il locale è provvisto di porte, armadi e/o cassette con serratura<br/>Il locale contiene dati personali, sensibili<br/>Nel locale vengono conservati dati contabili e paghe<br/>Gli addetti al controllo del locale sono ARUGA MARCO, PEPE ANNARITA</p> |
|-----------------------------|--|

|  |   |
|--|---|
| AMMINISTRAZIONE                                  | <p>Accesso pubblico, controllato</p> <p>Il locale è provvisto di porte, armadi e/o cassette con serratura</p> <p>Il locale contiene dati personali, sensibili</p> <p>Il locale contiene 2 elaboratori informatici</p> <p>Nel locale in cassaforte vengono conservate le cartelle cliniche sigillate dei dipendenti</p> <p>Gli addetti al controllo del locale sono CAGNASSO MAGDA, CORREALE AMALIA, PINTOR RENATA</p> |
| ARCHIVIO   | <p>Accesso controllato</p> <p>Il locale è provvisto di porte, armadi e/o cassette con serratura</p> <p>Il locale contiene dati personali, sensibili, giudiziari</p> <p>Gli addetti al controllo del locale sono CORREALE AMALIA, LEON FRANCESCA, PEPE ANNARITA, PINTOR RENATA</p>   |
| ARCHIVIO STORICO                                 | <p>Accesso controllato</p> <p>Il locale è provvisto di porte, armadi e/o cassette con serratura</p> <p>Il locale contiene dati personali, sensibili</p> <p>L'addetto al controllo del locale è MAUTINO ROBERTO</p>  |
| AREA SERVER                                      | <p>Accesso controllato</p> <p>Il locale è provvisto di porte, armadi e/o cassette con serratura</p> <p>Il locale contiene dati personali, sensibili, giudiziari</p> <p>Il locale contiene 1 server</p> <p>L'addetto al controllo del locale è D'ACRI ANTONIO MARCO</p>  |
| CALL CENTER                                      | <p>Accesso controllato</p> <p>Il locale è provvisto di porte, armadi e/o cassette con serratura</p> <p>Il locale contiene dati personali</p> <p>Il locale contiene 5 elaboratori informatici</p> <p>Gli addetti al controllo del locale sono BARAVELLI CRISTINA, BERTERO LUCA, BORGARO CHIARA, COCCIARDI STEFANO, EYNARD SIMONE FLAVIO, IACOBONE PASQUALE, VITRANI PAOLO</p>  |
| DIREZIONE  | <p>Accesso pubblico, controllato</p> <p>Il locale è provvisto di porte, armadi e/o cassette con serratura</p> <p>Il locale contiene dati personali, sensibili, giudiziari</p> <p>Gli incaricati che fanno base nel locale utilizzano 1 notebook</p> <p>Il locale contiene 3 elaboratori informatici</p> <p>Gli addetti al controllo del locale sono LEON FRANCESCA, RICCI SIMONA</p>                                  |
| SEGRETERIA<br>GENERALE /<br>ABBONAMENTO<br>MUSEI | <p>Accesso pubblico, controllato</p> <p>Il locale è provvisto di porte, armadi e/o cassette con serratura</p> <p>Il locale contiene dati personali, sensibili</p> <p>Il locale contiene 4 elaboratori informatici</p> <p>Gli addetti al controllo del locale sono MAUTINO ROBERTO, SERRA ELEONORA</p>   |

Segue l'elenco delle sedi e dei locali dei trattamenti svolti da responsabili esterni o autonomi titolari del trattamento

|             |                   |
|-------------|-------------------|
| <b>Sede</b> | BANCA SELLA       |
| <b>Note</b> | Istituto bancario |

|             |                                  |
|-------------|----------------------------------|
| <b>Sede</b> | BIPOINT                          |
| <b>Note</b> | Assistenza programma informatico |

|             |  |
|-------------|--|
| <b>Sede</b> | CITTA' DI TORINO   |
| <b>Note</b> | Telefonia per voce e dati, sia fissa che mobile + internet |

|             |                       |
|-------------|-----------------------|
| <b>Sede</b> | COMITATO ESECUTIVO    |
| <b>Note</b> | Organo amministrativo |

|             |                                  |
|-------------|----------------------------------|
| <b>Sede</b> | CRITICAL CASE                    |
| <b>Note</b> | Assistenza programma informatico |

|             |                   |
|-------------|-------------------|
| <b>Sede</b> | CSI PIEMONTE      |
| <b>Note</b> | Posta elettronica |

|             |  |
|-------------|--|
| <b>Sede</b> | DOTT. FRANZO ANGELO                        |
| <b>Note</b> | Medico competente (sorveglianza sanitaria) |

|             |   |
|-------------|---|
| <b>Sede</b> | DOTT. MARCO ALBERTO MALAGNINO                                   |
| <b>Note</b> | Consulente per sicurezza sul lavoro (d.lgs. 9 aprile 2008 n.81) |

|             |           |
|-------------|-----------|
| <b>Sede</b> | EVOLUTIVA |
| <b>Note</b> | Sito web  |

|             |          |
|-------------|----------|
| <b>Sede</b> | FORE     |
| <b>Note</b> | Sito web |

|             |                        |
|-------------|------------------------|
| <b>Sede</b> | GLS                    |
| <b>Note</b> | Trasporti e spedizioni |

|             |  |
|-------------|--|
| <b>Sede</b> | KOINE' SISTEMI   |
| <b>Note</b> | Assistenza programma informatico   |
| <b>Sede</b> | LEGAL MAIL   |
| <b>Note</b> | Provider pec   |
| <b>Sede</b> | LOTTOMATICA  |
| <b>Note</b> | Assistenza programma sistema prenotazione musei                              |
| <b>Sede</b> | PLUSERVICE   |
| <b>Note</b> | Assistenza programma informatico   |
| <b>Sede</b> | REALE MUTUA  |
| <b>Note</b> | Compagnia di assicurazione   |
| <b>Sede</b> | SEGRE MASSIMO  |
| <b>Note</b> | Revisore dei conti   |
| <b>Sede</b> | SPAZIOTTANTOTTO SRL  |
| <b>Note</b> | Consulente per la protezione dei dati personali (d.lgs. 30 marzo 2003 n.196) |
| <b>Sede</b> | STUDIO CODA  |
| <b>Note</b> | Commercialista ed elaborazione contabilita'                                  |
| <b>Sede</b> | STUDIO COMOLLO   |
| <b>Note</b> | Consulente del lavoro ed elaborazione cedolini paghe                         |
| <b>Sede</b> | STUDIO NOTARILE GANELLI MAROCCO  |
| <b>Note</b> | Studio notarile  |
| <b>Sede</b> | STUDIO TOSETTO WEIGMANN  |
| <b>Note</b> | Studio legale  |
| <b>Sede</b> | UNICREDIT BANCA  |
| <b>Note</b> | Istituto bancario  |

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |   |
|--------------------------------|---|
| <b>Nome</b>                    | <b>Agenda appuntamenti, visite e prenotazioni</b>                                   |
| <b>Riguarda</b>                | Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Clienti, fornitori, terzi identificati ed identificabili                            |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| BARAVELLI CRISTINA     |               | X         |
| BERTERO LUCA           |               | X         |
| BORGARO CHIARA         |               | X         |
| COCCIARDI STEFANO      |               | X         |
| EYNARD SIMONE FLAVIO   |               | X         |
| IACOBONE PASQUALE      |               | X         |
| VITRANI PAOLO          |               | X         |
| MAUTINO ROBERTO        |               | X         |
| PEPE ANNARITA          |               | X         |
| PINTOR RENATA          |               | X         |
| SERRA ELEONORA         |               | X         |
| ARUGA MARCO            |               | X         |
| CAGNASSO MAGDA         |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

Responsabili del trattamento:

LEON FRANCESCA

(continua...)

Responsabili del trattamento (...segue):

---

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

---

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA



## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |   |
|--------------------------------|---|
| <b>Nome</b>                    | <b>Anagrafica condivisa e rubrica</b>   |
| <b>Riguarda</b>                | Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Clienti, fornitori, terzi identificati ed identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| BARAVELLI CRISTINA     |               | X         |
| BERTERO LUCA           |               | X         |
| BORGARO CHIARA         |               | X         |
| COCCIARDI STEFANO      |               | X         |
| EYNARD SIMONE FLAVIO   |               | X         |
| IACOBONE PASQUALE      |               | X         |
| VITRANI PAOLO          |               | X         |
| MAUTINO ROBERTO        |               | X         |
| PEPE ANNARITA          |               | X         |
| PINTOR RENATA          |               | X         |
| SERRA ELEONORA         |               | X         |
| ARUGA MARCO            |               | X         |
| CAGNASSO MAGDA         |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

Responsabili del trattamento:

LEON FRANCESCA

## NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

---

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Attività di recupero crediti</b>                      |
| <b>Riguarda</b>                | Solleciti ai clienti per il pagamento di effetti scaduti |
| <b>Tipologia di dati</b>       | Dati economici riservati                                 |
| <b>Categoria interessati</b>   | Clienti  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non                              |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| PEPE ANNARITA          |               | X         |
| PINTOR RENATA          |               | X         |
| CAGNASSO MAGDA         |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

Responsabili del trattamento:

|                |
|----------------|
| LEON FRANCESCA |
|----------------|

Responsabili del trattamento in esterno:

| Responsabile                                | Soggetto di riferimento | Permessi* |
|---|-------------------------|-----------|
| COMITATO ESECUTIVO<br>Organo amministrativo |                         | C         |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

---

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |   |
|--------------------------------|---|
| <b>Nome</b>                    | <b>Banca dati associati</b>               |
| <b>Riguarda</b>                | Dati relativi agli associati              |
| <b>Tipologia di dati</b>       | Dati personali e potenzialmente sensibili |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili       |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non               |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| BARAVELLI CRISTINA     |               | X         |
| BERTERO LUCA           |               | X         |
| BORGARO CHIARA         |               | X         |
| COCCIARDI STEFANO      |               | X         |
| EYNARD SIMONE FLAVIO   |               | X         |
| IACOBONE PASQUALE      |               | X         |
| VITRANI PAOLO          |               | X         |
| MAUTINO ROBERTO        |               | X         |
| PEPE ANNARITA          |               | X         |
| PINTOR RENATA          |               | X         |
| SERRA ELEONORA         |               | X         |
| ARUGA MARCO            |               | X         |
| CAGNASSO MAGDA         |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

**Responsabili del trattamento:**

LEON FRANCESCA

(continua...)

Responsabili del trattamento (...segue):

Responsabili del trattamento in esterno:

| Responsabile                                | Soggetto di riferimento | Permessi* |
|---|-------------------------|-----------|
| COMITATO ESECUTIVO<br>Organo amministrativo |                         | C         |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Banca dati gestione e organizzazione eventi</b>       |
| <b>Riguarda</b>                | Dati relativi a location, budget, personale tecnico, ecc |
| <b>Tipologia di dati</b>       | Dati personali e potenzialmente sensibili                |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili                      |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non                              |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| MAUTINO ROBERTO        |               | X         |
| PEPE ANNARITA          |               | X         |
| PINTOR RENATA          |               | X         |
| SERRA ELEONORA         |               | X         |
| ARUGA MARCO            |               | X         |
| CAGNASSO MAGDA         |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

**Responsabili del trattamento:**

LEON FRANCESCA

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA



## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Banca dati istituzioni</b>                                |
| <b>Riguarda</b>                | Dati relativi alle istituzioni con cui sussistono dei legami |
| <b>Tipologia di dati</b>       | Dati personali e potenzialmente sensibili                    |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili                          |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non                                  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| BARAVELLI CRISTINA     |               | X         |
| BERTERO LUCA           |               | X         |
| BORGARO CHIARA         |               | X         |
| COCCIARDI STEFANO      |               | X         |
| EYNARD SIMONE FLAVIO   |               | X         |
| IACOBONE PASQUALE      |               | X         |
| VITRANI PAOLO          |               | X         |
| MAUTINO ROBERTO        |               | X         |
| PEPE ANNARITA          |               | X         |
| PINTOR RENATA          |               | X         |
| SERRA ELEONORA         |               | X         |
| ARUGA MARCO            |               | X         |
| CAGNASSO MAGDA         |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

Responsabili del trattamento:

LEON FRANCESCA

(continua...)

Responsabili del trattamento (...segue):

Responsabili del trattamento in esterno:

| Responsabile                                | Soggetto di riferimento | Permessi* |
|---|-------------------------|-----------|
| COMITATO ESECUTIVO<br>Organo amministrativo |                         | C         |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Banca dati promozione</b>                       |
| <b>Riguarda</b>                | Dati relativi alla promozione di servizi ed eventi |
| <b>Tipologia di dati</b>       | Dati personali e potenzialmente sensibili          |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili                |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non                        |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| MAUTINO ROBERTO        |               | X         |
| PEPE ANNARITA          |               | X         |
| PINTOR RENATA          |               | X         |
| SERRA ELEONORA         |               | X         |
| ARUGA MARCO            |               | X         |
| CAGNASSO MAGDA         |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

**Responsabili del trattamento:**

LEON FRANCESCA

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |   |
|--------------------------------|---|
| <b>Nome</b>                    | <b>Banca dati regolamento ed anagrafica contratti operatori esterni</b> |
| <b>Riguarda</b>                | Dati relativi ai regolamenti ed anagrafiche contratti operatori esterni |
| <b>Tipologia di dati</b>       | Dati personali e potenzialmente sensibili                               |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili                                     |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| MAUTINO ROBERTO        |               | X         |
| PEPE ANNARITA          |               | X         |
| PINTOR RENATA          |               | X         |
| SERRA ELEONORA         |               | X         |
| ARUGA MARCO            |               | X         |
| CAGNASSO MAGDA         |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

**Responsabili del trattamento:**

LEON FRANCESCA

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Banca dati sistema prenotazione musei</b>   |
| <b>Riguarda</b>                | Dati relativi ai servizi di prenotazione musei |
| <b>Tipologia di dati</b>       | Dati personali e potenzialmente sensibili      |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili            |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non                    |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| BARAVELLI CRISTINA     |               | X         |
| BERTERO LUCA           |               | X         |
| BORGARO CHIARA         |               | X         |
| COCCIARDI STEFANO      |               | X         |
| EYNARD SIMONE FLAVIO   |               | X         |
| IACOBONE PASQUALE      |               | X         |
| VITRANI PAOLO          |               | X         |
| MAUTINO ROBERTO        |               | X         |
| PEPE ANNARITA          |               | X         |
| PINTOR RENATA          |               | X         |
| SERRA ELEONORA         |               | X         |
| ARUGA MARCO            |               | X         |
| CAGNASSO MAGDA         |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | C         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

**Responsabili del trattamento:**

LEON FRANCESCA

(continua...)

Responsabili del trattamento (...segue):

---

Responsabili del trattamento in esterno:

| Responsabile                                    | Soggetto di riferimento | Permessi* |
|---|-------------------------|-----------|
| LOTTOMATICA                                     |                         | X         |
| Assistenza programma sistema prenotazione musei |                         |           |

---

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

**I** inserimento, raccolta, registrazione

**C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo

**M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione

**A** annullamento, blocco, cancellazione, distruzione

**T** trasporto/trasferimento

**N** solo conservazione dei supporti, senza accesso ai contenuti

**D** diffusione

**X** equivalente ai permessi ICMAT

**L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

---

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA



## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Banca dati utenti cessione terzi</b>  |
| <b>Riguarda</b>                | Dati anagrafici e di riferimento dei soggetti fornitori di servizi della struttura potenzialmente interessati a prodotti, eventi forniti da terzi da noi individuati |
| <b>Tipologia di dati</b>       | Dati personali e potenzialmente sensibili  |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| PEPE ANNARITA          |               | X         |
| PINTOR RENATA          |               | X         |
| SERRA ELEONORA         |               | X         |
| CAGNASSO MAGDA         |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

Responsabili del trattamento:

LEON FRANCESCA

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |   |
|--------------------------------|---|
| <b>Nome</b>                    | <b>Cartelle sanitarie di rischio dei lavoratori soggetti a sorveglianza sanitaria</b> |
| <b>Riguarda</b>                | Visite ed esami di medicina del lavoro svolte dai lavoratori soggetti                 |
| <b>Tipologia di dati</b>       | Dati sensibili  |
| <b>Categoria interessati</b>   | Lavoratori, dipendenti, soci, amministratori, collaboratori                           |
| <b>Modalità di trattamento</b> | Supporti cartacei   |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| EYNARD SIMONE FLAVIO   |               | T         |
| D'ACRI ANTONIO MARCO   |               | C         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |

**Responsabili del trattamento:**

LEON FRANCESCA

Responsabili del trattamento in esterno:

| Responsabile                               | Soggetto di riferimento | Permessi* |
|--|-------------------------|-----------|
| DOTT. FRANZO ANGELO                        |                         | X         |
| Medico competente (sorveglianza sanitaria) |                         |           |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |   |
|--------------------------------|---|
| <b>Nome</b>                    | <b>Comunicazioni telefoniche</b>  |
| <b>Riguarda</b>                | Informazioni circa chiamate in entrata e in uscita gestito per fini tecnici, amministrativi e commerciali |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Terzi identificati ed identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici   |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |

**Responsabili del trattamento:**

|                |
|----------------|
| LEON FRANCESCA |
|----------------|

Responsabili del trattamento in esterno:

| Responsabile   | Soggetto di riferimento | Permessi* |
|--|-------------------------|-----------|
| CITTA' DI TORINO   |                         | X         |
| Telefonia per voce e dati, sia fissa che mobile + internet |                         |           |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Contabilità propria</b>   |
| <b>Riguarda</b>                | Fatture, corrispettivi, multe, movimenti contabili, modelli fiscali, tributari, doganali, ecc.       |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| PINTOR RENATA          |               | X         |
| CAGNASSO MAGDA         |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | C         |
| D'ACRI ANTONIO MARCO   |               | C         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

Responsabili del trattamento:

LEON FRANCESCA

Responsabili del trattamento in esterno:

| Responsabile                               | Soggetto di riferimento | Permessi* |
|--|-------------------------|-----------|
| COMITATO ESECUTIVO                         |                         | C         |
| Organo amministrativo                      |                         |           |
| SEGRE MASSIMO                              |                         | C         |
| Revisore dei conti                         |                         |           |
| STUDIO CODA                                |                         | X         |
| Commercialista ed elaborazione contabilità |                         |           |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

---

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA



## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |   |
|--------------------------------|---|
| <b>Nome</b>                    | <b>Corrispondenza, comunicati e circolari</b>   |
| <b>Riguarda</b>                | Informazioni varie conservate a fini amministrativi o per future ed eventuali pratiche legali |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Clienti, fornitori, terzi identificati ed identificabili                                      |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| ARUGA MARCO            |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |

Responsabili del trattamento:

|                |
|----------------|
| LEON FRANCESCA |
|----------------|

Responsabili del trattamento in esterno:

| Responsabile                                | Soggetto di riferimento | Permessi* |
|---|-------------------------|-----------|
| COMITATO ESECUTIVO<br>Organo amministrativo |                         | C         |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Entratel</b>  |
| <b>Riguarda</b>                | Trasmissione telematica di dichiarazioni ed atti per effettuare gli adempimenti tributari, presentare il modello unico, pagare le imposte, presentare la dichiarazione dei sostituti di imposta (modello 770), registrare i contratti di locazione, presentare la dichiarazione di inizio o cessazione attività, accedere al cassetto fiscale che consente la consultazione di alcune informazioni personali relative a dati anagrafici e reddituali, rimborsi, versamenti effettuati tramite modello f24 e f23 ed altre, ecc. |
| <b>Tipologia di dati</b>       | Dati personali economici   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti e fornitori, terzi identificati e identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Programma/Attrezzatura</b>  | Entratel   |

### Responsabili del trattamento:

LEON FRANCESCA

### Responsabili del trattamento in esterno:

| Responsabile  | Soggetto di riferimento | Permessi* |
|---|-------------------------|-----------|
| STUDIO CODA<br>Commercialista ed elaborazione contabilità |                         | X         |

### NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Gestione acquisti e approvvigionamenti</b>  |
| <b>Riguarda</b>                | Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Fornitori e potenziali fornitori   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| BARAVELLI CRISTINA     |               | C         |
| BERTERO LUCA           |               | C         |
| BORGARO CHIARA         |               | C         |
| COCCIARDI STEFANO      |               | C         |
| EYNARD SIMONE FLAVIO   |               | C         |
| IACOBONE PASQUALE      |               | C         |
| VITRANI PAOLO          |               | C         |
| MAUTINO ROBERTO        |               | X         |
| PEPE ANNARITA          |               | X         |
| PINTOR RENATA          |               | X         |
| SERRA ELEONORA         |               | X         |
| ARUGA MARCO            |               | C         |
| CAGNASSO MAGDA         |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

**Responsabili del trattamento:**

LEON FRANCESCA

(continua...)

Responsabili del trattamento (...segue):

Responsabili del trattamento in esterno:

| Responsabile                                | Soggetto di riferimento | Permessi* |
|---|-------------------------|-----------|
| COMITATO ESECUTIVO<br>Organo amministrativo |                         | C         |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Gestione del rapporto di lavoro nei confronti dei propri lavoratori</b>   |
| <b>Riguarda</b>                | Relazioni con i propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese la registrazione delle presenze, l'elaborazione dei compensi, la gestione del libro unico del lavoro, i rapporti con enti previdenziali, assicurativi, sindacali, ecc. |
| <b>Tipologia di dati</b>       | Dati personali e sensibili   |
| <b>Categoria interessati</b>   | Lavoratori, dipendenti, soci, amministratori, collaboratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| PINTOR RENATA          |               | C         |
| CAGNASSO MAGDA         |               | C         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | C         |

Responsabili del trattamento:

LEON FRANCESCA

Responsabili del trattamento in esterno:

| Responsabile   | Soggetto di riferimento | Permessi* |
|--|-------------------------|-----------|
| STUDIO COMOLLO                                       |                         | X         |
| Consulente del lavoro ed elaborazione cedolini paghe |                         |           |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

---

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |   |
|--------------------------------|---|
| <b>Nome</b>                    | <b>Gestione della clientela</b>   |
| <b>Riguarda</b>                | Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Clienti e potenziali clienti  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| BARAVELLI CRISTINA     |               | C         |
| BERTERO LUCA           |               | C         |
| BORGARO CHIARA         |               | C         |
| COCCIARDI STEFANO      |               | C         |
| EYNARD SIMONE FLAVIO   |               | C         |
| IACOBONE PASQUALE      |               | C         |
| VITRANI PAOLO          |               | C         |
| MAUTINO ROBERTO        |               | X         |
| PEPE ANNARITA          |               | X         |
| PINTOR RENATA          |               | X         |
| SERRA ELEONORA         |               | X         |
| ARUGA MARCO            |               | C         |
| CAGNASSO MAGDA         |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

**Responsabili del trattamento:**

LEON FRANCESCA

(continua...)



Responsabili del trattamento (...segue):

---

Responsabili del trattamento in esterno:

| Responsabile                                | Soggetto di riferimento | Permessi* |
|---|-------------------------|-----------|
| COMITATO ESECUTIVO<br>Organo amministrativo |                         | C         |

---

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

---

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Gestione libri sociali</b>  |
| <b>Riguarda</b>                | Libro soci, libro giornale, verbali, ecc.  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |
| <b>Modalità di trattamento</b> | Supporti cartacei  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| MAUTINO ROBERTO        |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |

**Responsabili del trattamento:**

|                |
|----------------|
| LEON FRANCESCA |
|----------------|

Responsabili del trattamento in esterno:

| Responsabile                               | Soggetto di riferimento | Permessi* |
|--|-------------------------|-----------|
| COMITATO ESECUTIVO                         |                         | C         |
| Organo amministrativo                      |                         |           |
| SEGRE MASSIMO                              |                         | C         |
| Revisore dei conti                         |                         |           |
| STUDIO CODA                                |                         | X         |
| Commercialista ed elaborazione contabilità |                         |           |
| STUDIO NOTARILE GANELLI MAROCCO            |                         | X         |
| Studio notarile                            |                         |           |
| STUDIO TOSETTO WEIGMANN                    |                         | C         |

(continua...)

(...segue)

| <b>Responsabile</b> | <b>Soggetto di riferimento</b> | <b>Permessi*</b> |
|---------------------|--------------------------------|------------------|
| Studio legale       |                                |                  |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Gestione polizze assicurative</b>   |
| <b>Riguarda</b>                | Informazioni necessarie per la gestione delle polizze assicurative di cui si è contraente e/o beneficiario, ecc. |
| <b>Tipologia di dati</b>       | Dati personali eventualmente sensibili   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | X         |
| BRACCIALARGHE MAURIZIO |               | X         |
| COPPOLA MICHELE        |               | X         |

Responsabili del trattamento:

|                |
|----------------|
| LEON FRANCESCA |
|----------------|

Responsabili del trattamento in esterno:

| Responsabile               | Soggetto di riferimento | Permessi* |
|----------------------------|-------------------------|-----------|
| COMITATO ESECUTIVO         |                         | C         |
| Organo amministrativo      |                         |           |
| REALE MUTUA                |                         | X         |
| Compagnia di assicurazione |                         |           |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Incassi, pagamenti e operazioni bancarie</b>  |
| <b>Riguarda</b>                | Estratti conti, bonifici, assegni, versamenti, riba, rid, ecc.                                       |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| BARAVELLI CRISTINA     |               | X         |
| BERTERO LUCA           |               | X         |
| BORGARO CHIARA         |               | X         |
| COCCIARDI STEFANO      |               | X         |
| EYNARD SIMONE FLAVIO   |               | X         |
| IACOBONE PASQUALE      |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | C         |
| D'ACRI ANTONIO MARCO   |               | C         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |

**Responsabili del trattamento:**

|                |
|----------------|
| LEON FRANCESCA |
|----------------|

Responsabili del trattamento in esterno:

| Responsabile                                | Soggetto di riferimento | Permessi* |
|---|-------------------------|-----------|
| COMITATO ESECUTIVO<br>Organo amministrativo |                         | C         |

**Autonomi titolari del trattamento che forniscono determinati servizi e/o prodotti**

BANCA SELLA  
UNICREDIT BANCA

---

**NOTE:**

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

---

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Posta elettronica</b>   |
| <b>Riguarda</b>                | Mittente, destinatari, contenuto delle e-mail                        |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| MAUTINO ROBERTO        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |

Responsabili del trattamento:

|                |
|----------------|
| LEON FRANCESCA |
|----------------|

Responsabili del trattamento in esterno:

| Responsabile      | Soggetto di riferimento | Permessi* |
|-------------------|-------------------------|-----------|
| CSI PIEMONTE      |                         | X         |
| Posta elettronica |                         |           |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.



Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Posta elettronica certificata</b>                                 |
| <b>Riguarda</b>                | Mittente, destinatari, contenuto delle e-mail certificate            |
| <b>Tipologia di dati</b>       | Dati personali eventualmente sensibili                               |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| MAUTINO ROBERTO        |               | X         |
| SERRA ELEONORA         |               | X         |
| ARUGA MARCO            |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |

**Responsabili del trattamento:**

LEON FRANCESCA

**Autonomi titolari del trattamento che forniscono determinati servizi e/o prodotti**

LEGAL MAIL

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |   |
|--------------------------------|---|
| <b>Nome</b>                    | <b>Pratiche legali e contenziosi</b>  |
| <b>Riguarda</b>                | Dati giudiziari per cause civili, penali, di lavoro, amministrative, stragiudiziali, ecc. che interessano il titolare del trattamento e terzi identificati e identificabili |
| <b>Tipologia di dati</b>       | Dati giudiziari   |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili  |
| <b>Modalità di trattamento</b> | Cartacea; informatica mediante fax e/o computer, utilizzando file di suite da ufficio, quali fogli di calcolo ed elaboratori di testi; upporti cartacei                     |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| PEPE ANNARITA          |               | X         |
| PINTOR RENATA          |               | X         |
| ARUGA MARCO            |               | X         |
| CAGNASSO MAGDA         |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

Responsabili del trattamento:

LEON FRANCESCA

Responsabili del trattamento in esterno:

| Responsabile            | Soggetto di riferimento | Permessi* |
|-------------------------|-------------------------|-----------|
| COMITATO ESECUTIVO      |                         | C         |
| Organo amministrativo   |                         |           |
| STUDIO TOSETTO WEIGMANN |                         | X         |

(continua...)

(...segue)

| <b>Responsabile</b> | <b>Soggetto di riferimento</b> | <b>Permessi*</b> |
|---------------------|--------------------------------|------------------|
| Studio legale       |                                |                  |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Predisposizione dichiarazione dei redditi e bilancio</b>  |
| <b>Riguarda</b>                | Documenti vari necessari al corretto adempimento delle misure di legge in materia societaria, fiscale e tributaria |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, terzi identificati ed identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| PINTOR RENATA          |               | X         |
| CAGNASSO MAGDA         |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

Responsabili del trattamento:

LEON FRANCESCA

Responsabili del trattamento in esterno:

| Responsabile                               | Soggetto di riferimento | Permessi* |
|--|-------------------------|-----------|
| COMITATO ESECUTIVO                         |                         | C         |
| Organo amministrativo                      |                         |           |
| STUDIO CODA                                |                         | X         |
| Commercialista ed elaborazione contabilità |                         |           |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

---

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Registrazione e gestione delle presenze nei confronti dei propri lavoratori</b>   |
| <b>Riguarda</b>                | Dati inerenti alle presenze dei propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese le ferie, le malattie, i lutti, i permessi, gli straordinari, ecc. |
| <b>Tipologia di dati</b>       | Dati personali e sensibili   |
| <b>Categoria interessati</b>   | Lavoratori, dipendenti, soci, amministratori, collaboratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |

**Responsabili del trattamento:**

LEON FRANCESCA

Responsabili del trattamento in esterno:

| Responsabile   | Soggetto di riferimento | Permessi* |
|--|-------------------------|-----------|
| STUDIO COMOLLO<br>Consulente del lavoro ed elaborazione cedolini paghe |                         | C         |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:



- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

---

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |   |
|--------------------------------|---|
| <b>Nome</b>                    | <b>Relazioni pubbliche</b>                              |
| <b>Riguarda</b>                | Attività con istituzioni pubbliche, con la stampa, ecc. |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Soggetto stesso   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non                             |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | X         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | X         |
| COPPOLA MICHELE        |               | X         |

Responsabili del trattamento:

|                |
|----------------|
| LEON FRANCESCA |
|----------------|

Responsabili del trattamento in esterno:

| Responsabile                                | Soggetto di riferimento | Permessi* |
|---|-------------------------|-----------|
| COMITATO ESECUTIVO<br>Organo amministrativo |                         | C         |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Revisione dei conti e certificazione di bilancio</b>  |
| <b>Riguarda</b>                | Attività di controllo sui documenti contabili, societari, fiscali, tributari, previdenziali, ecc.    |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |

Responsabili del trattamento:

|                |
|----------------|
| LEON FRANCESCA |
|----------------|

Responsabili del trattamento in esterno:

| Responsabile       | Soggetto di riferimento | Permessi* |
|--------------------|-------------------------|-----------|
| SEGRE MASSIMO      |                         | X         |
| Revisore dei conti |                         |           |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Selezione del personale</b>   |
| <b>Riguarda</b>                | Curriculum vitae, questionari, prove di selezione di candidati per posti di lavoro |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Potenziali lavoratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | X         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | X         |
| COPPOLA MICHELE        |               | X         |

Responsabili del trattamento:

|                |
|----------------|
| LEON FRANCESCA |
|----------------|

Responsabili del trattamento in esterno:

| Responsabile                                | Soggetto di riferimento | Permessi* |
|---|-------------------------|-----------|
| COMITATO ESECUTIVO<br>Organo amministrativo |                         | X         |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Sistema di gestione della protezione del trattamento di dati</b>  |
| <b>Riguarda</b>                | Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03) |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| BARAVELLI CRISTINA     |               | C         |
| BERTERO LUCA           |               | C         |
| BORGARO CHIARA         |               | C         |
| COCCIARDI STEFANO      |               | C         |
| EYNARD SIMONE FLAVIO   |               | C         |
| IACOBONE PASQUALE      |               | C         |
| VITRANI PAOLO          |               | C         |
| MAUTINO ROBERTO        |               | C         |
| PEPE ANNARITA          |               | C         |
| PINTOR RENATA          |               | C         |
| SERRA ELEONORA         |               | C         |
| ARUGA MARCO            |               | C         |
| CAGNASSO MAGDA         |               | C         |
| CORREALE AMALIA        |               | C         |
| LEON FRANCESCA         |               | C         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | C         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | C         |

**Responsabili del trattamento:**

LEON FRANCESCA

Responsabili del trattamento in esterno:

| Responsabile   | Soggetto di riferimento | Permessi* |
|--|-------------------------|-----------|
| COMITATO ESECUTIVO<br>Organo amministrativo  |                         | C         |
| SPAZIOTTANTOTTO SRL<br>Consulente per la protezione dei dati personali<br>(d.lgs. 30 marzo 2003 n.196) |                         | X         |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA



## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Sistema di gestione della sicurezza sul lavoro</b>  |
| <b>Riguarda</b>                | Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08) |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)  |
| <b>Modalità di trattamento</b> | Supporti cartacei  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| BARAVELLI CRISTINA     |               | C         |
| BERTERO LUCA           |               | C         |
| BORGARO CHIARA         |               | C         |
| COCCIARDI STEFANO      |               | C         |
| EYNARD SIMONE FLAVIO   |               | C         |
| IACOBONE PASQUALE      |               | C         |
| VITRANI PAOLO          |               | C         |
| MAUTINO ROBERTO        |               | C         |
| PEPE ANNARITA          |               | C         |
| PINTOR RENATA          |               | C         |
| SERRA ELEONORA         |               | C         |
| ARUGA MARCO            |               | C         |
| CAGNASSO MAGDA         |               | C         |
| CORREALE AMALIA        |               | C         |
| LEON FRANCESCA         |               | C         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | C         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | C         |

Responsabili del trattamento:

LEON FRANCESCA

Responsabili del trattamento in esterno:

| Responsabile   | Soggetto di riferimento | Permessi* |
|--|-------------------------|-----------|
| COMITATO ESECUTIVO<br>Organo amministrativo  |                         | C         |
| DOTT. FRANZO ANGELO<br>Medico competente (sorveglianza sanitaria)                                |                         | X         |
| DOTT. MARCO ALBERTO MALAGNINO<br>Consulente per sicurezza sul lavoro (d.lgs. 9 aprile 2008 n.81) |                         | X         |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |   |
|--------------------------------|---|
| <b>Nome</b>                    | <b>Sistema informativo</b>  |
| <b>Riguarda</b>                | Informazioni necessarie per garantire il funzionamento dell'insieme di postazioni informatiche (computer fissi, portatili, palmari, ecc.), stampanti, attrezzature di rete (switch, router, access point, firewall, ecc.) e server, atto al trattamento dei dati sia dal punto di vista software che hardware; in particolare per quanto attiene ai sistemi di autenticazione ed autorizzazione |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Utenti del sistema informativo, lavoratori, collaboratori   |
| <b>Modalità di trattamento</b> | Strumenti elettronici   |
| <b>Programma/Attrezzatura</b>  | Sistemi operativi degli strumenti elettronici in uso  |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| MAUTINO ROBERTO        |               | X         |
| SERRA ELEONORA         |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |

**Responsabili del trattamento:**

LEON FRANCESCA

**Amministratori di sistema:**

KOINE' SISTEMI

Responsabili del trattamento in esterno:

| Responsabile                     | Soggetto di riferimento | Permessi* |
|----------------------------------|-------------------------|-----------|
| BIPOINT                          |                         | X         |
| Assistenza programma informatico |                         |           |
| CRITICAL CASE                    |                         | X         |
| Assistenza programma informatico |                         |           |
| PLUSERVICE                       |                         | X         |
| Assistenza programma informatico |                         |           |

## NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |   |
|--------------------------------|---|
| <b>Nome</b>                    | <b>Sito web</b>   |
| <b>Riguarda</b>                | Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc. |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici   |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| BARAVELLI CRISTINA     |               | X         |
| BERTERO LUCA           |               | X         |
| BORGARO CHIARA         |               | X         |
| COCCIARDI STEFANO      |               | X         |
| EYNARD SIMONE FLAVIO   |               | X         |
| IACOBONE PASQUALE      |               | X         |
| VITRANI PAOLO          |               | X         |
| MAUTINO ROBERTO        |               | X         |
| PEPE ANNARITA          |               | X         |
| SERRA ELEONORA         |               | X         |
| ARUGA MARCO            |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |

**Responsabili del trattamento:**

LEON FRANCESCA

Responsabili del trattamento in esterno:

| Responsabile | Soggetto di riferimento | Permessi* |
|--------------|-------------------------|-----------|
| EVOLUTIVA    |                         | X         |
| Sito web     |                         |           |
| FORE         |                         | X         |
| Sito web     |                         |           |

## NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Spedizione e ricezione di documenti e materiale</b> |
| <b>Riguarda</b>                | Documenti di trasporto, indirizzari, ecc.              |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti e fornitori                                    |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non                            |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| BARAVELLI CRISTINA     |               | C         |
| BERTERO LUCA           |               | C         |
| BORGARO CHIARA         |               | C         |
| COCCIARDI STEFANO      |               | C         |
| EYNARD SIMONE FLAVIO   |               | C         |
| IACOBONE PASQUALE      |               | C         |
| VITRANI PAOLO          |               | C         |
| MAUTINO ROBERTO        |               | X         |
| PEPE ANNARITA          |               | X         |
| PINTOR RENATA          |               | X         |
| SERRA ELEONORA         |               | X         |
| ARUGA MARCO            |               | C         |
| CAGNASSO MAGDA         |               | X         |
| CORREALE AMALIA        |               | X         |
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| RICCI SIMONA           |               | X         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |
| RINALDI VALERIA        |               | X         |

**Responsabili del trattamento:**

LEON FRANCESCA

(continua...)

Responsabili del trattamento (...segue):

---

Responsabili del trattamento in esterno:

| Responsabile                  | Soggetto di riferimento | Permessi* |
|-------------------------------|-------------------------|-----------|
| GLS<br>Trasporti e spedizioni |                         | X         |

---

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

**I** inserimento, raccolta, registrazione

**C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo

**M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione

**A** annullamento, blocco, cancellazione, distruzione

**T** trasporto/trasferimento

**N** solo conservazione dei supporti, senza accesso ai contenuti

**D** diffusione

**X** equivalente ai permessi ICMAT

**L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

---

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA



## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

|                                |   |
|--------------------------------|---|
| <b>Nome</b>                    | <b>Trasmissioni dati in internet (navigazione web, file sharing, ecc.)</b>  |
| <b>Riguarda</b>                | Indirizzi degli host coinvolti, dati trasmessi, ecc. compresi indirizzi e contenuti delle pagine web visitate, contenuti delle sessioni di messagerie |
| <b>Tipologia di dati</b>       | Dati personali e potenzialmente sensibili   |
| <b>Categoria interessati</b>   | Lavoratori, terzi identificati e identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |

Incaricati del trattamento:

| Incaricato             | Locali e Sedi | Permessi* |
|------------------------|---------------|-----------|
| LEON FRANCESCA         |               | X         |
| D'ACRI ANTONIO MARCO   |               | C         |
| BRACCIALARGHE MAURIZIO |               | C         |
| COPPOLA MICHELE        |               | C         |

Responsabili del trattamento:

LEON FRANCESCA

Responsabili del trattamento in esterno:

| Responsabile                     | Soggetto di riferimento | Permessi* |
|----------------------------------|-------------------------|-----------|
| KOINE' SISTEMI                   |                         | X         |
| Assistenza programma informatico |                         |           |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

### Elenco dei personal computer, ovvero delle workstation non portatili (desktop)

| # | Marca<br>Modello<br>S/N | Caratteristiche<br>e Sistema<br>Operativo | Nome Host<br>(IP Addr.) | Luogo<br>installazione  | Utilizzatori | Descrizione |
|---|-------------------------|---|-------------------------|---|--------------|-------------|
| 1 |                         |   |                         | sede C/O PALAZZO<br>DELLA REGIONE<br>C/O INFOPIEMONTE -<br>FRONT OFFICE - AREA<br>OPERATIVA |              |             |
| 2 |                         |   |                         | sede C/O PALAZZO<br>DELLA REGIONE<br>C/O INFOPIEMONTE -<br>FRONT OFFICE - AREA<br>OPERATIVA |              |             |
| 3 |                         |   |                         | sede C/O PALAZZO<br>DELLA REGIONE<br>C/O INFOPIEMONTE -<br>FRONT OFFICE - AREA<br>OPERATIVA |              |             |
| 4 |                         |   |                         | sede C/O PALAZZO<br>DELLA REGIONE<br>C/O INFOPIEMONTE -<br>FRONT OFFICE - AREA<br>OPERATIVA |              |             |
| 5 |                         |   |                         | sede C/O PALAZZO<br>DELLA REGIONE<br>C/O INFOPIEMONTE -<br>FRONT OFFICE - AREA<br>OPERATIVA |              |             |
| 6 |                         |   |                         | sede SEDE OPERATIVA<br>AMMINISTRAZIONE  |              |             |
| 7 |                         |   |                         | sede SEDE OPERATIVA<br>AMMINISTRAZIONE  |              |             |
| 8 |                         |   |                         | sede SEDE OPERATIVA<br>CALL CENTER  |              |             |
| 9 |                         |   |                         | sede SEDE OPERATIVA<br>CALL CENTER  |              |             |

|    |  |  |  |  |  |  |
|----|--|--|--|--|--|--|
| 10 |  |  |  | sede SEDE OPERATIVA<br>CALL CENTER                                     |  |  |
| 11 |  |  |  | sede SEDE OPERATIVA<br>CALL CENTER                                     |  |  |
| 12 |  |  |  | sede SEDE OPERATIVA<br>CALL CENTER                                     |  |  |
| 13 |  |  |  | sede SEDE OPERATIVA<br>DIREZIONE                                       |  |  |
| 14 |  |  |  | sede SEDE OPERATIVA<br>DIREZIONE                                       |  |  |
| 15 |  |  |  | sede SEDE OPERATIVA<br>DIREZIONE                                       |  |  |
| 16 |  |  |  | sede SEDE OPERATIVA<br>SEGRETERIA GENERALE<br>/ ABBONAMENTO MU-<br>SEI |  |  |
| 17 |  |  |  | sede SEDE OPERATIVA<br>SEGRETERIA GENERALE<br>/ ABBONAMENTO MU-<br>SEI |  |  |
| 18 |  |  |  | sede SEDE OPERATIVA<br>SEGRETERIA GENERALE<br>/ ABBONAMENTO MU-<br>SEI |  |  |
| 19 |  |  |  | sede SEDE OPERATIVA<br>SEGRETERIA GENERALE<br>/ ABBONAMENTO MU-<br>SEI |  |  |
| 20 |  |  |  |  |  |  |
| 21 |  |  |  |  |  |  |
| 22 |  |  |  |  |  |  |
| 23 |  |  |  |  |  |  |
| 24 |  |  |  |  |  |  |
| 25 |  |  |  |  |  |  |

## Elenco dei computer portatili (laptop, notebook, netbook, PDA, smartphone, ecc.)

| #  | Marca<br>Modello<br>S/N | Caratteristiche<br>e Sistema<br>Operativo | Nome Host<br>(IP Addr.) | Luogo<br>installazione           | Utilizzatori | Descrizione |
|----|-------------------------|---|-------------------------|----------------------------------|--------------|-------------|
| 1  |                         |   |                         | sede SEDE OPERATIVA<br>DIREZIONE |              |             |
| 2  |                         |   |                         |                                  |              |             |
| 3  |                         |   |                         |                                  |              |             |
| 4  |                         |   |                         |                                  |              |             |
| 5  |                         |   |                         |                                  |              |             |
| 6  |                         |   |                         |                                  |              |             |
| 7  |                         |   |                         |                                  |              |             |
| 8  |                         |   |                         |                                  |              |             |
| 9  |                         |   |                         |                                  |              |             |
| 10 |                         |   |                         |                                  |              |             |

## Elenco dei server

| #  | Marca<br>Modello<br>S/N | Caratteristiche<br>e Sistema<br>Operativo | Nome Host<br>(IP Addr.) | Luogo<br>installazione             | Utilizzatori | Descrizione |
|----|-------------------------|---|-------------------------|------------------------------------|--------------|-------------|
| 1  |                         |   |                         | sede SEDE OPERATIVA<br>AREA SERVER |              |             |
| 2  |                         |   |                         |                                    |              |             |
| 3  |                         |   |                         |                                    |              |             |
| 4  |                         |   |                         |                                    |              |             |
| 5  |                         |   |                         |                                    |              |             |
| 6  |                         |   |                         |                                    |              |             |
| 7  |                         |   |                         |                                    |              |             |
| 8  |                         |   |                         |                                    |              |             |
| 9  |                         |   |                         |                                    |              |             |
| 10 |                         |   |                         |                                    |              |             |

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

| # | Sito Web | Necessita autenticazione | Descrizione contenuti e attività |
|---|----------|--------------------------|----------------------------------|
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |
|   |          |                          |                                  |

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

| # | Casella | Lavorativa<br>o personale | Utilizzatore | Fiduciario |
|---|---------|---------------------------|--------------|------------|
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |



## **Appendice B**

# **Piano di Formazione**

Il comma 19.6 dell'Allegato B, Disciplinare tecnico in materia di misure minime di sicurezza, previsto dagli artt.33-36 del D.Lgs. 196/2003, richiede la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. Inoltre la formazione deve essere programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

Sono previsti interventi di formazione volti ad istruire e sensibilizzare le risorse incaricate del trattamento dei dati sensibili ed a carattere giudiziario per quanto concerne i rischi connessi al trattamento di tale tipologia di dati e a riguardo delle misure di protezione idonee ad evitare il verificarsi di tali rischi.

Gli interventi formativi sono programmati al verificarsi di una delle seguenti circostanze:

- nuova assunzione di un incaricato al trattamento;
- assegnazione ad una nuova mansione che comporti l'esigenza di accesso o di trattamento circa dati personali, sensibili o giudiziari e la conseguente qualifica di incaricato al trattamento;
- variazioni normative o variazioni alle norme o procedure interne per la sicurezza dei dati e dei trattamenti.

Tali interventi formativi possono avvenire sia internamente, a cura del Titolare del trattamento, del Responsabile della sicurezza dei dati personali, del Responsabile del trattamento oppure di altri soggetti esperti nella materia, sia esternamente presso soggetti specializzati.

Gli interventi formativi ed il piano di formazione sono coordinati e seguiti dal Responsabile dei Processi Formativi: **LEON FRANCESCA di COADIUVATA DA ING. MARTINI FABRIZIO**

In generale, i contenuti formativi riguardano la normativa vigente (Codice in materia di protezione di dati personali, Pareri ed Autorizzazioni del Garante per la Privacy, giurisprudenza di settore, ecc.) e le indicazioni operative da eseguire nell'espletamento delle varie mansioni.

Il calendario, il luogo di svolgimento e l'elenco dei partecipanti dei corsi con presenza frontale del docente sono stabiliti e definiti di volta.

Il calendario, il luogo di svolgimento e l'elenco dei partecipanti dei corsi svolti mediante supporti autodidattici (, ecc.) sono stabiliti e definiti di volta.

Segue una tabella per la pianificazione degli interventi formativi durante l'anno.



**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico al Responsabile dei Processi Formativi.**

In qualità di Responsabile della sicurezza del trattamento dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**LEON FRANCESCA**

di COADIUVATA DA ING. MARTINI FABRIZIO in incarico di **Responsabile dei Processi Formativi**.

Il Responsabile dei Processi Formativi ha il compito di:

- Verificare periodicamente e comunque non meno di una volta al mese la necessità di provvedere all'aggiornamento formativo degli incaricati e del responsabile del trattamento controllando le comunicazioni dell'Autorità Garante per la Privacy sul sito [www.garanteprivacy.it](http://www.garanteprivacy.it)
- Predisporre le sessioni di aggiornamento con materiale didattico adeguato

Il Responsabile dei Processi Formativi dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

Il Responsabile dei processi formativi  
LEON FRANCESCA

# Appendice C

## Analisi dei Rischi

L'analisi dei rischi è stata focalizzata sulle circostanze possibili o probabili che possano costituire il verificarsi di rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato e di trattamento non consentito o non conforme alle finalità della raccolta, indicati all'art. 31 del D.Lgs. 196/2003.

L'analisi dei rischi è stata ispirata alla verifica di linee guida e principi relativi ai concetti di:

- integrità: intesa come la gestione dell'accuratezza e completezza delle informazioni e delle relative applicazioni, la salvaguardia della esattezza dei dati, la difesa da manomissioni o modifiche non autorizzate, ecc;
- confidenzialità: o riservatezza, intesa come la garanzia che le informazioni siano accessibili solo alle persone autorizzate, la protezione delle trasmissioni, il controllo degli accessi, ecc.;
- disponibilità: intesa come l'assicurazione che l'accesso ai dati sia disponibile quando necessario, quindi la garanzia per gli utenti della fruibilità dei dati e dei servizi, evitando la loro perdita o riduzione.

Ad essi sono stati prudentemente aggiunte valutazioni di ulteriori possibili rischiosità in relazione a trattamenti che possono presentare specifici rischi riferendosi al trattamento dei dati diversi da quelli sensibili e giudiziari, ma che presentano (o possono presentare) rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare.

L'esame dei rischi è stato fatto anche in relazione alla natura dei dati, distinguendo tra i dati personali comuni e particolari (sensibili, giudiziari), ed in relazione alle caratteristiche del trattamento. I rischi esaminati sono stati individuati, classificati e descritti nei seguenti principali raggruppamenti:

- rischi ambientali,
- rischi sull'integrità dei dati,
- rischi sulla riservatezza dei dati, di trattamenti non consentiti o non conformi alle finalità della raccolta,
- rischi sulla disponibilità dei dati,
- rischi derivanti dall'accesso abusivo, di cui all'art. 615-ter del codice penale
- rischi specifici

### C.1 Rischi ambientali

Nella categoria dei rischi ambientali sono stati compresi, classificati ed esaminati, quei rischi che generalmente non trovano una valida protezione nei sistemi di difesa classici. In particolare, sono

considerati come rischi ambientali le minacce derivanti dalla collocazione territoriale del titolare del trattamento, l'ubicazione dei luoghi in cui vengono custoditi i dati e svolte le diverse operazioni di trattamento. In dettaglio si è verificato che:

- sotto l'aspetto dei rischi sismici, la Sede del titolare del trattamento e i locali dove avviene l'elaborazione dei dati, sono ubicate in fascia territoriale geografica che, come indicato nell'Ordinanza del Presidente del Consiglio dei Ministri n° 3274 del 20 marzo 2003, non risultano classificate tra le zone a grado di pericolosità elevato o medio. Di conseguenza non è necessario adottare ulteriori e specifiche misure di sicurezza per le strutture degli edifici, né per garantire la continuità degli approvvigionamento dei diversi servizi a tutela diretta o indiretta dei trattamenti e delle banche dati (telecomunicazioni, energia elettrica);
- non risultano, nelle vicinanze, insediamenti di impianti industriali o altre installazioni di aziende che svolgono attività pericolose.

In generale, non risultano quindi rischi ambientali prevedibili e probabili, correlati alla ubicazione geografica della sede del titolare del trattamento, che richiedano particolari cautele rispetto a quanto indicato di seguito.

## **C.2 Rischi sull'integrità dei dati**

L'analisi sulle minacce all'integrità dei dati ha riguardato soprattutto la protezione dei dati stessi dai rischi di possibili modifiche o distruzione accidentali o deliberate.// I rischi possibili individuati circa le minacce all'integrità dei dati sono:

- rischi di carattere accidentale;
- rischi di carattere volontario
- rischi derivanti da programmi di cui all'art. 615-quinquies del codice penale;

### **C.2.1 Rischi di carattere accidentale**

Riguardano l'involontaria sovrascrittura o alterazione dei dati imputabili ad azioni umane errate oppure a guasti delle apparecchiature dedicate alla memorizzazione. In particolare:

- malfunzionamenti hardware (es.: guasto dei dischi);
- deterioramento nel tempo dei supporti di memorizzazione e del mezzo fisico che li ospita;
- eventi disastrosi che superino i livelli ipotizzati all'atto della stesura delle contromisure.

### **C.2.2 Rischi di carattere volontario**

Sono considerate in questa categoria le alterazioni dell'integrità conseguenti ad una teorica azione deliberatamente perpetrata da un soggetto allo scopo di:

- modificare volontariamente i dati,
- inserire nuovi dati,
- distruggere i dati.

### **C.2.3 Rischi da programmi pericolosi**

I rischi connessi alla diffusione dei virus e dei programmi pericolosi di cui all'art. 615-quinquies del Codice Penale possono causare:

- corruzione dei files eseguibili e, a volte, dei dati;
- corruzione di documenti;
- perdita di files;
- cattivi funzionamenti del sistema;
- degrado delle prestazioni del sistema;
- impossibilità di utilizzo del sistema;
- rischi legali in violazione dell'art. 615-quinquies del codice penale;

Viene inoltre considerata la pericolosità di quei programmi (chiamati backdoor o hacktools) che consentono l'amministrazione remota dei sistemi in rete e possono essere installati sulle postazioni senza che l'operatore se ne accorga, e che una volta attivati consentono collegamenti via TCP/IP permettendo ad intrusi di manipolare e controllare varie funzioni del PC. Questi programmi, seppure non propriamente definibili virus o cavalli di Troia, sono generalmente identificati nella classe dei malware. I modi con cui i virus ed i programmi pericolosi possono penetrare nei computer del titolare del trattamento sono:

- tramite supporti infettati provenienti da terzi;
- tramite supporti infettati importati dai dipendenti senza l'autorizzazione dell'Ente;
- tramite files scambiati in rete per posta elettronica o scaricati da Internet.

## **C.3 Rischi sulla riservatezza dei dati**

Per quanto attiene alla riservatezza dei dati si è fatto riferimento alla natura ed al grado di confidenzialità, riservatezza e particolarità dei dati, al fine di proteggere le informazioni da eventuali comunicazioni non autorizzate, consentendone l'utilizzo ed il trattamento solamente ai soggetti incaricati dei trattamenti. Tale rischio è stato esaminato in relazione alla possibilità di una ipotetica comunicazione e/o diffusione di informazioni da parte di soggetti non autorizzati, ovvero in relazione ad accessi non autorizzati ai dati oggetto di trattamento.

### **C.3.1 Trattamenti non consentiti o non conformi alle finalità della raccolta**

Sono state ricercate le circostanze in cui possono essere svolti trattamenti di dati personali per i quali sia necessario un consenso informato da parte dell'interessato, e in cui il titolare del trattamento rischi involontariamente di svolgere trattamenti di dati senza disporre di tale consenso. L'attenzione è stata pertanto rivolta in particolare alle circostanze organizzative nelle quali, a causa di una possibile gestione non corretta dei consensi, si determinino trattamenti non conformi alle finalità per le quali i dati sono stati raccolti. Si è fatto riferimento alla natura ed al grado di confidenzialità, riservatezza e particolarità dei dati, al fine di garantire le informazioni da ipotetiche divulgazioni non autorizzate, consentendone l'utilizzo ed il trattamento solamente ai soggetti fisici incaricati dei trattamenti. In tale ambito è stata verificata anche la possibilità:

- che vengano svolti trattamenti in violazione della legge, e più in particolare in violazione delle misure minime di sicurezza di cui agli artt. 34 e 35;
- che i dati non rispettino i requisiti di cui all'art. 11 (liceità e correttezza dei trattamenti, legittimità degli scopi, esattezza, pertinenza, non eccedenza dei dati acquisiti, ecc.) e a tal fine sono state impartite opportune istruzioni agli incaricati.

### **C.3.2 Rischi di accessi non autorizzati**

Tale rischio è stato esaminato in relazione alla possibilità che si realizzino rilasci non autorizzati di informazioni e/o accessi non autorizzati ai dati. Il rischio di accessi non autorizzati è stato determinato sulla base delle seguenti fattispecie:

- rischi di accessi fraudolenti dall'interno;
- rischi di accessi fraudolenti dall'esterno;
- altri rischi di trattamento non autorizzato di dati personali.

#### **Rischi di accessi fraudolenti dall'interno**

Sono stati presi in considerazione rischi:

- dovuti a un profilo di autorizzazione all'accesso non aderente al ruolo assegnato, oppure causato dall'assegnazione di privilegi di accesso eccessivi;
- dovuti a inferenza, ossia alla cattura o conoscenza di informazioni che, correlate tra loro, consentono di giungere alla conoscenza indiretta di dati;
- dovuti ad utilizzo dei privilegi di amministratori di sistema per l'accesso ad archivi;
- dovuti a impersonificazione, ossia all'assunzione delle caratteristiche identificative di un dipendente autorizzato all'accesso ai sistemi;
- dovuti a manomissione delle autorizzazioni da parte del personale addetto al controllo ed all'amministrazione dei profili di accesso;
- dovuti a conoscenze dei punti deboli del sistema (es. banchi di sistema o di programmi).

#### **Rischi di accessi fraudolenti dall'esterno**

Sono stati presi in considerazione rischi:

- dovuti ad accessi tramite sistemi di collegamento remoto installati per la manutenzione o la trasmissione di software;
- dovuti a impersonificazione di un dipendente autorizzato all'accesso remoto ai sistemi;
- dovuti a intercettazione di comunicazioni telematiche;
- dovuti a conoscenza di punti deboli del sistema telematico (es. banchi di sistema o di programmi).

#### **Altri rischi di trattamento non autorizzato di dati personali**

Sono stati presi in considerazione rischi:

- consistenti nella comunicazione o diffusione non consentita, accidentale o volontaria, di dati, con o senza l'ausilio di mezzi elettronici, o altri trattamenti non consentiti o non conformi nella modalità o nella durata;
- dovuti ad ignoranza o non rispetto della normativa interna e/o della legislazione vigente;

## **C.4 Disponibilità dei dati**

Il concetto di disponibilità si riferisce alla necessità, e al conseguente diritto dei soggetti interessati, che i dati personali possano essere utilizzati in tutte le forme e le circostanze previste. Deve quindi essere assicurato che i dati siano disponibili al momento di una richiesta effettuata dai soggetti in possesso delle autorizzazioni necessarie. La disponibilità dei dati è posta anche in relazione agli utenti interni (incaricati) che debbono trattarli. I rischi di non disponibilità sono stati esaminati in relazione ad eventi di natura accidentale o intenzionale.



### **C.4.1 Rischi di natura accidentale**

In questa famiglia di rischi è stata compresa l'eventualità che le informazioni non siano disponibili a causa di eventi non volontari e/o non previsti, dovuti a:

- anomalie in programmi che avrebbero dovuto elaborare i dati e che non hanno potuto completare la loro esecuzione (p.e. a causa di interruzioni di procedure per input errati, o errori di realizzazione);
- errate azioni del personale incaricato, che impediscono l'accesso alle informazioni (p.e. mancata copia di un archivio o mancato montaggio di un supporto);
- malfunzionamento dell'hardware (p.e. guasti alle unità di elaborazione, di memorizzazione o di trasmissione);
- dimensionamento non sufficiente delle risorse tecnologiche deputate alla trasmissione ed alla memorizzazione.

### **C.4.2 Rischi di natura intenzionale**

Rientrano in questa tipologia di rischi le fattispecie in cui le informazioni non siano disponibili a causa di azioni umane volontarie, poste in essere con lo scopo preciso e determinato di impedire l'accesso alle informazioni da parte dei soggetti che ne hanno il diritto. Tali minacce sono state ipoteticamente relazionate a:

- generica infedeltà o comunque, negligenza e/o disobbedienza del personale addetto al controllo ed alla amministrazione delle informazioni;
- danneggiamento o manomissione delle attrezzature e/o delle connessioni da parte di dipendenti o di terzi;
- attacchi di tipo denial of service.

### **C.4.3 Rischi derivanti da accessi abusivi**

I rischi connessi all'accesso abusivo a un sistema informatico o telematico di cui all'art. 615-ter del Codice Penale possono comportare tutti precedenti rischi che gravano sulla integrità, disponibilità e riservatezza dei dati trattati. In particolare, si considerano abusivi quegli accessi che avvengano nelle seguenti circostanze che 1) il sistema sia protetto, 2) l'accesso sia abusivo, 3) l'eventuale intruso nel sistema si tratti in esso senza averne il diritto, contrariamente alla volontà di chi ha il diritto di escluderlo. Gli accessi abusivi considerati riguardano sia chi potrebbe penetrare illecitamente nel sistema, o in parte di esso, dall'interno dell'azienda (insider), sia chi si introduce dall'esterno dell'organizzazione aziendale (hacker). Gli accessi abusivi comportano sia rischi connessi alle violazioni di legge, sia altri rischi diretti e indiretti di tipo tecnico, operativo, legale e di reputazione dell'azienda colpita. Più analiticamente tali rischi riguardano:

- conoscenza dei dati da parte di persone non autorizzate;
- distruzione e perdita totale o parziale dei dati;
- danneggiamento dei dati;
- diffusione di documenti, comuni e riservati;
- negazione del servizio agli utenti;
- impossibilità di svolgere operazioni di trattamento;
- diffusione di programmi informatici infetti;
- malfunzionamento di programmi;

- rallentamento delle capacità del sistema;
- perdita di tempo;
- pubblicazione di notizie nocive all'immagine e reputazione dell'azienda;
- sequestro di mezzi informatici;
- risarcimento del danno;
- violazioni di leggi e regolamenti.

Tra le principali circostanze che favoriscono gli accessi abusivi e i rischi precedentemente elencati, si è considerato, pur se in linea teorica, che tali rischi possono verificarsi soprattutto in presenza di una o più delle seguenti criticità.

1. Il sistema informatico deve essere configurato in maniera tale da consentire l'accesso solo tramite parole chiave associate a codici identificativi personali, ma nel caso non sia riservata la dovuta attenzione alla robustezza delle chiavi ed ai criteri di composizione dei codici identificativi, potrà accadere che i codici siano ricavabili e le parole chiave calcolabili in breve tempo. Perciò tutti i sistemi protetti da parole chiave deboli (o addirittura predefinite) sono facilmente attaccabili.
2. I sistemi telematici funzionano e comunicano tra loro attraverso canali di comunicazione che, all'ingresso del cosiddetto domicilio informatico del proprio sistema, assumono il nome di porta. Le porte sono numerose ed hanno precise funzioni. Molti utenti ne ignorano l'esistenza e le lasciano attive, cioè aperte, anche quando non sono necessarie per i propri motivi di lavoro. Queste porte, involontariamente lasciate aperte, costituiscono una delle maggiori criticità, quindi rappresentano potenziali vulnerabilità del sistema da correggere.
3. Gli accessi abusivi a un sistema protetto sono facilitati dalle debolezze del sistema, dalle cosiddette vulnerabilità. Le vulnerabilità possono riguardare i sistemi operativi, i protocolli, le applicazioni, qualunque software in genere, il sistema fisico, il sistema delle trasmissioni. Le vulnerabilità, se sfruttate, danno origine a diverse tipologie d'attacco; le più comuni individuate nell'analisi dei rischi, specialmente in ambiente web, riguardano:
  - (a) Rischi da ricerca delle password  
Sono metodi che consistono nel trovare i codici d'accesso o parti di esso, anche mediante l'utilizzo di dizionari o programmi automatizzati detti tools a forza bruta. Questi programmi permettono di provare mediante elaborazione milioni di combinazioni di caratteri. Le parole chiave possono essere individuate anche con altri metodi privi di violenza sulla cose, come il metodo comunemente detto dell'ingegneria sociale.
  - (b) Rischi da intercettazione di dati  
Il metodo consiste nel tentativo di intercettare i dati, o meglio i cosiddetti pacchetti scambiati nella rete. Se un pacchetto è intercettato e copiato sarà possibile ricavarne molte informazioni, tra esse l'identificativo del server di trasmissione, il nome dell'utente e la password ad esso associata.
  - (c) Rischi da ricerca di file con accesso privilegiato  
Si tratta di un tipologia di attacco indirizzata a reti con sistemi operativi che nell'ambito delle possibilità gestionali prevedono meccanismi di accesso privilegiato al sistema.
  - (d) Rischi da azioni verso il protocollo ip  
Si tratta di metodi finalizzati ad ottenere il dirottamento dei dati in transito sulla rete sotto forma di pacchetti IP verso false destinazioni simulando (impersonificando) un host di destinazione.
  - (e) Rischi da dirottamento di sessioni  
Sono una variante degli attacchi al protocollo IP, finalizzata all'esportazione di dati dal flusso di pacchetti.

(f) Rischi da sostituzione delle librerie condivise

Una libreria condivisa è costituita da un gruppo di funzioni che il sistema operativo assume su richiesta di un programma informatico. L'attacco consiste nel sostituire le librerie ufficiali con nuove funzioni modificate di proposito che permettono l'intrusione nel sistema.

## C.5 Altri specifici rischi

L'art. 17 del Codice prevede particolari aspetti di tutela per quei dati, diversi da quelli sensibili e giudiziari il cui trattamento ... presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare. Tale trattamento ... è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti. Detti accorgimenti ... sono prescritti dal Garante in applicazione dei principi sanciti dal presente Codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare. Tale categoria di dati non sono oggetto di trattamento.

## C.6 Riepilogo dell'analisi dei rischi

L'analisi dei rischi è stata svolta considerando gli eventi che possono condurre al verificarsi dei macro-rischi indicati dall'art. 31 del D.Lgs. 196/03, ovvero i rischi di

- distruzione o perdita, anche accidentale, dei dati stessi
- accesso non autorizzato
- trattamento non consentito o non conforme alle finalità della raccolta.

La valutazione del rischio è stata fatta con riferimento al rischio residuo. A ciascun rischio è stato attribuito un valore (basso, medio o alto) valutato di volta in volta sulla base delle seguenti soglie di rischio relative alla probabilità di accadimento e e all'eventuale impatto dell'evento (gravità stimata):

### SOGLIA DI RISCHIO

| INDICE | DESCRIZIONE   |
|--------|---|
| BASSO  | Con questa soglia viene individuato un rischio che, in relazione alle misure di sicurezza adottate, risulta essere molto basso con una minaccia remota e comunque rapidamente reversibile ed ovviabile.   |
| MEDIO  | Con questa soglia viene individuato un rischio superiore al precedente e che, in relazione alle misure di sicurezza adottate, identifica una minaccia remota ma i cui effetti non sono totalmente o parzialmente reversibili od ovviabili. In tal caso è opportuno individuare degli accorgimenti per contenere il rischio. |
| ALTO   | Con questa soglia viene individuato un rischio elevato che, anche in relazione alle misure di sicurezza adottate, identifica una minaccia non remota e i cui effetti non sono totalmente o parzialmente reversibili od ovviabili. . In tal caso è opportuno individuare immediate misure correttive.                        |

L'esame dei rischi è stato effettuato anche in relazione alla natura dei dati, distinguendo tra i dati personali comuni e quelli sensibili e giudiziari e alle caratteristiche del trattamento.

I tre macro-rischi sono stati valutati tramite l'analisi di una serie di eventi tramite i quali potrebbero concretizzarsi i macro-rischi stessi. Per ciascun evento sono stati valutati qualitativamente il massimo impatto possibile e la probabilità di accadimento, usando lo stesso modello e le stesse scale di valutazione a cinque valori applicate per l'analisi dei rischi aziendali.

In tale modello, i valori attribuibili all'impatto sono: Basso, Moderato, Rilevante.

I valori attribuibili alla probabilità sono: Rara, Possibile, Quasi certa.

I valori attribuiti al rischio sono: Basso, Medio, Alto.

La valutazione è stata condotta mediante valutazioni separate di impatto e probabilità. A partire da tali valutazioni stato attribuito il livello di rischio, secondo il seguente schema:

|                   | Probabilità rara | Probabilità possibile | Probabilità quasi certa |
|-------------------|------------------|-----------------------|-------------------------|
| Impatto basso     | Rischio basso    | Rischio basso         | Rischio medio           |
| Impatto moderato  | Rischio basso    | Rischio medio         | Rischio alto            |
| Impatto rilevante | Rischio medio    | Rischio alto          | Rischio alto            |

Nel seguito sono riportati i modelli descrittivi per le tre tipologie di rischio: comportamenti degli operatori, eventi relativi agli strumenti, eventi relativi al contesto. Per ogni rischio specifico sono descritte le contromisure adottate.

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**ANALISI DEI RISCHI RELATIVI AI COMPORTAMENTI DEGLI OPERATORI**

- Il rischio relativo a **SOTTRAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE** è applicabile.  
L'impatto di tale rischio sulla sicurezza attualmente è basso.  
Le misure adottate, in base alle valutazioni dell'impatto sulla sicurezza del trattamento, sono:
  1. custodia delle credenziali mediante buste
  2. istruzioni scritte al personale che utilizza gli elaboratori
- Il rischio relativo a **DISATTENZIONE O INCURIA** è applicabile.  
L'impatto di tale rischio sulla sicurezza attualmente è basso.  
Le misure adottate, in base alle valutazioni dell'impatto sulla sicurezza del trattamento, sono:
  1. back-up degli archivi
  2. incarichi per amministratori di sistema
- Il rischio relativo a **COMPORTAMENTI SLEALI O FRAUDOLENTI** è applicabile.  
L'impatto di tale rischio sulla sicurezza attualmente è basso.  
Le misure adottate, in base alle valutazioni dell'impatto sulla sicurezza del trattamento, sono:
  1. sensibilizzazione di personale e collaboratori mediante lettere di incarico
  2. regolamenti e codici etici
  3. nomina dei fiduciari per la posta elettronica
  4. adozione del Provvedimento del Garante del 27-11-2008 per le funzioni di Amministratore di sistema
- Il rischio relativo a **ERRORE SISTEMATICO** è applicabile.  
L'impatto di tale rischio sulla sicurezza attualmente è basso.  
Le misure adottate, in base alle valutazioni dell'impatto sulla sicurezza del trattamento, sono:
  1. revisione e monitoraggio delle procedure
  2. back-up archivi

---

Il Titolare del trattamento  
D'ACRI ANTONIO MARCO

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**ANALISI DEI RISCHI CONNESSI AD EVENTI RELATIVI AGLI STRUMENTI**

- Il rischio relativo a **AZIONI DI VIRUS INFORMATICI O DI PROGRAMMI SUSCETTIBILI DI RECARE DANNO** è applicabile.  
L'impatto di tale rischio sulla sicurezza attualmente è basso.  
Le misure adottate, in base alle valutazioni dell'impatto sulla sicurezza del trattamento, sono:
  1. uso di sistema antivirus su ogni elaboratore
  2. NORTON ANTIVIRUS
  - 3.
  4. NORTON ANTIVIRUS
  - 5.
  6. NORTON ANTIVIRUS
  - 7.
  8. NORTON ANTIVIRUS
- Il rischio relativo a **AZIONI DI SPAMMING, SPYWARE, MALWARE O TECNICHE DI SABOTAGGIO** è applicabile.  
L'impatto di tale rischio sulla sicurezza attualmente è basso.  
Le misure adottate, in base alle valutazioni dell'impatto sulla sicurezza del trattamento, sono:
  1. uso di filtri antispam sulla posta in uscita
  2. uso di programmi anti-spyware
  3. uso di log per accessi e operazioni
  4. NORTON ANTIVIRUS
  - 5.
  6. NORTON ANTIVIRUS
- Il rischio relativo a **MALFUNZIONAMENTO, INDISPONIBILITÀ O DEGRADO DEGLI STRUMENTI** è applicabile.  
L'impatto di tale rischio sulla sicurezza attualmente è basso.  
Le misure adottate, in base alle valutazioni dell'impatto sulla sicurezza del trattamento, sono:
  1. assistenza e manutenzione fornita da azienda informatica esterna
  2. utilizzo di UPS per prevenire problematiche di tipo elettrico
  3. ESISTONO GRUPPI UPS
  4. TUTTI GLI ELABORATORI (SERVER E WORKSTATION) SONO PROTETTI
  - 5.
  6. ESISTONO GRUPPI UPS
  7. TUTTI GLI ELABORATORI (SERVER E WORKSTATION) SONO PROTETTI
- Il rischio relativo a **ACCESSI ESTERNI NON AUTORIZZATI SULLA RETE O SUGLI ELABORATORI INFORMATICI** è applicabile.  
L'impatto di tale rischio sulla sicurezza attualmente è rilevante-basso.  
Le misure adottate, in base alle valutazioni dell'impatto sulla sicurezza del trattamento, sono:
  1. uso di sistema firewall con intrusion detection system
  2. uso di credenziali di autenticazione, ruotate periodicamente secondo la normativa vigente

3. adozione delle procedure previste dal Provvedimento del Garante del 13-10-2008 per riciclaggio e smaltimento di supporti contenenti dati personali
  4. uso di dispositivi mobili appositamente protetti
  5. connettori remote per assistenza e manutenzione solo su richiesta ed autorizzazione dell'utente, all'interno della rete
- Il rischio relativo a **INTERCETTAZIONI DI INFORMAZIONI IN RETE** è applicabile.  
L'impatto di tale rischio sulla sicurezza attualmente è basso.  
Le misure adottate, in base alle valutazioni dell'impatto sulla sicurezza del trattamento, sono:
    1. uso di trasmissioni crittografate per connessioni VPN
    2. uso di firewall
    3. connettori remote per assistenza e manutenzione solo su richiesta ed autorizzazione dell'utente, all'interno della rete

---

Il Titolare del trattamento  
D'ACRI ANTONIO MARCO

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**ANALISI DEI RISCHI CONNESSI AD EVENTI RELATIVI AL CONTESTO**

- Il rischio relativo a **ACCESSI NON AUTORIZZATI A LOCALI/REPARTI AD ACCESSO RISTRETTO** è applicabile.  
L'impatto di tale rischio sulla sicurezza attualmente è moderato-basso.  
La misura adottata, in base alle valutazioni dell'impatto sulla sicurezza del trattamento, è:
  1. locali dotati di serrature sulle porte di ingresso, regolarmente chiusi in assenza del personale autorizzato
- Il rischio relativo a **SOTTRAZIONE DI STRUMENTI E ARCHIVI CONTENENTI DATI** è applicabile.  
L'impatto di tale rischio sulla sicurezza attualmente è moderato-basso.  
La misura adottata, in base alle valutazioni dell'impatto sulla sicurezza del trattamento, è:
  1. utilizzo di armadi, cassetti o contenitori con serratura
- Il rischio relativo a **EVENTI DISTRUTTIVI, NATURALI O ARTIFICIALI, NONCHÉ DOLOSI, ACCIDENTALI O DOVUTI AD INCURIA** è applicabile.  
L'impatto di tale rischio sulla sicurezza attualmente è basso.  
In base alle valutazioni dell'impatto sulla sicurezza non sono previste misure preventive.
- Il rischio relativo a **GUASTO AI SISTEMI COMPLEMENTARI (IMPIANTO ELETTRICO, CLIMATIZZAZIONE, ECC.)** è applicabile.  
L'impatto di tale rischio sulla sicurezza attualmente è basso.  
Le misure adottate, in base alle valutazioni dell'impatto sulla sicurezza del trattamento, sono:
  1. impianti a norma di legge
  2. controlli periodici agli impianti
  3. adozione delle misure indicate da D.Lgs.81/08
- Il rischio relativo a **ERRORI UMANI NELLA GESTIONE DELLA SICUREZZA FISICA** è applicabile.  
L'impatto di tale rischio sulla sicurezza attualmente è basso.  
La misura adottata, in base alle valutazioni dell'impatto sulla sicurezza del trattamento, è:
  1. adozione delle misure indicate da D.Lgs.81/08

---

Il Titolare del trattamento  
D'ACRI ANTONIO MARCO



## Appendice D

# Lettere di Incarico

Seguono le lettere di incarico per

- Titolare del trattamento
- Responsabile/i del trattamento
- Incaricato/i del trattamento
- Addetto/i al controllo dei locali

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Titolare del trattamento dei dati personali.**

Ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplina-  
re tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03),  
siccome l'attività compete a persona giuridica, il Titolare del trattamento è l'enti-  
tà nel suo complesso nella persona di:

**D'ACRI ANTONIO MARCO**

Il Titolare del trattamento ha il compito di

- Individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più Responsabili della sicurezza del trattamento con il compito di garantire la sicurezza del trattamento dei dati personali.
- Verificare e controllare l'operato dei Responsabili nell'adempimento dei loro compiti.

Qualora il Titolare del Trattamento ritenga di non nominare alcun Responsabile della sicurezza trattamento, ne assumerà tutte le responsabilità e funzioni.

Il Titolare del Trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

19/05/2014

Il Titolare del trattamento  
D'ACRI ANTONIO MARCO

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Dichiarazione sulla titolarità dei trattamenti.**

In qualità di Titolare del trattamento dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03), del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03) si dichiara che:

**BANCA SELLA**

è un titolare autonomo e indipendente, ai sensi dell'art. 28 del Codice, per quanto riguarda i dati personali trattati nei servizi e prodotti di cui la scrivente usufruisce nella propria attività, in particolare per i seguenti trattamenti:

|                              |  |
|------------------------------|--|
| <b>Nome</b>                  | <b>Incassi, pagamenti e operazioni bancarie</b>  |
| <b>Riguarda</b>              | Estratti conti, bonifici, assegni, versamenti, riba, rid, ecc.                                       |
| <b>Tipologia di dati</b>     | Dati personali   |
| <b>Categoria interessati</b> | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |

Il titolare del trattamento  
D'ACRI ANTONIO MARCO

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Dichiarazione sulla titolarità dei trattamenti.**

In qualità di Titolare del trattamento dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03), del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03) si dichiara che:

**LEGAL MAIL**

è un titolare autonomo e indipendente, ai sensi dell'art. 28 del Codice, per quanto riguarda i dati personali trattati nei servizi e prodotti di cui la scrivente usufruisce nella propria attività, in particolare per i seguenti trattamenti:

|                              |  |
|------------------------------|--|
| <b>Nome</b>                  | <b>Posta elettronica certificata</b>                                 |
| <b>Riguarda</b>              | Mittente, destinatari, contenuto delle e-mail certificate            |
| <b>Tipologia di dati</b>     | Dati personali eventualmente sensibili                               |
| <b>Categoria interessati</b> | Clienti, fornitori, lavoratori, terzi identificati ed identificabili |

Il titolare del trattamento  
D'ACRI ANTONIO MARCO

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Dichiarazione sulla titolarità dei trattamenti.**

In qualità di Titolare del trattamento dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03), del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03) si dichiara che:

**UNICREDIT BANCA**

è un titolare autonomo e indipendente, ai sensi dell'art. 28 del Codice, per quanto riguarda i dati personali trattati nei servizi e prodotti di cui la scrivente usufruisce nella propria attività, in particolare per i seguenti trattamenti:

|                              |  |
|------------------------------|--|
| <b>Nome</b>                  | <b>Incassi, pagamenti e operazioni bancarie</b>  |
| <b>Riguarda</b>              | Estratti conti, bonifici, assegni, versamenti, riba, rid, ecc.                                       |
| <b>Tipologia di dati</b>     | Dati personali   |
| <b>Categoria interessati</b> | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |

Il titolare del trattamento  
D'ACRI ANTONIO MARCO

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico al Responsabile della sicurezza dei dati personali.**

In qualità di Titolare del trattamento dei dati personali, ai sensi dell'art.29 del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**LEON FRANCESCA**

l'incarico di **Responsabile della sicurezza dei dati personali** .

Il Responsabile della sicurezza dei dati personali ha il compito di

- Garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
- Redigere ed aggiornare ad ogni variazione l'elenco delle sedi e locali in cui sono trattati i dati.
- Redigere ed aggiornare ad ogni variazione l'elenco delle banche dati oggetto di trattamento.
- Decidere se affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.
- Nominare e incaricare per iscritto, in relazione all'attività svolta, se lo ritiene opportuno, uno o più Responsabili del trattamento con il compito di individuare e incaricare gli Incaricati del trattamento dei dati personali e di organizzare e sovraintendere alle operazioni di trattamento.
- Nominare e incaricare per iscritto, in relazione all'attività svolta, gli Incaricati del trattamento dei dati personali.
- Qualora il trattamento dei dati sia stato affidato in tutto o in parte all'esterno della struttura del titolare controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
- Se il trattamento è effettuato con mezzi informatici, nominare e incaricare per iscritto, in relazione all'attività svolta, se lo ritiene opportuno, uno o più Responsabili della gestione della strumentazione elettronica.
- Se il trattamento è effettuato con mezzi informatici, redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Responsabili della gestione e della manutenzione degli strumenti elettronici.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, in relazione all'attività svolta, se lo ritiene opportuno, uno o più Amministratori di sistema.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati della custodia delle copie delle credenziali qualora vi sia più di un incaricato del trattamento.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati delle copie di sicurezza delle banche dati.
- Intraprendere idonee misure per custodire e conservare i supporti utilizzati per le copie dei dati.
- Definire e successivamente verificare con cadenza semestrale le modalità di accesso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia ed accessibilità come specificato in seguito.

- Periodicamente, e comunque almeno annualmente, verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione dei responsabili e degli incaricati del trattamento dei dati personali.

Il Responsabile della sicurezza dei dati personali dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Titolare del trattamento  
D'ACRI ANTONIO MARCO

Il Responsabile della sicurezza  
dei dati personali  
per accettazione  
LEON FRANCESCA

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**ARUGA MARCO**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **ABBONAMENTO MUSEI + CARD** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, casseti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
ARUGA MARCO



**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**BARAVELLI CRISTINA**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **C/O INFOPIEMONTE - FRONT OFFICE - AREA OPERATIVA** della sede denominata **C/O PALAZZO DELLA REGIONE**
- al locale definito **CALL CENTER** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, cassetti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
BARAVELLI CRISTINA

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**BERTERO LUCA**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **C/O INFOPIEMONTE - FRONT OFFICE - AREA OPERATIVA** della sede denominata **C/O PALAZZO DELLA REGIONE**
- al locale definito **CALL CENTER** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, cassetti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
BERTERO LUCA

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**BORGARO CHIARA**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **C/O INFOPIEMONTE - FRONT OFFICE - AREA OPERATIVA** della sede denominata **C/O PALAZZO DELLA REGIONE**
- al locale definito **CALL CENTER** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, cassetti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
BORGARO CHIARA

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**CAGNASSO MAGDA**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **AMMINISTRAZIONE** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, cassetti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
CAGNASSO MAGDA

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**COCCIARDI STEFANO**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **C/O INFOPIEMONTE - FRONT OFFICE - AREA OPERATIVA** della sede denominata **C/O PALAZZO DELLA REGIONE**
- al locale definito **CALL CENTER** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, cassetti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
COCCIARDI STEFANO

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**CORREALE AMALIA**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **AMMINISTRAZIONE** della sede denominata **SEDE OPERATIVA**
- al locale definito **ARCHIVIO** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, cassetti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
CORREALE AMALIA

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**D'ACRI ANTONIO MARCO**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **AREA SERVER** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, cassetti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
D'ACRI ANTONIO MARCO

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**EYNARD SIMONE FLAVIO**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **C/O INFOPIEMONTE - FRONT OFFICE - AREA OPERATIVA** della sede denominata **C/O PALAZZO DELLA REGIONE**
- al locale definito **CALL CENTER** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, cassetti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
EYNARD SIMONE FLAVIO



**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**IACOBONE PASQUALE**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **C/O INFOPIEMONTE - FRONT OFFICE - AREA OPERATIVA** della sede denominata **C/O PALAZZO DELLA REGIONE**
- al locale definito **CALL CENTER** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, cassetti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
IACOBONE PASQUALE

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**LEON FRANCESCA**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **ARCHIVIO** della sede denominata **SEDE OPERATIVA**
- al locale definito **DIREZIONE** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, cassetti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
LEON FRANCESCA

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**MAUTINO ROBERTO**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **MAGAZZINO/ARCHIVIO** della sede denominata **MAGAZZINO / ARCHIVIO**
- al locale definito **ARCHIVIO STORICO** della sede denominata **SEDE OPERATIVA**
- al locale definito **SEGRETERIA GENERALE / ABBONAMENTO MUSEI** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, cassetti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
MAUTINO ROBERTO

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**PEPE ANNARITA**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **MAGAZZINO/ARCHIVIO** della sede denominata **MAGAZZINO / ARCHIVIO**
- al locale definito **ABBONAMENTO MUSEI + CARD** della sede denominata **SEDE OPERATIVA**
- al locale definito **ARCHIVIO** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, casseti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
PEPE ANNARITA

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**PINTOR RENATA**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **MAGAZZINO/ARCHIVIO** della sede denominata **MAGAZZINO / ARCHIVIO**
- al locale definito **AMMINISTRAZIONE** della sede denominata **SEDE OPERATIVA**
- al locale definito **ARCHIVIO** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, cassetti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
PINTOR RENATA

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**RICCI SIMONA**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **DIREZIONE** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, casseti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
RICCI SIMONA

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**SERRA ELEONORA**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **MAGAZZINO/ARCHIVIO** della sede denominata **MAGAZZINO / ARCHIVIO**
- al locale definito **SEGRETERIA GENERALE / ABBONAMENTO MUSEI** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, cassetti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
SERRA ELEONORA

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Addetto al controllo dei locali.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**VITRANI PAOLO**

l'incarico di controllare direttamente i sistemi e le apparecchiature di accesso

- al locale definito **C/O INFOPIEMONTE - FRONT OFFICE - AREA OPERATIVA** della sede denominata **C/O PALAZZO DELLA REGIONE**
- al locale definito **CALL CENTER** della sede denominata **SEDE OPERATIVA**

allo scopo di impedire intrusioni o danneggiamenti.

L'incarico non corrisponde ad una responsabilità oggettiva circa eventuali mancanze organizzative o strutturali, che invece sono a carico del Responsabile e del Titolare del trattamento, bensì rappresenta una richiesta di coinvolgimento dell'addetto, volto alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

L'Addetto al controllo dei locali dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a:

- Quando presente nei locali che gli sono stati affidati in custodia, impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, di un locale.
- Quando presente nei locali che gli sono stati affidati in custodia, impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento.
- Quando presente nei locali che gli sono stati affidati in custodia, identificare e registrare i soggetti ammessi dopo l'orario di chiusura dei locali stessi.
- Conservare i documenti contenenti i dati sensibili e giudiziari in contenitori (stanze, armadi, cassetti, scatole, ecc.) muniti di serratura.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Addetto al controllo dei locali  
per accettazione  
VITRANI PAOLO



## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**BARAVELLI CRISTINA**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |   |
|---|---|
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p>   |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p> |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>  |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati istituzioni</b><br/>Dati relativi alle istituzioni con cui sussistono dei legami</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>  |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati sistema prenotazione musei</b><br/>Dati relativi ai servizi di prenotazione musei</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>   |

|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Fornitori e potenziali fornitori<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Clienti e potenziali clienti<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b>   | <b>Incassi, pagamenti e operazioni bancarie</b><br>Estratti conti, bonifici, assegni, versamenti, riba, rid, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |
| <b>Modalità di trattamento</b><br><b>Permessi*</b>   | Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sistema di gestione della protezione del trattamento di dati</b><br>Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)                             |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sistema di gestione della sicurezza sul lavoro</b><br>Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Supporti cartacei<br>C   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sito web</b><br>Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Terzi identificati e identificabili<br>Strumenti elettronici<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Spedizione e ricezione di documenti e materiale</b><br>Documenti di trasporto, indirizzari, ecc.<br>Dati personali<br>Clienti e fornitori<br>Strumenti elettronici e non<br>C  |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I inserimento, raccolta, registrazione
- C archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A annullamento, blocco, cancellazione, distruzione
- T trasporto/trasferimento
- N solo conservazione dei supporti, senza accesso ai contenuti
- D diffusione
- X equivalente ai permessi ICMAT
- L modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
BARAVELLI CRISTINA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**BERTERO LUCA**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |   |
|---|---|
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p>   |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p> |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>  |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati istituzioni</b><br/>Dati relativi alle istituzioni con cui sussistono dei legami</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>  |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati sistema prenotazione musei</b><br/>Dati relativi ai servizi di prenotazione musei</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>   |

|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Fornitori e potenziali fornitori<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Clienti e potenziali clienti<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b>   | <b>Incassi, pagamenti e operazioni bancarie</b><br>Estratti conti, bonifici, assegni, versamenti, riba, rid, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |
| <b>Modalità di trattamento</b><br><b>Permessi*</b>   | Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sistema di gestione della protezione del trattamento di dati</b><br>Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)                             |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sistema di gestione della sicurezza sul lavoro</b><br>Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Supporti cartacei<br>C   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sito web</b><br>Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Terzi identificati e identificabili<br>Strumenti elettronici<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Spedizione e ricezione di documenti e materiale</b><br>Documenti di trasporto, indirizzari, ecc.<br>Dati personali<br>Clienti e fornitori<br>Strumenti elettronici e non<br>C  |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I inserimento, raccolta, registrazione
- C archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A annullamento, blocco, cancellazione, distruzione
- T trasporto/trasferimento
- N solo conservazione dei supporti, senza accesso ai contenuti
- D diffusione
- X equivalente ai permessi ICMAT
- L modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
BERTERO LUCA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**BORGARO CHIARA**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |   |
|---|---|
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b></p> <p>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b></p> <p>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p> |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati associati</b></p> <p>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>  |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati istituzioni</b></p> <p>Dati relativi alle istituzioni con cui sussistono dei legami</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>  |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati sistema prenotazione musei</b></p> <p>Dati relativi ai servizi di prenotazione musei</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |

|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Fornitori e potenziali fornitori<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Clienti e potenziali clienti<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b>   | <b>Incassi, pagamenti e operazioni bancarie</b><br>Estratti conti, bonifici, assegni, versamenti, riba, rid, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |
| <b>Modalità di trattamento</b><br><b>Permessi*</b>   | Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sistema di gestione della protezione del trattamento di dati</b><br>Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)                             |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sistema di gestione della sicurezza sul lavoro</b><br>Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Supporti cartacei<br>C   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sito web</b><br>Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Terzi identificati e identificabili<br>Strumenti elettronici<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Spedizione e ricezione di documenti e materiale</b><br>Documenti di trasporto, indirizzari, ecc.<br>Dati personali<br>Clienti e fornitori<br>Strumenti elettronici e non<br>C  |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:



- I inserimento, raccolta, registrazione
- C archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A annullamento, blocco, cancellazione, distruzione
- T trasporto/trasferimento
- N solo conservazione dei supporti, senza accesso ai contenuti
- D diffusione
- X equivalente ai permessi ICMAT
- L modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
BORGARO CHIARA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**COCCIARDI STEFANO**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |   |
|---|---|
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p>   |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p> |
| <p><b>Nome</b><br/><b>Riguarda</b><br/><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p>    | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>  |
| <p><b>Nome</b><br/><b>Riguarda</b><br/><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p>    | <p><b>Banca dati istituzioni</b><br/>Dati relativi alle istituzioni con cui sussistono dei legami</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>  |
| <p><b>Nome</b><br/><b>Riguarda</b><br/><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p>    | <p><b>Banca dati sistema prenotazione musei</b><br/>Dati relativi ai servizi di prenotazione musei</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>   |

|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Fornitori e potenziali fornitori<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Clienti e potenziali clienti<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b>   | <b>Incassi, pagamenti e operazioni bancarie</b><br>Estratti conti, bonifici, assegni, versamenti, riba, rid, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |
| <b>Modalità di trattamento</b><br><b>Permessi*</b>   | Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sistema di gestione della protezione del trattamento di dati</b><br>Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)                             |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sistema di gestione della sicurezza sul lavoro</b><br>Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Supporti cartacei<br>C   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sito web</b><br>Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Terzi identificati e identificabili<br>Strumenti elettronici<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Spedizione e ricezione di documenti e materiale</b><br>Documenti di trasporto, indirizzari, ecc.<br>Dati personali<br>Clienti e fornitori<br>Strumenti elettronici e non<br>C  |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I inserimento, raccolta, registrazione
- C archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A annullamento, blocco, cancellazione, distruzione
- T trasporto/trasferimento
- N solo conservazione dei supporti, senza accesso ai contenuti
- D diffusione
- X equivalente ai permessi ICMAT
- L modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
COCCIARDI STEFANO

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**EYNARD SIMONE FLAVIO**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |  |
|---|--|
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p> |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>  |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati istituzioni</b><br/>Dati relativi alle istituzioni con cui sussistono dei legami</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>  |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati sistema prenotazione musei</b><br/>Dati relativi ai servizi di prenotazione musei</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Cartelle sanitarie di rischio dei lavoratori soggetti a sorveglianza sanitaria</b>  |
| <b>Riguarda</b>                | Visite ed esami di medicina del lavoro svolte dai lavoratori soggetti  |
| <b>Tipologia di dati</b>       | Dati sensibili   |
| <b>Categoria interessati</b>   | Lavoratori, dipendenti, soci, amministratori, collaboratori  |
| <b>Modalità di trattamento</b> | Supporti cartacei  |
| <b>Permessi*</b>               | T  |
| <b>Nome</b>                    | <b>Gestione acquisti e approvvigionamenti</b>  |
| <b>Riguarda</b>                | Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Fornitori e potenziali fornitori   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Gestione della clientela</b>  |
| <b>Riguarda</b>                | Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing                                      |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti e potenziali clienti   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Incassi, pagamenti e operazioni bancarie</b>  |
| <b>Riguarda</b>                | Estratti conti, bonifici, assegni, versamenti, riba, rid, ecc.   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili                                     |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Sistema di gestione della protezione del trattamento di dati</b>  |
| <b>Riguarda</b>                | Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03) |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Sistema di gestione della sicurezza sul lavoro</b>  |
| <b>Riguarda</b>                | Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)  |
| <b>Modalità di trattamento</b> | Supporti cartacei  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Sito web</b>  |
| <b>Riguarda</b>                | Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.              |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Spedizione e ricezione di documenti e materiale</b>   |
| <b>Riguarda</b>                | Documenti di trasporto, indirizzari, ecc.  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti e fornitori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I inserimento, raccolta, registrazione
- C archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A annullamento, blocco, cancellazione, distruzione
- T trasporto/trasferimento
- N solo conservazione dei supporti, senza accesso ai contenuti
- D diffusione
- X equivalente ai permessi ICMAT
- L modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
EYNARD SIMONE FLAVIO

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**IACOBONE PASQUALE**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |   |
|---|---|
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p>   |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p> |
| <p><b>Nome</b><br/><b>Riguarda</b><br/><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p>    | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>  |
| <p><b>Nome</b><br/><b>Riguarda</b><br/><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p>    | <p><b>Banca dati istituzioni</b><br/>Dati relativi alle istituzioni con cui sussistono dei legami</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>  |
| <p><b>Nome</b><br/><b>Riguarda</b><br/><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p>    | <p><b>Banca dati sistema prenotazione musei</b><br/>Dati relativi ai servizi di prenotazione musei</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>   |



|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Fornitori e potenziali fornitori<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Clienti e potenziali clienti<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b>   | <b>Incassi, pagamenti e operazioni bancarie</b><br>Estratti conti, bonifici, assegni, versamenti, riba, rid, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |
| <b>Modalità di trattamento</b><br><b>Permessi*</b>   | Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sistema di gestione della protezione del trattamento di dati</b><br>Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)                             |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sistema di gestione della sicurezza sul lavoro</b><br>Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Supporti cartacei<br>C   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sito web</b><br>Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Terzi identificati e identificabili<br>Strumenti elettronici<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Spedizione e ricezione di documenti e materiale</b><br>Documenti di trasporto, indirizzari, ecc.<br>Dati personali<br>Clienti e fornitori<br>Strumenti elettronici e non<br>C  |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I inserimento, raccolta, registrazione
- C archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A annullamento, blocco, cancellazione, distruzione
- T trasporto/trasferimento
- N solo conservazione dei supporti, senza accesso ai contenuti
- D diffusione
- X equivalente ai permessi ICMAT
- L modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
IACOBONE PASQUALE

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**VITRANI PAOLO**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |   |
|---|---|
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p>   |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p> |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>  |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati istituzioni</b><br/>Dati relativi alle istituzioni con cui sussistono dei legami</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>  |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati sistema prenotazione musei</b><br/>Dati relativi ai servizi di prenotazione musei</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>   |

|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | Dati personali<br>Fornitori e potenziali fornitori<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | Dati personali<br>Clienti e potenziali clienti<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sistema di gestione della protezione del trattamento di dati</b><br>Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03) |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sistema di gestione della sicurezza sul lavoro</b><br>Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)                 |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Supporti cartacei<br>C   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sito web</b><br>Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | Dati personali<br>Terzi identificati e identificabili<br>Strumenti elettronici<br>X   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Spedizione e ricezione di documenti e materiale</b><br>Documenti di trasporto, indirizzari, ecc.   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | Dati personali<br>Clienti e fornitori<br>Strumenti elettronici e non<br>C   |

## NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in

dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
VITRANI PAOLO

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**MAUTINO ROBERTO**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |  |
|---|--|
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p> |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>  |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati gestione e organizzazione eventi</b><br/>Dati relativi a location, budget, personale tecnico, ecc</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati istituzioni</b><br/>Dati relativi alle istituzioni con cui sussistono dei legami</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>  |

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Banca dati promozione</b>   |
| <b>Riguarda</b>                | Dati relativi alla promozione di servizi ed eventi   |
| <b>Tipologia di dati</b>       | Dati personali e potenzialmente sensibili  |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Banca dati regolamento ed anagrafica contratti operatori esterni</b>                              |
| <b>Riguarda</b>                | Dati relativi ai regolamenti ed anagrafiche contratti operatori esterni                              |
| <b>Tipologia di dati</b>       | Dati personali e potenzialmente sensibili  |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Banca dati sistema prenotazione musei</b>   |
| <b>Riguarda</b>                | Dati relativi ai servizi di prenotazione musei   |
| <b>Tipologia di dati</b>       | Dati personali e potenzialmente sensibili  |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Gestione acquisti e approvvigionamenti</b>  |
| <b>Riguarda</b>                | Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori           |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Fornitori e potenziali fornitori   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Gestione della clientela</b>  |
| <b>Riguarda</b>                | Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti e potenziali clienti   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Gestione libri sociali</b>  |
| <b>Riguarda</b>                | Libro soci, libro giornale, verbali, ecc.  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |
| <b>Modalità di trattamento</b> | Supporti cartacei  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Posta elettronica</b>   |
| <b>Riguarda</b>                | Mittente, destinatari, contenuto delle e-mail  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili                                 |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Posta elettronica certificata</b>   |
| <b>Riguarda</b>                | Mittente, destinatari, contenuto delle e-mail certificate  |
| <b>Tipologia di dati</b>       | Dati personali eventualmente sensibili   |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili                                 |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |

|                                  |   |
|----------------------------------|---|
| <b>Nome</b>                      | <b>Sistema di gestione della protezione del trattamento di dati</b>   |
| <b>Riguarda</b>                  | Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)  |
| <b>Tipologia di dati</b>         | Dati personali  |
| <b>Categoria interessati</b>     | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)   |
| <b>Modalità di trattamento</b>   | Strumenti elettronici e non   |
| <b>Permessi*</b>                 | C   |
| <b>Nome</b>                      | <b>Sistema di gestione della sicurezza sul lavoro</b>   |
| <b>Riguarda</b>                  | Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)  |
| <b>Tipologia di dati</b>         | Dati personali  |
| <b>Categoria interessati</b>     | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)   |
| <b>Modalità di trattamento</b>   | Supporti cartacei   |
| <b>Permessi*</b>                 | C   |
| <b>Nome</b>                      | <b>Sistema informativo</b>  |
| <b>Riguarda</b>                  | Informazioni necessarie per garantire il funzionamento dell'insieme di postazioni informatiche (computer fissi, portatili, palmari, ecc.), stampanti, attrezzature di rete (switch, router, access point, firewall, ecc.) e server, atto al trattamento dei dati sia dal punto di vista software che hardware; in particolare per quanto attiene ai sistemi di autenticazione ed autorizzazione |
| <b>Tipologia di dati</b>         | Dati personali  |
| <b>Categoria interessati</b>     | Utenti del sistema informativo, lavoratori, collaboratori   |
| <b>Modalità di trattamento</b>   | Strumenti elettronici   |
| <b>Programma/Attrezzatura</b>    | Sistemi operativi degli strumenti elettronici in uso  |
| <b>Amministratori di sistema</b> | KOINE' SISTEMI  |
| <b>Permessi*</b>                 | X   |
| <b>Nome</b>                      | <b>Sito web</b>   |
| <b>Riguarda</b>                  | Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.   |
| <b>Tipologia di dati</b>         | Dati personali  |
| <b>Categoria interessati</b>     | Terzi identificati e identificabili   |
| <b>Modalità di trattamento</b>   | Strumenti elettronici   |
| <b>Permessi*</b>                 | X   |
| <b>Nome</b>                      | <b>Spedizione e ricezione di documenti e materiale</b>  |
| <b>Riguarda</b>                  | Documenti di trasporto, indirizzari, ecc.   |
| <b>Tipologia di dati</b>         | Dati personali  |
| <b>Categoria interessati</b>     | Clienti e fornitori   |
| <b>Modalità di trattamento</b>   | Strumenti elettronici e non   |
| <b>Permessi*</b>                 | X   |

## NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elabo-



ratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
MAUTINO ROBERTO

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**PEPE ANNARITA**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |  |
|---|--|
| <p><b>Nome Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |
| <p><b>Nome Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p> |
| <p><b>Nome Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Attività di recupero crediti</b><br/>Solleciti ai clienti per il pagamento di effetti scaduti</p> <p>Dati economici riservati</p> <p>Clienti</p> <p>Strumenti elettronici e non</p> <p>X</p>   |
| <p><b>Nome Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>  |
| <p><b>Nome Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati gestione e organizzazione eventi</b><br/>Dati relativi a location, budget, personale tecnico, ecc</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |

|  |  |
|--|--|
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati istituzioni</b><br>Dati relativi alle istituzioni con cui sussistono dei legami<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati promozione</b><br>Dati relativi alla promozione di servizi ed eventi<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati regolamento ed anagrafica contratti operatori esterni</b><br>Dati relativi ai regolamenti ed anagrafiche contratti operatori esterni<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati sistema prenotazione musei</b><br>Dati relativi ai servizi di prenotazione musei<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Banca dati utenti cessione terzi</b><br>Dati anagrafici e di riferimento dei soggetti fornitori di servizi della struttura potenzialmente interessati a prodotti, eventi forniti da terzi da noi individuati<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori<br>Dati personali<br>Fornitori e potenziali fornitori<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing<br>Dati personali<br>Clienti e potenziali clienti<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><br><b>Permessi*</b> | <b>Pratiche legali e contenziosi</b><br>Dati giudiziari per cause civili, penali, di lavoro, amministrative, stragiudiziali, ecc. che interessano il titolare del trattamento e terzi identificati e identificabili<br>Dati giudiziari<br>Clienti, fornitori, lavoratori, terzi identificati ed identificabili<br>Cartacea; informatica mediante fax e/o computer, utilizzando file di suite da ufficio, quali fogli di calcolo ed elaboratori di testi; upporti cartacei<br>X |

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Sistema di gestione della protezione del trattamento di dati</b>  |
| <b>Riguarda</b>                | Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03) |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Sistema di gestione della sicurezza sul lavoro</b>  |
| <b>Riguarda</b>                | Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)  |
| <b>Modalità di trattamento</b> | Supporti cartacei  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Sito web</b>  |
| <b>Riguarda</b>                | Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.              |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Spedizione e ricezione di documenti e materiale</b>   |
| <b>Riguarda</b>                | Documenti di trasporto, indirizzari, ecc.  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti e fornitori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |

## NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;

- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
PEPE ANNARITA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**PINTOR RENATA**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |  |
|---|--|
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p> |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Attività di recupero crediti</b><br/>Solleciti ai clienti per il pagamento di effetti scaduti</p> <p>Dati economici riservati</p> <p>Clienti</p> <p>Strumenti elettronici e non</p> <p>X</p>   |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>  |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati gestione e organizzazione eventi</b><br/>Dati relativi a location, budget, personale tecnico, ecc</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |

|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>             | <b>Banca dati istituzioni</b><br>Dati relativi alle istituzioni con cui sussistono dei legami<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>             | <b>Banca dati promozione</b><br>Dati relativi alla promozione di servizi ed eventi<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>             | <b>Banca dati regolamento ed anagrafica contratti operatori esterni</b><br>Dati relativi ai regolamenti ed anagrafiche contratti operatori esterni<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>             | <b>Banca dati sistema prenotazione musei</b><br>Dati relativi ai servizi di prenotazione musei<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati utenti cessione terzi</b><br>Dati anagrafici e di riferimento dei soggetti fornitori di servizi della struttura potenzialmente interessati a prodotti, eventi forniti da terzi da noi individuati<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Contabilità propria</b><br>Fatture, corrispettivi, multe, movimenti contabili, modelli fiscali, tributari, doganali, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori<br>Dati personali<br>Fornitori e potenziali fornitori<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><br><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Gestione del rapporto di lavoro nei confronti dei propri lavoratori</b><br>Relazioni con i propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese la registrazione delle presenze, l'elaborazione dei compensi, la gestione del libro unico del lavoro, i rapporti con enti previdenziali, assicurativi, sindacali, ecc.<br>Dati personali e sensibili<br>Lavoratori, dipendenti, soci, amministratori, collaboratori<br>Strumenti elettronici e non<br>C |

|                                |   |
|--------------------------------|---|
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing  |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Clienti e potenziali clienti  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |
| <b>Permessi*</b>               | X   |
| <b>Nome</b><br><b>Riguarda</b> | <b>Pratiche legali e contenziosi</b><br>Dati giudiziari per cause civili, penali, di lavoro, amministrative, stragiudiziali, ecc. che interessano il titolare del trattamento e terzi identificati e identificabili |
| <b>Tipologia di dati</b>       | Dati giudiziari   |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili  |
| <b>Modalità di trattamento</b> | Cartacea; informatica mediante fax e/o computer, utilizzando file di suite da ufficio, quali fogli di calcolo ed elaboratori di testi; upport cartacei  |
| <b>Permessi*</b>               | X   |
| <b>Nome</b><br><b>Riguarda</b> | <b>Predisposizione dichiarazione dei redditi e bilancio</b><br>Documenti vari necessari al corretto adempimento delle misure di legge in materia societaria, fiscale e tributaria                                   |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Soggetto stesso, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |
| <b>Permessi*</b>               | X   |
| <b>Nome</b><br><b>Riguarda</b> | <b>Sistema di gestione della protezione del trattamento di dati</b><br>Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)     |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |
| <b>Permessi*</b>               | C   |
| <b>Nome</b><br><b>Riguarda</b> | <b>Sistema di gestione della sicurezza sul lavoro</b><br>Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)                     |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)   |
| <b>Modalità di trattamento</b> | Supporti cartacei   |
| <b>Permessi*</b>               | C   |
| <b>Nome</b><br><b>Riguarda</b> | <b>Spedizione e ricezione di documenti e materiale</b><br>Documenti di trasporto, indirizzari, ecc.   |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Clienti e fornitori   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |
| <b>Permessi*</b>               | X   |

## NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.



In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
PINTOR RENATA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**SERRA ELEONORA**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |   |
|---|---|
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p>   |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p> |
| <p><b>Nome</b><br/><b>Riguarda</b><br/><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p>    | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>  |
| <p><b>Nome</b><br/><b>Riguarda</b><br/><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p>    | <p><b>Banca dati gestione e organizzazione eventi</b><br/>Dati relativi a location, budget, personale tecnico, ecc</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>   |
| <p><b>Nome</b><br/><b>Riguarda</b><br/><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p>    | <p><b>Banca dati istituzioni</b><br/>Dati relativi alle istituzioni con cui sussistono dei legami</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>  |

|  |  |
|--|--|
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Banca dati promozione</b><br>Dati relativi alla promozione di servizi ed eventi<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Banca dati regolamento ed anagrafica contratti operatori esterni</b><br>Dati relativi ai regolamenti ed anagrafiche contratti operatori esterni<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Banca dati sistema prenotazione musei</b><br>Dati relativi ai servizi di prenotazione musei<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Banca dati utenti cessione terzi</b><br>Dati anagrafici e di riferimento dei soggetti fornitori di servizi della struttura potenzialmente interessati a prodotti, eventi forniti da terzi da noi individuati<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X                |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori<br>Dati personali<br>Fornitori e potenziali fornitori<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing<br>Dati personali<br>Clienti e potenziali clienti<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Posta elettronica certificata</b><br>Mittente, destinatari, contenuto delle e-mail certificate<br>Dati personali eventualmente sensibili<br>Clienti, fornitori, lavoratori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Sistema di gestione della protezione del trattamento di dati</b><br>Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)<br>Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Strumenti elettronici e non<br>C |

|   |   |
|---|---|
| <b>Nome</b><br><b>Riguarda</b>  | <b>Sistema di gestione della sicurezza sul lavoro</b><br>Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Supporti cartacei<br>C   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Sistema informativo</b><br>Informazioni necessarie per garantire il funzionamento dell'insieme di postazioni informatiche (computer fissi, portatili, palmari, ecc.), stampanti, attrezzature di rete (switch, router, access point, firewall, ecc.) e server, atto al trattamento dei dati sia dal punto di vista software che hardware; in particolare per quanto attiene ai sistemi di autenticazione ed autorizzazione |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Programma/Attrezzatura</b><br><b>Amministratori di sistema</b><br><b>Permessi*</b> | Dati personali<br>Utenti del sistema informativo, lavoratori, collaboratori<br>Strumenti elettronici<br>Sistemi operativi degli strumenti elettronici in uso<br>KOINE' SISTEMI<br>X   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Sito web</b><br>Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali<br>Terzi identificati e identificabili<br>Strumenti elettronici<br>X   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Spedizione e ricezione di documenti e materiale</b><br>Documenti di trasporto, indirizzari, ecc.   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali<br>Clienti e fornitori<br>Strumenti elettronici e non<br>X   |

## NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;

- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
SERRA ELEONORA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**ARUGA MARCO**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |  |
|---|--|
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p> |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>  |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati gestione e organizzazione eventi</b><br/>Dati relativi a location, budget, personale tecnico, ecc</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati istituzioni</b><br/>Dati relativi alle istituzioni con cui sussistono dei legami</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>  |

|  |  |
|--|--|
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati promozione</b><br>Dati relativi alla promozione di servizi ed eventi<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati regolamento ed anagrafica contratti operatori esterni</b><br>Dati relativi ai regolamenti ed anagrafiche contratti operatori esterni<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati sistema prenotazione musei</b><br>Dati relativi ai servizi di prenotazione musei<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Corrispondenza, comunicati e circolari</b><br>Informazioni varie conservate a fini amministrativi o per future ed eventuali pratiche legali<br>Dati personali<br>Clienti, fornitori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori<br>Dati personali<br>Fornitori e potenziali fornitori<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing<br>Dati personali<br>Clienti e potenziali clienti<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Posta elettronica certificata</b><br>Mittente, destinatari, contenuto delle e-mail certificate<br>Dati personali eventualmente sensibili<br>Clienti, fornitori, lavoratori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><br><b>Permessi*</b> | <b>Pratiche legali e contenziosi</b><br>Dati giudiziari per cause civili, penali, di lavoro, amministrative, stragiudiziali, ecc. che interessano il titolare del trattamento e terzi identificati e identificabili<br>Dati giudiziari<br>Clienti, fornitori, lavoratori, terzi identificati ed identificabili<br>Cartacea; informatica mediante fax e/o computer, utilizzando file di suite da ufficio, quali fogli di calcolo ed elaboratori di testi; upporti cartacei<br>X |

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Sistema di gestione della protezione del trattamento di dati</b>  |
| <b>Riguarda</b>                | Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03) |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Sistema di gestione della sicurezza sul lavoro</b>  |
| <b>Riguarda</b>                | Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)  |
| <b>Modalità di trattamento</b> | Supporti cartacei  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Sito web</b>  |
| <b>Riguarda</b>                | Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.              |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Spedizione e ricezione di documenti e materiale</b>   |
| <b>Riguarda</b>                | Documenti di trasporto, indirizzari, ecc.  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti e fornitori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |

## NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;



- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
ARUGA MARCO

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**CAGNASSO MAGDA**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|                                |  |
|--------------------------------|--|
| <b>Nome<br/>Riguarda</b>       | <b>Agenda appuntamenti, visite e prenotazioni</b><br>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti, fornitori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome<br/>Riguarda</b>       | <b>Anagrafica condivisa e rubrica</b><br>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti, fornitori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome<br/>Riguarda</b>       | <b>Attività di recupero crediti</b><br>Solleciti ai clienti per il pagamento di effetti scaduti  |
| <b>Tipologia di dati</b>       | Dati economici riservati   |
| <b>Categoria interessati</b>   | Clienti  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome<br/>Riguarda</b>       | <b>Banca dati associati</b><br>Dati relativi agli associati  |
| <b>Tipologia di dati</b>       | Dati personali e potenzialmente sensibili  |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome<br/>Riguarda</b>       | <b>Banca dati gestione e organizzazione eventi</b><br>Dati relativi a location, budget, personale tecnico, ecc   |
| <b>Tipologia di dati</b>       | Dati personali e potenzialmente sensibili  |
| <b>Categoria interessati</b>   | Terzi identificati e identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |

|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati istituzioni</b><br>Dati relativi alle istituzioni con cui sussistono dei legami<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati promozione</b><br>Dati relativi alla promozione di servizi ed eventi<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati regolamento ed anagrafica contratti operatori esterni</b><br>Dati relativi ai regolamenti ed anagrafiche contratti operatori esterni<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati sistema prenotazione musei</b><br>Dati relativi ai servizi di prenotazione musei<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Banca dati utenti cessione terzi</b><br>Dati anagrafici e di riferimento dei soggetti fornitori di servizi della struttura potenzialmente interessati a prodotti, eventi forniti da terzi da noi individuati<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Contabilità propria</b><br>Fatture, corrispettivi, multe, movimenti contabili, modelli fiscali, tributari, doganali, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori<br>Dati personali<br>Fornitori e potenziali fornitori<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Gestione del rapporto di lavoro nei confronti dei propri lavoratori</b><br>Relazioni con i propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese la registrazione delle presenze, l'elaborazione dei compensi, la gestione del libro unico del lavoro, i rapporti con enti previdenziali, assicurativi, sindacali, ecc.<br>Dati personali e sensibili<br>Lavoratori, dipendenti, soci, amministratori, collaboratori<br>Strumenti elettronici e non<br>C |

|                                |   |
|--------------------------------|---|
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing  |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Clienti e potenziali clienti  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |
| <b>Permessi*</b>               | X   |
| <b>Nome</b><br><b>Riguarda</b> | <b>Pratiche legali e contenziosi</b><br>Dati giudiziari per cause civili, penali, di lavoro, amministrative, stragiudiziali, ecc. che interessano il titolare del trattamento e terzi identificati e identificabili |
| <b>Tipologia di dati</b>       | Dati giudiziari   |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili  |
| <b>Modalità di trattamento</b> | Cartacea; informatica mediante fax e/o computer, utilizzando file di suite da ufficio, quali fogli di calcolo ed elaboratori di testi; upport cartacei  |
| <b>Permessi*</b>               | X   |
| <b>Nome</b><br><b>Riguarda</b> | <b>Predisposizione dichiarazione dei redditi e bilancio</b><br>Documenti vari necessari al corretto adempimento delle misure di legge in materia societaria, fiscale e tributaria                                   |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Soggetto stesso, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |
| <b>Permessi*</b>               | X   |
| <b>Nome</b><br><b>Riguarda</b> | <b>Sistema di gestione della protezione del trattamento di dati</b><br>Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)     |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |
| <b>Permessi*</b>               | C   |
| <b>Nome</b><br><b>Riguarda</b> | <b>Sistema di gestione della sicurezza sul lavoro</b><br>Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)                     |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)   |
| <b>Modalità di trattamento</b> | Supporti cartacei   |
| <b>Permessi*</b>               | C   |
| <b>Nome</b><br><b>Riguarda</b> | <b>Spedizione e ricezione di documenti e materiale</b><br>Documenti di trasporto, indirizzari, ecc.   |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Clienti e fornitori   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |
| <b>Permessi*</b>               | X   |

## NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
CAGNASSO MAGDA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

### CORREALE AMALIA

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |   |
|---|---|
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p>   |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p> |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Attività di recupero crediti</b><br/>Solleciti ai clienti per il pagamento di effetti scaduti</p> <p>Dati economici riservati<br/>Clienti<br/>Strumenti elettronici e non<br/>X</p>   |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>  |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati gestione e organizzazione eventi</b><br/>Dati relativi a location, budget, personale tecnico, ecc</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>   |

|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati istituzioni</b><br>Dati relativi alle istituzioni con cui sussistono dei legami<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati regolamento ed anagrafica contratti operatori esterni</b><br>Dati relativi ai regolamenti ed anagrafiche contratti operatori esterni<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati sistema prenotazione musei</b><br>Dati relativi ai servizi di prenotazione musei<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Contabilità propria</b><br>Fatture, corrispettivi, multe, movimenti contabili, modelli fiscali, tributari, doganali, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Corrispondenza, comunicati e circolari</b><br>Informazioni varie conservate a fini amministrativi o per future ed eventuali pratiche legali<br>Dati personali<br>Clienti, fornitori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori<br>Dati personali<br>Fornitori e potenziali fornitori<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Gestione del rapporto di lavoro nei confronti dei propri lavoratori</b><br>Relazioni con i propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese la registrazione delle presenze, l'elaborazione dei compensi, la gestione del libro unico del lavoro, i rapporti con enti previdenziali, assicurativi, sindacali, ecc.<br>Dati personali e sensibili<br>Lavoratori, dipendenti, soci, amministratori, collaboratori<br>Strumenti elettronici e non<br>X |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing<br>Dati personali<br>Clienti e potenziali clienti<br>Strumenti elettronici e non<br>X  |

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Gestione libri sociali</b>  |
| <b>Riguarda</b>                | Libro soci, libro giornale, verbali, ecc.  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Supporti cartacei  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Incassi, pagamenti e operazioni bancarie</b>  |
| <b>Riguarda</b>                | Estratti conti, bonifici, assegni, versamenti, riba, rid, ecc.   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Posta elettronica certificata</b>   |
| <b>Riguarda</b>                | Mittente, destinatari, contenuto delle e-mail certificate  |
| <b>Tipologia di dati</b>       | Dati personali eventualmente sensibili   |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Pratiche legali e contenziosi</b>   |
| <b>Riguarda</b>                | Dati giudiziari per cause civili, penali, di lavoro, amministrative, stragiudiziali, ecc. che interessano il titolare del trattamento e terzi identificati e identificabili      |
| <b>Tipologia di dati</b>       | Dati giudiziari  |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Cartacea; informatica mediante fax e/o computer, utilizzando file di suite da ufficio, quali fogli di calcolo ed elaboratori di testi; upporti cartacei                          |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Predisposizione dichiarazione dei redditi e bilancio</b>  |
| <b>Riguarda</b>                | Documenti vari necessari al corretto adempimento delle misure di legge in materia societaria, fiscale e tributaria   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, terzi identificati ed identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Registrazione e gestione delle presenze nei confronti dei propri lavoratori</b>   |
| <b>Riguarda</b>                | Dati inerenti alle presenze dei propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese le ferie, le malattie, i lutti, i permessi, gli straordinari, ecc. |
| <b>Tipologia di dati</b>       | Dati personali e sensibili   |
| <b>Categoria interessati</b>   | Lavoratori, dipendenti, soci, amministratori, collaboratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Selezione del personale</b>   |
| <b>Riguarda</b>                | Curriculum vitae, questionari, prove di selezione di candidati per posti di lavoro   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Potenziali lavoratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |



|                                  |   |
|----------------------------------|---|
| <b>Nome</b>                      | <b>Sistema di gestione della protezione del trattamento di dati</b>   |
| <b>Riguarda</b>                  | Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)  |
| <b>Tipologia di dati</b>         | Dati personali  |
| <b>Categoria interessati</b>     | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)   |
| <b>Modalità di trattamento</b>   | Strumenti elettronici e non   |
| <b>Permessi*</b>                 | C   |
| <b>Nome</b>                      | <b>Sistema di gestione della sicurezza sul lavoro</b>   |
| <b>Riguarda</b>                  | Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)  |
| <b>Tipologia di dati</b>         | Dati personali  |
| <b>Categoria interessati</b>     | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)   |
| <b>Modalità di trattamento</b>   | Supporti cartacei   |
| <b>Permessi*</b>                 | C   |
| <b>Nome</b>                      | <b>Sistema informativo</b>  |
| <b>Riguarda</b>                  | Informazioni necessarie per garantire il funzionamento dell'insieme di postazioni informatiche (computer fissi, portatili, palmari, ecc.), stampanti, attrezzature di rete (switch, router, access point, firewall, ecc.) e server, atto al trattamento dei dati sia dal punto di vista software che hardware; in particolare per quanto attiene ai sistemi di autenticazione ed autorizzazione |
| <b>Tipologia di dati</b>         | Dati personali  |
| <b>Categoria interessati</b>     | Utenti del sistema informativo, lavoratori, collaboratori   |
| <b>Modalità di trattamento</b>   | Strumenti elettronici   |
| <b>Programma/Attrezzatura</b>    | Sistemi operativi degli strumenti elettronici in uso  |
| <b>Amministratori di sistema</b> | KOINE' SISTEMI  |
| <b>Permessi*</b>                 | X   |
| <b>Nome</b>                      | <b>Spedizione e ricezione di documenti e materiale</b>  |
| <b>Riguarda</b>                  | Documenti di trasporto, indirizzari, ecc.   |
| <b>Tipologia di dati</b>         | Dati personali  |
| <b>Categoria interessati</b>     | Clienti e fornitori   |
| <b>Modalità di trattamento</b>   | Strumenti elettronici e non   |
| <b>Permessi*</b>                 | X   |

## NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;

- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
CORREALE AMALIA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**LEON FRANCESCA**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |  |
|---|--|
| <p><b>Nome Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |
| <p><b>Nome Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p> |
| <p><b>Nome Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Attività di recupero crediti</b><br/>Solleciti ai clienti per il pagamento di effetti scaduti</p> <p>Dati economici riservati</p> <p>Clienti</p> <p>Strumenti elettronici e non</p> <p>X</p>   |
| <p><b>Nome Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>  |
| <p><b>Nome Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati gestione e organizzazione eventi</b><br/>Dati relativi a location, budget, personale tecnico, ecc</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |

|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati istituzioni</b><br>Dati relativi alle istituzioni con cui sussistono dei legami<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati promozione</b><br>Dati relativi alla promozione di servizi ed eventi<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati regolamento ed anagrafica contratti operatori esterni</b><br>Dati relativi ai regolamenti ed anagrafiche contratti operatori esterni<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati sistema prenotazione musei</b><br>Dati relativi ai servizi di prenotazione musei<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Banca dati utenti cessione terzi</b><br>Dati anagrafici e di riferimento dei soggetti fornitori di servizi della struttura potenzialmente interessati a prodotti, eventi forniti da terzi da noi individuati<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Comunicazioni telefoniche</b><br>Informazioni circa chiamate in entrata e in uscita gestito per fini tecnici, amministrativi e commerciali<br>Dati personali<br>Terzi identificati ed identificabili<br>Strumenti elettronici<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Contabilità propria</b><br>Fatture, corrispettivi, multe, movimenti contabili, modelli fiscali, tributari, doganali, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Corrispondenza, comunicati e circolari</b><br>Informazioni varie conservate a fini amministrativi o per future ed eventuali pratiche legali<br>Dati personali<br>Clienti, fornitori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>X  |

|  |  |
|--|--|
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Fornitori e potenziali fornitori<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione del rapporto di lavoro nei confronti dei propri lavoratori</b><br>Relazioni con i propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese la registrazione delle presenze, l'elaborazione dei compensi, la gestione del libro unico del lavoro, i rapporti con enti previdenziali, assicurativi, sindacali, ecc. |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali e sensibili<br>Lavoratori, dipendenti, soci, amministratori, collaboratori<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali<br>Clienti e potenziali clienti<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b>   | <b>Gestione libri sociali</b><br>Libro soci, libro giornale, verbali, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b><br><b>Permessi*</b>   | Supporti cartacei<br>X   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Gestione polizze assicurative</b><br>Informazioni necessarie per la gestione delle polizze assicurative di cui si è contraente e/o beneficiario, ecc.   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>                                   | Dati personali eventualmente sensibili<br>Soggetto stesso, lavoratori<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b>   | <b>Incassi, pagamenti e operazioni bancarie</b><br>Estratti conti, bonifici, assegni, versamenti, riba, rid, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili  |
| <b>Modalità di trattamento</b><br><b>Permessi*</b>   | Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Posta elettronica</b><br>Mittente, destinatari, contenuto delle e-mail<br>Dati personali<br>Clienti, fornitori, lavoratori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Posta elettronica certificata</b><br>Mittente, destinatari, contenuto delle e-mail certificate<br>Dati personali eventualmente sensibili<br>Clienti, fornitori, lavoratori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>X  |

|                                |  |
|--------------------------------|--|
| <b>Nome</b><br><b>Riguarda</b> | <b>Pratiche legali e contenziosi</b><br>Dati giudiziari per cause civili, penali, di lavoro, amministrative, stragiudiziali, ecc. che interessano il titolare del trattamento e terzi identificati e identificabili  |
| <b>Tipologia di dati</b>       | Dati giudiziari  |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Cartacea; informatica mediante fax e/o computer, utilizzando file di suite da ufficio, quali fogli di calcolo ed elaboratori di testi; upport cartacei   |
| <b>Permessi*</b>               | X  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Predisposizione dichiarazione dei redditi e bilancio</b><br>Documenti vari necessari al corretto adempimento delle misure di legge in materia societaria, fiscale e tributaria  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, terzi identificati ed identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Registrazione e gestione delle presenze nei confronti dei propri lavoratori</b><br>Dati inerenti alle presenze dei propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese le ferie, le malattie, i lutti, i permessi, gli straordinari, ecc. |
| <b>Tipologia di dati</b>       | Dati personali e sensibili   |
| <b>Categoria interessati</b>   | Lavoratori, dipendenti, soci, amministratori, collaboratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Relazioni pubbliche</b><br>Attività con istituzioni pubbliche, con la stampa, ecc.  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Selezione del personale</b><br>Curriculum vitae, questionari, prove di selezione di candidati per posti di lavoro   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Potenziali lavoratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Sistema di gestione della protezione del trattamento di dati</b><br>Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Sistema di gestione della sicurezza sul lavoro</b><br>Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)  |
| <b>Modalità di trattamento</b> | Supporti cartacei  |
| <b>Permessi*</b>               | C  |

|   |   |
|---|---|
| <b>Nome</b><br><b>Riguarda</b>  | <b>Sistema informativo</b><br>Informazioni necessarie per garantire il funzionamento dell'insieme di postazioni informatiche (computer fissi, portatili, palmari, ecc.), stampanti, attrezzature di rete (switch, router, access point, firewall, ecc.) e server, atto al trattamento dei dati sia dal punto di vista software che hardware; in particolare per quanto attiene ai sistemi di autenticazione ed autorizzazione |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Programma/Attrezzatura</b><br><b>Amministratori di sistema</b><br><b>Permessi*</b> | Dati personali<br>Utenti del sistema informativo, lavoratori, collaboratori<br>Strumenti elettronici<br>Sistemi operativi degli strumenti elettronici in uso<br>KOINE' SISTEMI<br>X   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Sito web</b><br>Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali<br>Terzi identificati e identificabili<br>Strumenti elettronici<br>X   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Spedizione e ricezione di documenti e materiale</b><br>Documenti di trasporto, indirizzari, ecc.   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali<br>Clienti e fornitori<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Trasmissioni dati in internet (navigazione web, file sharing, ecc.)</b><br>Indirizzi degli host coinvolti, dati trasmessi, ecc. compresi indirizzi e contenuti delle pagine web visitate, contenuti delle sessioni di messengerie  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali e potenzialmente sensibili<br>Lavoratori, terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |

## NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;

- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
LEON FRANCESCA



## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**D'ACRI ANTONIO MARCO**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |   |
|---|---|
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>C</p>   |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>C</p> |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Attività di recupero crediti</b><br/>Solleciti ai clienti per il pagamento di effetti scaduti</p> <p>Dati economici riservati<br/>Clienti<br/>Strumenti elettronici e non<br/>C</p>   |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>C</p>  |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati gestione e organizzazione eventi</b><br/>Dati relativi a location, budget, personale tecnico, ecc</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>C</p>   |

|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati istituzioni</b><br>Dati relativi alle istituzioni con cui sussistono dei legami<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati promozione</b><br>Dati relativi alla promozione di servizi ed eventi<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati regolamento ed anagrafica contratti operatori esterni</b><br>Dati relativi ai regolamenti ed anagrafiche contratti operatori esterni<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati sistema prenotazione musei</b><br>Dati relativi ai servizi di prenotazione musei<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Banca dati utenti cessione terzi</b><br>Dati anagrafici e di riferimento dei soggetti fornitori di servizi della struttura potenzialmente interessati a prodotti, eventi forniti da terzi da noi individuati<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Cartelle sanitarie di rischio dei lavoratori soggetti a sorveglianza sanitaria</b><br>Visite ed esami di medicina del lavoro svolte dai lavoratori soggetti<br>Dati sensibili<br>Lavoratori, dipendenti, soci, amministratori, collaboratori<br>Supporti cartacei<br>C   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Comunicazioni telefoniche</b><br>Informazioni circa chiamate in entrata e in uscita gestito per fini tecnici, amministrativi e commerciali<br>Dati personali<br>Terzi identificati ed identificabili<br>Strumenti elettronici<br>C   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Contabilità propria</b><br>Fatture, corrispettivi, multe, movimenti contabili, modelli fiscali, tributari, doganali, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>C  |

|                                |  |
|--------------------------------|--|
| <b>Nome</b><br><b>Riguarda</b> | <b>Corrispondenza, comunicati e circolari</b><br>Informazioni varie conservate a fini amministrativi o per future ed eventuali pratiche legali   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti, fornitori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Fornitori e potenziali fornitori   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione del rapporto di lavoro nei confronti dei propri lavoratori</b><br>Relazioni con i propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese la registrazione delle presenze, l'elaborazione dei compensi, la gestione del libro unico del lavoro, i rapporti con enti previdenziali, assicurativi, sindacali, ecc. |
| <b>Tipologia di dati</b>       | Dati personali e sensibili   |
| <b>Categoria interessati</b>   | Lavoratori, dipendenti, soci, amministratori, collaboratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti e potenziali clienti   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione libri sociali</b><br>Libro soci, libro giornale, verbali, ecc.   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Supporti cartacei  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione polizze assicurative</b><br>Informazioni necessarie per la gestione delle polizze assicurative di cui si è contraente e/o beneficiario, ecc.   |
| <b>Tipologia di dati</b>       | Dati personali eventualmente sensibili   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Incassi, pagamenti e operazioni bancarie</b><br>Estratti conti, bonifici, assegni, versamenti, riba, rid, ecc.  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Posta elettronica</b><br>Mittente, destinatari, contenuto delle e-mail  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Posta elettronica certificata</b>   |
| <b>Riguarda</b>                | Mittente, destinatari, contenuto delle e-mail certificate  |
| <b>Tipologia di dati</b>       | Dati personali eventualmente sensibili   |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Pratiche legali e contenziosi</b>   |
| <b>Riguarda</b>                | Dati giudiziari per cause civili, penali, di lavoro, amministrative, stragiudiziali, ecc. che interessano il titolare del trattamento e terzi identificati e identificabili      |
| <b>Tipologia di dati</b>       | Dati giudiziari  |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Cartacea; informatica mediante fax e/o computer, utilizzando file di suite da ufficio, quali fogli di calcolo ed elaboratori di testi; upport cartacei                           |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Predisposizione dichiarazione dei redditi e bilancio</b>  |
| <b>Riguarda</b>                | Documenti vari necessari al corretto adempimento delle misure di legge in materia societaria, fiscale e tributaria   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, terzi identificati ed identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Registrazione e gestione delle presenze nei confronti dei propri lavoratori</b>   |
| <b>Riguarda</b>                | Dati inerenti alle presenze dei propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese le ferie, le malattie, i lutti, i permessi, gli straordinari, ecc. |
| <b>Tipologia di dati</b>       | Dati personali e sensibili   |
| <b>Categoria interessati</b>   | Lavoratori, dipendenti, soci, amministratori, collaboratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Relazioni pubbliche</b>   |
| <b>Riguarda</b>                | Attività con istituzioni pubbliche, con la stampa, ecc.  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Selezione del personale</b>   |
| <b>Riguarda</b>                | Curriculum vitae, questionari, prove di selezione di candidati per posti di lavoro   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Potenziali lavoratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Sistema di gestione della protezione del trattamento di dati</b>  |
| <b>Riguarda</b>                | Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Sistema di gestione della sicurezza sul lavoro</b>  |
| <b>Riguarda</b>                | Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)  |
| <b>Modalità di trattamento</b> | Supporti cartacei  |
| <b>Permessi*</b>               | C  |

|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sistema informativo</b><br>Informazioni necessarie per garantire il funzionamento dell'insieme di postazioni informatiche (computer fissi, portatili, palmari, ecc.), stampanti, attrezzature di rete (switch, router, access point, firewall, ecc.) e server, atto al trattamento dei dati sia dal punto di vista software che hardware; in particolare per quanto attiene ai sistemi di autenticazione ed autorizzazione |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | Dati personali<br>Utenti del sistema informativo, lavoratori, collaboratori<br>Strumenti elettronici<br>C   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Sito web</b><br>Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | Dati personali<br>Terzi identificati e identificabili<br>Strumenti elettronici<br>C   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Spedizione e ricezione di documenti e materiale</b><br>Documenti di trasporto, indirizzari, ecc.   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | Dati personali<br>Clienti e fornitori<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b>   | <b>Trasmissioni dati in internet (navigazione web, file sharing, ecc.)</b><br>Indirizzi degli host coinvolti, dati trasmessi, ecc. compresi indirizzi e contenuti delle pagine web visitate, contenuti delle sessioni di messengerie  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | Dati personali e potenzialmente sensibili<br>Lavoratori, terzi identificati e identificabili<br>Strumenti elettronici e non<br>C  |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

Si rammenta la mancanza di autorizzazione all'utilizzo di elaboratori elettronici per lo svolgimento dei compiti assegnati.

In particolare gli incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
D'ACRI ANTONIO MARCO

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**RICCI SIMONA**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |  |
|---|--|
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p> |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>  |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati gestione e organizzazione eventi</b><br/>Dati relativi a location, budget, personale tecnico, ecc</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>   |
| <p><b>Nome<br/>Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati istituzioni</b><br/>Dati relativi alle istituzioni con cui sussistono dei legami</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>X</p>  |

|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Banca dati promozione</b><br>Dati relativi alla promozione di servizi ed eventi<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Banca dati regolamento ed anagrafica contratti operatori esterni</b><br>Dati relativi ai regolamenti ed anagrafiche contratti operatori esterni<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Banca dati sistema prenotazione musei</b><br>Dati relativi ai servizi di prenotazione musei<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Banca dati utenti cessione terzi</b><br>Dati anagrafici e di riferimento dei soggetti fornitori di servizi della struttura potenzialmente interessati a prodotti, eventi forniti da terzi da noi individuati<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori<br>Dati personali<br>Fornitori e potenziali fornitori<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing<br>Dati personali<br>Clienti e potenziali clienti<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Gestione libri sociali</b><br>Libro soci, libro giornale, verbali, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili<br>Supporti cartacei<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Posta elettronica certificata</b><br>Mittente, destinatari, contenuto delle e-mail certificate<br>Dati personali eventualmente sensibili<br>Clienti, fornitori, lavoratori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>X   |



|   |  |
|---|--|
| <b>Nome</b><br><b>Riguarda</b>  | <b>Pratiche legali e contenziosi</b><br>Dati giudiziari per cause civili, penali, di lavoro, amministrative, stragiudiziali, ecc. che interessano il titolare del trattamento e terzi identificati e identificabili  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b>  | Dati giudiziari<br>Clienti, fornitori, lavoratori, terzi identificati ed identificabili<br>Cartacea; informatica mediante fax e/o computer, utilizzando file di suite da ufficio, quali fogli di calcolo ed elaboratori di testi; upport cartacei  |
| <b>Permessi*</b>  | X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | <b>Relazioni pubbliche</b><br>Attività con istituzioni pubbliche, con la stampa, ecc.<br>Dati personali<br>Soggetto stesso<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | <b>Selezione del personale</b><br>Curriculum vitae, questionari, prove di selezione di candidati per posti di lavoro<br>Dati personali<br>Potenziali lavoratori<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | <b>Sistema di gestione della protezione del trattamento di dati</b><br>Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)<br>Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | <b>Sistema di gestione della sicurezza sul lavoro</b><br>Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)<br>Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Supporti cartacei<br>C   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Programma/Attrezzatura</b><br><b>Amministratori di sistema</b><br><b>Permessi*</b> | <b>Sistema informativo</b><br>Informazioni necessarie per garantire il funzionamento dell'insieme di postazioni informatiche (computer fissi, portatili, palmari, ecc.), stampanti, attrezzature di rete (switch, router, access point, firewall, ecc.) e server, atto al trattamento dei dati sia dal punto di vista software che hardware; in particolare per quanto attiene ai sistemi di autenticazione ed autorizzazione<br>Dati personali<br>Utenti del sistema informativo, lavoratori, collaboratori<br>Strumenti elettronici<br>Sistemi operativi degli strumenti elettronici in uso<br>KOINE' SISTEMI<br>X |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | <b>Sito web</b><br>Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.<br>Dati personali<br>Terzi identificati e identificabili<br>Strumenti elettronici<br>X  |

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Spedizione e ricezione di documenti e materiale</b> |
| <b>Riguarda</b>                | Documenti di trasporto, indirizzari, ecc.              |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti e fornitori                                    |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non                            |
| <b>Permessi*</b>               | X  |

## NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
RICCI SIMONA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**BRACCIALARGHE MAURIZIO**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |   |
|---|---|
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>C</p>   |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>C</p> |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Attività di recupero crediti</b><br/>Solleciti ai clienti per il pagamento di effetti scaduti</p> <p>Dati economici riservati<br/>Clienti<br/>Strumenti elettronici e non<br/>C</p>   |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>C</p>  |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati gestione e organizzazione eventi</b><br/>Dati relativi a location, budget, personale tecnico, ecc</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>C</p>   |

|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati istituzioni</b><br>Dati relativi alle istituzioni con cui sussistono dei legami<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati promozione</b><br>Dati relativi alla promozione di servizi ed eventi<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati regolamento ed anagrafica contratti operatori esterni</b><br>Dati relativi ai regolamenti ed anagrafiche contratti operatori esterni<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati sistema prenotazione musei</b><br>Dati relativi ai servizi di prenotazione musei<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Banca dati utenti cessione terzi</b><br>Dati anagrafici e di riferimento dei soggetti fornitori di servizi della struttura potenzialmente interessati a prodotti, eventi forniti da terzi da noi individuati<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Cartelle sanitarie di rischio dei lavoratori soggetti a sorveglianza sanitaria</b><br>Visite ed esami di medicina del lavoro svolte dai lavoratori soggetti<br>Dati sensibili<br>Lavoratori, dipendenti, soci, amministratori, collaboratori<br>Supporti cartacei<br>C   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Comunicazioni telefoniche</b><br>Informazioni circa chiamate in entrata e in uscita gestito per fini tecnici, amministrativi e commerciali<br>Dati personali<br>Terzi identificati ed identificabili<br>Strumenti elettronici<br>C   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Contabilità propria</b><br>Fatture, corrispettivi, multe, movimenti contabili, modelli fiscali, tributari, doganali, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>C  |

|                                |  |
|--------------------------------|--|
| <b>Nome</b><br><b>Riguarda</b> | <b>Corrispondenza, comunicati e circolari</b><br>Informazioni varie conservate a fini amministrativi o per future ed eventuali pratiche legali   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti, fornitori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Fornitori e potenziali fornitori   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione del rapporto di lavoro nei confronti dei propri lavoratori</b><br>Relazioni con i propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese la registrazione delle presenze, l'elaborazione dei compensi, la gestione del libro unico del lavoro, i rapporti con enti previdenziali, assicurativi, sindacali, ecc. |
| <b>Tipologia di dati</b>       | Dati personali e sensibili   |
| <b>Categoria interessati</b>   | Lavoratori, dipendenti, soci, amministratori, collaboratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti e potenziali clienti   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione libri sociali</b><br>Libro soci, libro giornale, verbali, ecc.   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Supporti cartacei  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione polizze assicurative</b><br>Informazioni necessarie per la gestione delle polizze assicurative di cui si è contraente e/o beneficiario, ecc.   |
| <b>Tipologia di dati</b>       | Dati personali eventualmente sensibili   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Incassi, pagamenti e operazioni bancarie</b><br>Estratti conti, bonifici, assegni, versamenti, riba, rid, ecc.  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Posta elettronica</b><br>Mittente, destinatari, contenuto delle e-mail  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Posta elettronica certificata</b>   |
| <b>Riguarda</b>                | Mittente, destinatari, contenuto delle e-mail certificate  |
| <b>Tipologia di dati</b>       | Dati personali eventualmente sensibili   |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Pratiche legali e contenziosi</b>   |
| <b>Riguarda</b>                | Dati giudiziari per cause civili, penali, di lavoro, amministrative, stragiudiziali, ecc. che interessano il titolare del trattamento e terzi identificati e identificabili      |
| <b>Tipologia di dati</b>       | Dati giudiziari  |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Cartacea; informatica mediante fax e/o computer, utilizzando file di suite da ufficio, quali fogli di calcolo ed elaboratori di testi; upporti cartacei                          |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Predisposizione dichiarazione dei redditi e bilancio</b>  |
| <b>Riguarda</b>                | Documenti vari necessari al corretto adempimento delle misure di legge in materia societaria, fiscale e tributaria   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, terzi identificati ed identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Registrazione e gestione delle presenze nei confronti dei propri lavoratori</b>   |
| <b>Riguarda</b>                | Dati inerenti alle presenze dei propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese le ferie, le malattie, i lutti, i permessi, gli straordinari, ecc. |
| <b>Tipologia di dati</b>       | Dati personali e sensibili   |
| <b>Categoria interessati</b>   | Lavoratori, dipendenti, soci, amministratori, collaboratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Relazioni pubbliche</b>   |
| <b>Riguarda</b>                | Attività con istituzioni pubbliche, con la stampa, ecc.  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Revisione dei conti e certificazione di bilancio</b>  |
| <b>Riguarda</b>                | Attività di controllo sui documenti contabili, societari, fiscali, tributari, previdenziali, ecc.  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Selezione del personale</b>   |
| <b>Riguarda</b>                | Curriculum vitae, questionari, prove di selezione di candidati per posti di lavoro   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Potenziali lavoratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |

|   |   |
|---|---|
| <b>Nome</b><br><b>Riguarda</b>  | <b>Sistema di gestione della protezione del trattamento di dati</b><br>Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Sistema di gestione della sicurezza sul lavoro</b><br>Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Supporti cartacei<br>C   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Sistema informativo</b><br>Informazioni necessarie per garantire il funzionamento dell'insieme di postazioni informatiche (computer fissi, portatili, palmari, ecc.), stampanti, attrezzature di rete (switch, router, access point, firewall, ecc.) e server, atto al trattamento dei dati sia dal punto di vista software che hardware; in particolare per quanto attiene ai sistemi di autenticazione ed autorizzazione |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Programma/Attrezzatura</b><br><b>Amministratori di sistema</b><br><b>Permessi*</b> | Dati personali<br>Utenti del sistema informativo, lavoratori, collaboratori<br>Strumenti elettronici<br>Sistemi operativi degli strumenti elettronici in uso<br>KOINE' SISTEMI<br>C   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Sito web</b><br>Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali<br>Terzi identificati e identificabili<br>Strumenti elettronici<br>C   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Spedizione e ricezione di documenti e materiale</b><br>Documenti di trasporto, indirizzari, ecc.   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali<br>Clienti e fornitori<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Trasmissioni dati in internet (navigazione web, file sharing, ecc.)</b><br>Indirizzi degli host coinvolti, dati trasmessi, ecc. compresi indirizzi e contenuti delle pagine web visitate, contenuti delle sessioni di messengerie  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali e potenzialmente sensibili<br>Lavoratori, terzi identificati e identificabili<br>Strumenti elettronici e non<br>C  |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:



- I inserimento, raccolta, registrazione
- C archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A annullamento, blocco, cancellazione, distruzione
- T trasporto/trasferimento
- N solo conservazione dei supporti, senza accesso ai contenuti
- D diffusione
- X equivalente ai permessi ICMAT
- L modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
BRACCIALARGHE MAURIZIO

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**COPPOLA MICHELE**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, per i seguenti trattamenti, archivi o banche dati:

|   |  |
|---|--|
| <p><b>Nome Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>C</p>   |
| <p><b>Nome Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali</p> <p>Clienti, fornitori, terzi identificati ed identificabili</p> <p>Strumenti elettronici e non</p> <p>C</p> |
| <p><b>Nome Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Attività di recupero crediti</b><br/>Solleciti ai clienti per il pagamento di effetti scaduti</p> <p>Dati economici riservati</p> <p>Clienti</p> <p>Strumenti elettronici e non</p> <p>C</p>   |
| <p><b>Nome Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>C</p>  |
| <p><b>Nome Riguarda</b></p> <p><b>Tipologia di dati</b></p> <p><b>Categoria interessati</b></p> <p><b>Modalità di trattamento</b></p> <p><b>Permessi*</b></p> | <p><b>Banca dati gestione e organizzazione eventi</b><br/>Dati relativi a location, budget, personale tecnico, ecc</p> <p>Dati personali e potenzialmente sensibili</p> <p>Terzi identificati e identificabili</p> <p>Strumenti elettronici e non</p> <p>C</p>   |

|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati istituzioni</b><br>Dati relativi alle istituzioni con cui sussistono dei legami<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati promozione</b><br>Dati relativi alla promozione di servizi ed eventi<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati regolamento ed anagrafica contratti operatori esterni</b><br>Dati relativi ai regolamenti ed anagrafiche contratti operatori esterni<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati sistema prenotazione musei</b><br>Dati relativi ai servizi di prenotazione musei<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Banca dati utenti cessione terzi</b><br>Dati anagrafici e di riferimento dei soggetti fornitori di servizi della struttura potenzialmente interessati a prodotti, eventi forniti da terzi da noi individuati<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>C |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Cartelle sanitarie di rischio dei lavoratori soggetti a sorveglianza sanitaria</b><br>Visite ed esami di medicina del lavoro svolte dai lavoratori soggetti<br>Dati sensibili<br>Lavoratori, dipendenti, soci, amministratori, collaboratori<br>Supporti cartacei<br>C   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Comunicazioni telefoniche</b><br>Informazioni circa chiamate in entrata e in uscita gestito per fini tecnici, amministrativi e commerciali<br>Dati personali<br>Terzi identificati ed identificabili<br>Strumenti elettronici<br>C   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Contabilità propria</b><br>Fatture, corrispettivi, multe, movimenti contabili, modelli fiscali, tributari, doganali, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>C  |

|                                |  |
|--------------------------------|--|
| <b>Nome</b><br><b>Riguarda</b> | <b>Corrispondenza, comunicati e circolari</b><br>Informazioni varie conservate a fini amministrativi o per future ed eventuali pratiche legali   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti, fornitori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Fornitori e potenziali fornitori   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione del rapporto di lavoro nei confronti dei propri lavoratori</b><br>Relazioni con i propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese la registrazione delle presenze, l'elaborazione dei compensi, la gestione del libro unico del lavoro, i rapporti con enti previdenziali, assicurativi, sindacali, ecc. |
| <b>Tipologia di dati</b>       | Dati personali e sensibili   |
| <b>Categoria interessati</b>   | Lavoratori, dipendenti, soci, amministratori, collaboratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti e potenziali clienti   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione libri sociali</b><br>Libro soci, libro giornale, verbali, ecc.   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Supporti cartacei  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione polizze assicurative</b><br>Informazioni necessarie per la gestione delle polizze assicurative di cui si è contraente e/o beneficiario, ecc.   |
| <b>Tipologia di dati</b>       | Dati personali eventualmente sensibili   |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Incassi, pagamenti e operazioni bancarie</b><br>Estratti conti, bonifici, assegni, versamenti, riba, rid, ecc.  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b><br><b>Riguarda</b> | <b>Posta elettronica</b><br>Mittente, destinatari, contenuto delle e-mail  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |

|                                |  |
|--------------------------------|--|
| <b>Nome</b>                    | <b>Posta elettronica certificata</b>   |
| <b>Riguarda</b>                | Mittente, destinatari, contenuto delle e-mail certificate  |
| <b>Tipologia di dati</b>       | Dati personali eventualmente sensibili   |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Pratiche legali e contenziosi</b>   |
| <b>Riguarda</b>                | Dati giudiziari per cause civili, penali, di lavoro, amministrative, stragiudiziali, ecc. che interessano il titolare del trattamento e terzi identificati e identificabili      |
| <b>Tipologia di dati</b>       | Dati giudiziari  |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Cartacea; informatica mediante fax e/o computer, utilizzando file di suite da ufficio, quali fogli di calcolo ed elaboratori di testi; upport cartacei                           |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Predisposizione dichiarazione dei redditi e bilancio</b>  |
| <b>Riguarda</b>                | Documenti vari necessari al corretto adempimento delle misure di legge in materia societaria, fiscale e tributaria   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, terzi identificati ed identificabili  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Registrazione e gestione delle presenze nei confronti dei propri lavoratori</b>   |
| <b>Riguarda</b>                | Dati inerenti alle presenze dei propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese le ferie, le malattie, i lutti, i permessi, gli straordinari, ecc. |
| <b>Tipologia di dati</b>       | Dati personali e sensibili   |
| <b>Categoria interessati</b>   | Lavoratori, dipendenti, soci, amministratori, collaboratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Relazioni pubbliche</b>   |
| <b>Riguarda</b>                | Attività con istituzioni pubbliche, con la stampa, ecc.  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |
| <b>Nome</b>                    | <b>Revisione dei conti e certificazione di bilancio</b>  |
| <b>Riguarda</b>                | Attività di controllo sui documenti contabili, societari, fiscali, tributari, previdenziali, ecc.  |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | C  |
| <b>Nome</b>                    | <b>Selezione del personale</b>   |
| <b>Riguarda</b>                | Curriculum vitae, questionari, prove di selezione di candidati per posti di lavoro   |
| <b>Tipologia di dati</b>       | Dati personali   |
| <b>Categoria interessati</b>   | Potenziali lavoratori  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non  |
| <b>Permessi*</b>               | X  |

|   |   |
|---|---|
| <b>Nome</b><br><b>Riguarda</b>  | <b>Sistema di gestione della protezione del trattamento di dati</b><br>Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Sistema di gestione della sicurezza sul lavoro</b><br>Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>Supporti cartacei<br>C   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Sistema informativo</b><br>Informazioni necessarie per garantire il funzionamento dell'insieme di postazioni informatiche (computer fissi, portatili, palmari, ecc.), stampanti, attrezzature di rete (switch, router, access point, firewall, ecc.) e server, atto al trattamento dei dati sia dal punto di vista software che hardware; in particolare per quanto attiene ai sistemi di autenticazione ed autorizzazione |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Programma/Attrezzatura</b><br><b>Amministratori di sistema</b><br><b>Permessi*</b> | Dati personali<br>Utenti del sistema informativo, lavoratori, collaboratori<br>Strumenti elettronici<br>Sistemi operativi degli strumenti elettronici in uso<br>KOINE' SISTEMI<br>C   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Sito web</b><br>Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali<br>Terzi identificati e identificabili<br>Strumenti elettronici<br>C   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Spedizione e ricezione di documenti e materiale</b><br>Documenti di trasporto, indirizzari, ecc.   |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali<br>Clienti e fornitori<br>Strumenti elettronici e non<br>C   |
| <b>Nome</b><br><b>Riguarda</b>  | <b>Trasmissioni dati in internet (navigazione web, file sharing, ecc.)</b><br>Indirizzi degli host coinvolti, dati trasmessi, ecc. compresi indirizzi e contenuti delle pagine web visitate, contenuti delle sessioni di messengerie  |
| <b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>  | Dati personali e potenzialmente sensibili<br>Lavoratori, terzi identificati e identificabili<br>Strumenti elettronici e non<br>C  |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I inserimento, raccolta, registrazione
- C archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A annullamento, blocco, cancellazione, distruzione
- T trasporto/trasferimento
- N solo conservazione dei supporti, senza accesso ai contenuti
- D diffusione
- X equivalente ai permessi ICMAT
- L modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
COPPOLA MICHELE

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato al trattamento dei dati.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si nomina:

**RINALDI VALERIA**

quale **Incaricato del trattamento**, ai sensi dell'art.30 comma 2 del Codice, (LEGGE 104) per i seguenti trattamenti, archivi o banche dati:

|   |   |
|---|---|
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Agenda appuntamenti, visite e prenotazioni</b><br/>Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p>   |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Anagrafica condivisa e rubrica</b><br/>Dati identificativi e recapiti di clienti, fornitori, lavoratori, collaboratori e persone (fisiche e giuridiche) o enti coinvolti anche nel passato con l'attività del titolare del trattamento</p> <p>Dati personali<br/>Clienti, fornitori, terzi identificati ed identificabili<br/>Strumenti elettronici e non<br/>X</p> |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Attività di recupero crediti</b><br/>Solleciti ai clienti per il pagamento di effetti scaduti</p> <p>Dati economici riservati<br/>Clienti<br/>Strumenti elettronici e non<br/>X</p>   |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati associati</b><br/>Dati relativi agli associati</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>  |
| <p><b>Nome</b><br/><b>Riguarda</b></p> <p><b>Tipologia di dati</b><br/><b>Categoria interessati</b><br/><b>Modalità di trattamento</b><br/><b>Permessi*</b></p> | <p><b>Banca dati gestione e organizzazione eventi</b><br/>Dati relativi a location, budget, personale tecnico, ecc</p> <p>Dati personali e potenzialmente sensibili<br/>Terzi identificati e identificabili<br/>Strumenti elettronici e non<br/>X</p>   |



|  |   |
|--|---|
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati istituzioni</b><br>Dati relativi alle istituzioni con cui sussistono dei legami<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati promozione</b><br>Dati relativi alla promozione di servizi ed eventi<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati regolamento ed anagrafica contratti operatori esterni</b><br>Dati relativi ai regolamenti ed anagrafiche contratti operatori esterni<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>         | <b>Banca dati sistema prenotazione musei</b><br>Dati relativi ai servizi di prenotazione musei<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Banca dati utenti cessione terzi</b><br>Dati anagrafici e di riferimento dei soggetti fornitori di servizi della struttura potenzialmente interessati a prodotti, eventi forniti da terzi da noi individuati<br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Contabilità propria</b><br>Fatture, corrispettivi, multe, movimenti contabili, modelli fiscali, tributari, doganali, ecc.<br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili<br>Strumenti elettronici e non<br>X  |
| <b>Nome</b><br><b>Riguarda</b><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b>     | <b>Gestione acquisti e approvvigionamenti</b><br>Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori<br>Dati personali<br>Fornitori e potenziali fornitori<br>Strumenti elettronici e non<br>X   |
| <b>Nome</b><br><b>Riguarda</b><br><br><br><b>Tipologia di dati</b><br><b>Categoria interessati</b><br><b>Modalità di trattamento</b><br><b>Permessi*</b> | <b>Gestione del rapporto di lavoro nei confronti dei propri lavoratori</b><br>Relazioni con i propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese la registrazione delle presenze, l'elaborazione dei compensi, la gestione del libro unico del lavoro, i rapporti con enti previdenziali, assicurativi, sindacali, ecc.<br>Dati personali e sensibili<br>Lavoratori, dipendenti, soci, amministratori, collaboratori<br>Strumenti elettronici e non<br>C |

|                                |   |
|--------------------------------|---|
| <b>Nome</b><br><b>Riguarda</b> | <b>Gestione della clientela</b><br>Offerte, fatture, comunicazioni a clienti e potenziali clienti, attività commerciale e di marketing  |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Clienti e potenziali clienti  |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |
| <b>Permessi*</b>               | X   |
| <b>Nome</b><br><b>Riguarda</b> | <b>Pratiche legali e contenziosi</b><br>Dati giudiziari per cause civili, penali, di lavoro, amministrative, stragiudiziali, ecc. che interessano il titolare del trattamento e terzi identificati e identificabili |
| <b>Tipologia di dati</b>       | Dati giudiziari   |
| <b>Categoria interessati</b>   | Clienti, fornitori, lavoratori, terzi identificati ed identificabili  |
| <b>Modalità di trattamento</b> | Cartacea; informatica mediante fax e/o computer, utilizzando file di suite da ufficio, quali fogli di calcolo ed elaboratori di testi; upport cartacei  |
| <b>Permessi*</b>               | X   |
| <b>Nome</b><br><b>Riguarda</b> | <b>Predisposizione dichiarazione dei redditi e bilancio</b><br>Documenti vari necessari al corretto adempimento delle misure di legge in materia societaria, fiscale e tributaria                                   |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Soggetto stesso, terzi identificati ed identificabili   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |
| <b>Permessi*</b>               | X   |
| <b>Nome</b><br><b>Riguarda</b> | <b>Sistema di gestione della protezione del trattamento di dati</b><br>Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di legge (spec. d.lgs. 196/03)     |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |
| <b>Permessi*</b>               | C   |
| <b>Nome</b><br><b>Riguarda</b> | <b>Sistema di gestione della sicurezza sul lavoro</b><br>Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di legge (spec. d.lgs. 81/08)                     |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)   |
| <b>Modalità di trattamento</b> | Supporti cartacei   |
| <b>Permessi*</b>               | C   |
| <b>Nome</b><br><b>Riguarda</b> | <b>Spedizione e ricezione di documenti e materiale</b><br>Documenti di trasporto, indirizzari, ecc.   |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Clienti e fornitori   |
| <b>Modalità di trattamento</b> | Strumenti elettronici e non   |
| <b>Permessi*</b>               | X   |

## NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In accordo con i Responsabili della gestione della strumentazione elettronica (EYNARD SIMONE FLAVIO, KOINE' SISTEMI, MAUTINO ROBERTO), si conferma l'autorizzazione all'utilizzo delle attrezzature elettroniche in dotazione (computer, stampanti, fax, scanner, fotocopiatrici, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute. Inoltre, si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, come previsto dal Regolamento Informatico vigente.

In particolare gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave, ove utilizzata, non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- gli incaricati non devono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli incaricati devono attenersi alle istruzioni impartite dal Responsabile o dal Titolare del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione di essi, verificando che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'Incaricato del trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato del trattamento  
per accettazione  
RINALDI VALERIA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

### Oggetto: Lettera di incarico per trattamento dei dati in esterno.

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

**BIPOINT**

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (ASSISTENZA PROGRAMMA INFORMATICO).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

| Nome Archivio            | Sistema informativo                                       |
|--------------------------|---|
| Tipo di Dati             | Dati personali  |
| Categoria di Interessati | Utenti del sistema informativo, lavoratori, collaboratori |
| Permessi*                | X   |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
BIPOINT

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

### Oggetto: Lettera di incarico per trattamento dei dati in esterno.

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

### CITTA' DI TORINO

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (TELEFONIA PER VOCE E DATI, SIA FISSA CHE MOBILE + INTERNET).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

| Nome Archivio                   | Comunicazioni telefoniche            |
|---------------------------------|--------------------------------------|
| <b>Tipo di Dati</b>             | Dati personali                       |
| <b>Categoria di Interessati</b> | Terzi identificati ed identificabili |
| <b>Permessi*</b>                | X                                    |

#### NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
CITTA' DI TORINO

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico per trattamento dei dati in esterno.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

### COMITATO ESECUTIVO

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (ORGANO AMMINISTRATIVO).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

|  |   |
|--|---|
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Attività di recupero crediti</b><br>Dati economici riservati<br>Clienti<br>C   |
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Banca dati associati</b><br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>C                                      |
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Banca dati istituzioni</b><br>Dati personali e potenzialmente sensibili<br>Terzi identificati e identificabili<br>C                                    |
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Contabilità propria</b><br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili<br>C |
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Corrispondenza, comunicati e circolari</b><br>Dati personali<br>Clienti, fornitori, terzi identificati ed identificabili<br>C                          |
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Gestione acquisti e approvvigionamenti</b><br>Dati personali<br>Fornitori e potenziali fornitori<br>C  |



|  |  |
|--|--|
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Gestione della clientela</b><br>Dati personali<br>Clienti e potenziali clienti<br>C   |
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Gestione libri sociali</b><br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili<br>C                   |
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Gestione polizze assicurative</b><br>Dati personali eventualmente sensibili<br>Soggetto stesso, lavoratori<br>C   |
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Incassi, pagamenti e operazioni bancarie</b><br>Dati personali<br>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili<br>C |
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Pratiche legali e contenziosi</b><br>Dati giudiziari<br>Clienti, fornitori, lavoratori, terzi identificati ed identificabili<br>C   |
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Predisposizione dichiarazione dei redditi e bilancio</b><br>Dati personali<br>Soggetto stesso, terzi identificati ed identificabili<br>C                                    |
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Relazioni pubbliche</b><br>Dati personali<br>Soggetto stesso<br>C   |
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Selezione del personale</b><br>Dati personali<br>Potenziati lavoratori<br>X   |
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Sistema di gestione della protezione del trattamento di dati</b><br>Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>C    |
| <b>Nome Archivio</b><br><b>Tipo di Dati</b><br><b>Categoria di Interessati</b><br><b>Permessi*</b> | <b>Sistema di gestione della sicurezza sul lavoro</b><br>Dati personali<br>Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)<br>C                  |

## NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
COMITATO ESECUTIVO

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

### Oggetto: Lettera di incarico per trattamento dei dati in esterno.

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

### CRITICAL CASE

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (ASSISTENZA PROGRAMMA INFORMATICO).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

| Nome Archivio                   | Sistema informativo                                       |
|---------------------------------|---|
| <b>Tipo di Dati</b>             | Dati personali  |
| <b>Categoria di Interessati</b> | Utenti del sistema informativo, lavoratori, collaboratori |
| <b>Permessi*</b>                | X   |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
CRITICAL CASE

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

### Oggetto: Lettera di incarico per trattamento dei dati in esterno.

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

**CSI PIEMONTE**

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (POSTA ELETTRONICA).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

| Nome Archivio            | Posta elettronica  |
|--------------------------|--|
| Tipo di Dati             | Dati personali   |
| Categoria di Interessati | Clienti, fornitori, lavoratori, terzi identificati ed identificabili |
| Permessi*                | X  |

#### NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
CSI PIEMONTE

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico per trattamento dei dati in esterno.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

**DOTT. FRANZO ANGELO**

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (MEDICO COMPETENTE (SORVEGLIANZA SANITARIA)).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

|                                 |   |
|---------------------------------|---|
| <b>Nome Archivio</b>            | <b>Cartelle sanitarie di rischio dei lavoratori soggetti a sorveglianza sanitaria</b> |
| <b>Tipo di Dati</b>             | Dati sensibili  |
| <b>Categoria di Interessati</b> | Lavoratori, dipendenti, soci, amministratori, collaboratori                           |
| <b>Permessi*</b>                | X   |
| <b>Nome Archivio</b>            | <b>Sistema di gestione della sicurezza sul lavoro</b>                                 |
| <b>Tipo di Dati</b>             | Dati personali  |
| <b>Categoria di Interessati</b> | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori)         |
| <b>Permessi*</b>                | X   |

**NOTE:**

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.

- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
DOTT. FRANZO ANGELO



## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico per trattamento dei dati in esterno.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

**DOTT. MARCO ALBERTO  
MALAGNINO**

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (CONSULENTE PER SICUREZZA SUL LAVORO (D.LGS. 9 APRILE 2008 N.81)).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

| Nome Archivio                   | Sistema di gestione della sicurezza sul lavoro                                |
|---------------------------------|---|
| <b>Tipo di Dati</b>             | Dati personali  |
| <b>Categoria di Interessati</b> | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori) |
| <b>Permessi*</b>                | X   |

**NOTE:**

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.

- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
DOTT. MARCO ALBERTO MALAGNINO

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

### Oggetto: Lettera di incarico per trattamento dei dati in esterno.

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

### EVOLUTIVA

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (SITO WEB).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

| Nome Archivio            | Sito web                            |
|--------------------------|-------------------------------------|
| Tipo di Dati             | Dati personali                      |
| Categoria di Interessati | Terzi identificati e identificabili |
| Permessi*                | X                                   |

#### NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
EVOLUTIVA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

### Oggetto: Lettera di incarico per trattamento dei dati in esterno.

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

FORE

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (SITO WEB).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

| Nome Archivio            | Sito web                            |
|--------------------------|-------------------------------------|
| Tipo di Dati             | Dati personali                      |
| Categoria di Interessati | Terzi identificati e identificabili |
| Permessi*                | X                                   |

#### NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I inserimento, raccolta, registrazione
- C archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A annullamento, blocco, cancellazione, distruzione
- T trasporto/trasferimento
- N solo conservazione dei supporti, senza accesso ai contenuti
- D diffusione
- X equivalente ai permessi ICMAT
- L modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
FORE

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico per trattamento dei dati in esterno.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

GLS

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (TRASPORTI E SPEDIZIONI).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

| <b>Nome Archivio</b>            | <b>Spedizione e ricezione di documenti e materiale</b> |
|---------------------------------|--|
| <b>Tipo di Dati</b>             | Dati personali   |
| <b>Categoria di Interessati</b> | Clienti e fornitori                                    |
| <b>Permessi*</b>                | X  |

**NOTE:**

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
GLS



## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

### Oggetto: Lettera di incarico per trattamento dei dati in esterno.

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

### KOINE' SISTEMI

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (ASSISTENZA PROGRAMMA INFORMATICO).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

| Nome Archivio            | Trasmissioni dati in internet (navigazione web, file sharing, ecc.) |
|--------------------------|---|
| Tipo di Dati             | Dati personali e potenzialmente sensibili                           |
| Categoria di Interessati | Lavoratori, terzi identificati e identificabili                     |
| Permessi*                | X   |

#### NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
KOINE' SISTEMI

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

### Oggetto: Lettera di incarico per trattamento dei dati in esterno.

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

### LOTTOMATICA

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (ASSISTENZA PROGRAMMA SISTEMA PRENOTAZIONE MUSEI).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

| Nome Archivio                   | Banca dati sistema prenotazione musei     |
|---------------------------------|---|
| <b>Tipo di Dati</b>             | Dati personali e potenzialmente sensibili |
| <b>Categoria di Interessati</b> | Terzi identificati e identificabili       |
| <b>Permessi*</b>                | X   |

#### NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
LOTTOMATICA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

### Oggetto: Lettera di incarico per trattamento dei dati in esterno.

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

### PLUSERVICE

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (ASSISTENZA PROGRAMMA INFORMATICO).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

| Nome Archivio            | Sistema informativo                                       |
|--------------------------|---|
| Tipo di Dati             | Dati personali  |
| Categoria di Interessati | Utenti del sistema informativo, lavoratori, collaboratori |
| Permessi*                | X   |

#### NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
PLUSERVICE

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico per trattamento dei dati in esterno.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

### REALE MUTUA

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (COMPAGNIA DI ASSICURAZIONE).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

| Nome Archivio            | Gestione polizze assicurative          |
|--------------------------|--|
| Tipo di Dati             | Dati personali eventualmente sensibili |
| Categoria di Interessati | Soggetto stesso, lavoratori            |
| Permessi*                | X                                      |

**NOTE:**

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
REALE MUTUA



## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico per trattamento dei dati in esterno.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

### SEGRE MASSIMO

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (REVISORE DEI CONTI).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

|  |  |
|--|--|
| <p><b>Nome Archivio</b><br/><b>Tipo di Dati</b><br/><b>Categoria di Interessati</b><br/><b>Permessi*</b></p> | <p><b>Contabilità propria</b><br/>Dati personali<br/>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili<br/>C</p>                              |
| <p><b>Nome Archivio</b><br/><b>Tipo di Dati</b><br/><b>Categoria di Interessati</b><br/><b>Permessi*</b></p> | <p><b>Gestione libri sociali</b><br/>Dati personali<br/>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili<br/>C</p>                           |
| <p><b>Nome Archivio</b><br/><b>Tipo di Dati</b><br/><b>Categoria di Interessati</b><br/><b>Permessi*</b></p> | <p><b>Revisione dei conti e certificazione di bilancio</b><br/>Dati personali<br/>Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili<br/>X</p> |

NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
SEGRE MASSIMO

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

### Oggetto: Lettera di incarico per trattamento dei dati in esterno.

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

### SPAZIOTTANTOTTO SRL

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (CONSULENTE PER LA PROTEZIONE DEI DATI PERSONALI (D.LGS. 30 MARZO 2003 N.196)).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

| Nome Archivio            | Sistema di gestione della protezione del trattamento di dati                  |
|--------------------------|---|
| Tipo di Dati             | Dati personali  |
| Categoria di Interessati | Soggetto stesso, lavoratori (dipendenti, soci, amministratori, collaboratori) |
| Permessi*                | X   |

#### NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
SPAZIOTTANTOTTO SRL

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

### Oggetto: Lettera di incarico per trattamento dei dati in esterno.

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

### STUDIO CODA

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (COMMERCIALISTA ED ELABORAZIONE CONTABILITA').

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

|                                 |  |
|---------------------------------|--|
| <b>Nome Archivio</b>            | <b>Contabilità propria</b>   |
| <b>Tipo di Dati</b>             | Dati personali   |
| <b>Categoria di Interessati</b> | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |
| <b>Permessi*</b>                | X  |
| <b>Nome Archivio</b>            | <b>Entratel</b>  |
| <b>Tipo di Dati</b>             | Dati personali economici   |
| <b>Categoria di Interessati</b> | Soggetto stesso, clienti e fornitori, terzi identificati e identificabili                            |
| <b>Permessi*</b>                | X  |
| <b>Nome Archivio</b>            | <b>Gestione libri sociali</b>  |
| <b>Tipo di Dati</b>             | Dati personali   |
| <b>Categoria di Interessati</b> | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |
| <b>Permessi*</b>                | X  |
| <b>Nome Archivio</b>            | <b>Predisposizione dichiarazione dei redditi e bilancio</b>  |
| <b>Tipo di Dati</b>             | Dati personali   |
| <b>Categoria di Interessati</b> | Soggetto stesso, terzi identificati ed identificabili  |
| <b>Permessi*</b>                | X  |

#### NOTE:

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
STUDIO CODA

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico per trattamento dei dati in esterno.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

### STUDIO COMOLLO

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (CONSULENTE DEL LAVORO ED ELABORAZIONE CEDOLINI PAGHE).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

|                                 |  |
|---------------------------------|--|
| <b>Nome Archivio</b>            | <b>Gestione del rapporto di lavoro nei confronti dei propri lavoratori</b>         |
| <b>Tipo di Dati</b>             | Dati personali e sensibili   |
| <b>Categoria di Interessati</b> | Lavoratori, dipendenti, soci, amministratori, collaboratori                        |
| <b>Permessi*</b>                | X  |
| <b>Nome Archivio</b>            | <b>Registrazione e gestione delle presenze nei confronti dei propri lavoratori</b> |
| <b>Tipo di Dati</b>             | Dati personali e sensibili   |
| <b>Categoria di Interessati</b> | Lavoratori, dipendenti, soci, amministratori, collaboratori                        |
| <b>Permessi*</b>                | C  |

**NOTE:**

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.

- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
STUDIO COMOLLO



## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico per trattamento dei dati in esterno.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

**STUDIO NOTARILE GANELLI  
MAROCCO**

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (STUDIO NOTARILE).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

| Nome Archivio                   | Gestione libri sociali   |
|---------------------------------|--|
| <b>Tipo di Dati</b>             | Dati personali   |
| <b>Categoria di Interessati</b> | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |
| <b>Permessi*</b>                | X  |

**NOTE:**

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
STUDIO NOTARILE GANELLI MAROCCO

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico per trattamento dei dati in esterno.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si indica:

### STUDIO TOSETTO WEIGMANN

quale **Responsabile esterno del trattamento**, ex. art. 29 D.Lgs. 196/03 (STUDIO LEGALE).

Le banche dati coinvolte nel trattamento in esterno sono di seguito riportate:

|                                 |  |
|---------------------------------|--|
| <b>Nome Archivio</b>            | <b>Gestione libri sociali</b>  |
| <b>Tipo di Dati</b>             | Dati personali   |
| <b>Categoria di Interessati</b> | Soggetto stesso, clienti, fornitori, collaboratori, lavoratori, terzi identificati ed identificabili |
| <b>Permessi*</b>                | C  |

|                                 |  |
|---------------------------------|--|
| <b>Nome Archivio</b>            | <b>Pratiche legali e contenziosi</b>                                 |
| <b>Tipo di Dati</b>             | Dati giudiziari  |
| <b>Categoria di Interessati</b> | Clienti, fornitori, lavoratori, terzi identificati ed identificabili |
| <b>Permessi*</b>                | X  |

**NOTE:**

(\*) La sigla di permesso va letta secondo la seguente legenda:

- I** inserimento, raccolta, registrazione
- C** archiviazione, comunicazione, conservazione, consultazione, estrazione, organizzazione, raffronto, selezione, stampa, utilizzo
- M** elaborazione, estrazione, interconnessione, modifica, organizzazione, raffronto, selezione
- A** annullamento, blocco, cancellazione, distruzione
- T** trasporto/trasferimento
- N** solo conservazione dei supporti, senza accesso ai contenuti
- D** diffusione
- X** equivalente ai permessi ICMAT
- L** modificatore che contrae l'ambito di applicazione dei permessi ai soli dati di competenza dell'incaricato all'interno dell'ambito complessivo del trattamento

In assenza di permessi il soggetto non ha diritti e responsabilità sul trattamento.

In particolare per il trattamento in esterno dei dati personali debbono osservare le seguenti disposizioni:

- Il Responsabile del trattamento e gli incaricati devono garantire che nella struttura esterna, presso cui effettuano il trattamento dei dati loro affidati, siano adottate idonee misure di sicurezza e attuate almeno le misure minime indicate nell'Allegato B del D.Lgs. 196/03.
- Il Responsabile del trattamento e gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico, nel caso ne utilizzino uno, durante una sessione di trattamento dei dati personali.
- Il Responsabile del trattamento e gli incaricati devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.

- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati al Responsabile del trattamento ed agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi fino alla loro restituzione, verificando che non vi accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

Il Responsabile del trattamento in esterno dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

Il Responsabile del trattamento in esterno  
per accettazione  
STUDIO TOSETTO WEIGMANN

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico al Responsabile della gestione e della manutenzione degli strumenti elettronici.**

In qualità di Responsabile della sicurezza del trattamento dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**MAUTINO ROBERTO**

l'incarico di **Responsabile della gestione e della manutenzione degli strumenti elettronici.**

Il Responsabile della gestione e della manutenzione degli strumenti elettronici ha il compito di:

- Attivare le credenziali di autenticazione agli Incaricati del trattamento, su indicazione del Responsabile del trattamento, per tutti i trattamenti effettuati con strumenti informatici.
- Definire quali politiche adottare per la protezione dei sistemi contro i virus informatici e verificarne l'efficacia con cadenza almeno semestrale.
- Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers").
- Informare il Responsabile del trattamento nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici è autorizzato ad accedere agli archivi presenti sugli elaboratori elettronici per svolgere le proprie mansioni; altresì è tenuto alla massima riservatezza, con espresso e permanente divieto di comunicare o diffondere qualunque dato personale e soprattutto sensibile di cui venga a conoscenza durante la propria attività di gestione e manutenzione.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

Il Responsabile della gestione e  
della manutenzione degli strumenti elettro-  
nici  
per accettazione  
MAUTINO ROBERTO

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico al Responsabile della gestione e della manutenzione degli strumenti elettronici.**

In qualità di Responsabile della sicurezza del trattamento dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**EYNARD SIMONE FLAVIO**

l'incarico di **Responsabile della gestione e della manutenzione degli strumenti elettronici**.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici ha il compito di:

- Attivare le credenziali di autenticazione agli Incaricati del trattamento, su indicazione del Responsabile del trattamento, per tutti i trattamenti effettuati con strumenti informatici.
- Definire quali politiche adottare per la protezione dei sistemi contro i virus informatici e verificarne l'efficacia con cadenza almeno semestrale.
- Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers").
- Informare il Responsabile del trattamento nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici è autorizzato ad accedere agli archivi presenti sugli elaboratori elettronici per svolgere le proprie mansioni; altresì è tenuto alla massima riservatezza, con espresso e permanente divieto di comunicare o diffondere qualunque dato personale e soprattutto sensibile di cui venga a conoscenza durante la propria attività di gestione e manutenzione.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

Il Responsabile della gestione e  
della manutenzione degli strumenti elettro-  
nici  
per accettazione  
EYNARD SIMONE FLAVIO

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

### Oggetto: Lettera di incarico per Amministratore di sistema.

In qualità di Responsabile della sicurezza del trattamento dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03), del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03) e dei provvedimenti del 25 giugno 2009 (G.U. n. 149 del 30 giugno 2009) e del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008) del Garante per la protezione dei dati personali, previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, si affida a:

**KOINE' SISTEMI**

l'incarico di **Amministratore di sistema**, quale Responsabile del trattamento ex. art. 29 D.Lgs. 196/03 per i seguenti trattamenti, archivi o banche dati:

|                                |   |
|--------------------------------|---|
| <b>Nome<br/>Riguarda</b>       | <b>Sistema informativo</b><br>Informazioni necessarie per garantire il funzionamento dell'insieme di postazioni informatiche (computer fissi, portatili, palmari, ecc.), stampanti, attrezzature di rete (switch, router, access point, firewall, ecc.) e server, atto al trattamento dei dati sia dal punto di vista software che hardware; in particolare per quanto attiene ai sistemi di autenticazione ed autorizzazione |
| <b>Tipologia di dati</b>       | Dati personali  |
| <b>Categoria interessati</b>   | Utenti del sistema informativo, lavoratori, collaboratori   |
| <b>Modalità di trattamento</b> | Strumenti elettronici   |
| <b>Programma/Attrezzatura</b>  | Sistemi operativi degli strumenti elettronici in uso  |

Le funzioni attribuite riguardano la gestione, l'amministrazione, la manutenzione e il controllo dei sistemi hardware e software utilizzati nel trattamento indicato, limitate alle competenze specifiche: assistenza programma informatico.

L'Amministratore di sistema ha il compito di:

- sovrintendere al buon funzionamento di banche di dati e di sistemi software complessi
- proteggere le banche dati e i sistemi software complessi dal rischio di intrusione o di accesso non autorizzato
- registrare gli accessi logici (autenticazione informatica) alle banche di dati ed ai sistemi software complessi: registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate; devono essere conservate per un congruo periodo, non inferiore a sei mesi; inoltre devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità
- Informare il Responsabile della sicurezza dei dati personali nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.
- Fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
- Predisporre un elenco con gli estremi identificativi delle persone fisiche preposte ad amministrare i sistemi oggetto di codesta nomina.

Inoltre per il trattamento in esterno dei dati personali si debbono osservare le seguenti disposizioni:

- nella struttura esterna, presso cui si effettui il trattamento dei dati, devono essere adottate idonee misure di sicurezza e devono essere attuate almeno le misure minime indicate nell' Allegato B del D.Lgs. 196/03.
- durante una sessione di trattamento dei dati personali, lo strumento elettronico non deve essere lasciato incustodito e accessibile

Si comunica preventivamente che l'operato dell'Amministratore di Sistema sarà oggetto, con cadenza almeno annuale, di attività di verifica, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

L'Amministratore di sistema (per mezzo del personale incaricato) è autorizzato ad accedere agli archivi presenti sugli elaboratori elettronici per svolgere le proprie mansioni; altresì è tenuto alla massima riservatezza, con espresso e permanente divieto di comunicare o diffondere qualunque dato personale e soprattutto sensibile di cui venga a conoscenza durante la propria attività di gestione e manutenzione.

L'Amministratore di sistema dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte, garantendo il pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Amministratore di sistema  
per accettazione  
KOINE' SISTEMI



**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato della custodia delle copie delle credenziali di autenticazione.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si affida a:

**LEON FRANCESCA**

l'incarico di **Incaricato della custodia delle copie delle credenziali di autenticazione.**

L'Incaricato della custodia delle copie delle credenziali di autenticazione ha il compito di:

- Attivare le credenziali di autenticazione agli Incaricati del trattamento, su indicazione del Responsabile del trattamento, per tutti i trattamenti effettuati con strumenti informatici.
- Gestire e custodire le credenziali per l'accesso ai dati degli Incaricati del trattamento.
- Istruire gli Incaricati del trattamento sull'uso delle parole chiave, e sulle caratteristiche che debbono avere, e sulle modalità per la loro modifica in autonomia.
- Revocare tutte le credenziali non utilizzate in caso di perdita della qualità che consentiva all'incaricato l'accesso ai dati personali.
- Revocare le credenziali per l'accesso ai dati degli Incaricati del trattamento nel caso di mancato utilizzo per oltre 6 (sei) mesi.

L'Incaricato della custodia delle copie delle credenziali di autenticazione dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato della custodia delle copie  
delle credenziali di autenticazione  
per accettazione  
LEON FRANCESCA

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato delle copie di sicurezza delle banche dati elettroniche.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), premesso che le operazioni volte a garantire la disponibilità dei dati attraverso le copie di sicurezza delle banche dati elettroniche sono:

- definite a priori dal Responsabile della Gestione della Strumentazione Elettronica
- implementate per l'esecuzione automatica

si affida a:

**MAUTINO ROBERTO**

l'incarico di **Incaricato delle copie di sicurezza delle banche dati elettroniche.**

L'Incaricato ha il compito di gestire e sovrintendere l'**esecuzione** delle copie di sicurezza delle banche dati elettroniche. In particolare :

- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal Responsabile del trattamento
- Assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro, verificando che l'usura dei supporti utilizzati non possa pregiudicare il corretto salvataggio dei dati e la loro correttezza e consistenza
- Di provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato.
- Di segnalare tempestivamente al Responsabile della gestione e della manutenzione degli strumenti elettronici, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.
- Seguire le seguenti istruzioni per le banche dati elettroniche TUTTI
  1. Il supporto di memorizzazione da utilizzare è HARD DISK ESTERNO .
  2. Il numero di supporti da impiegare ad ogni salvataggio è 1. Il numero di supporti da usare annualmente è 1+1.
  3. La periodicità del salvataggio deve essere: TUTTI I GIORNI.
  4. Le copie devono essere conservate presso la sede, in un locale controllato e protetto.
  5. I supporti magnetici ed ottici per la copia possono essere riutilizzati al massimo una volta durante la stessa settimana ed al più complessivamente 100 (cento) volte dalla data di primo utilizzo e comunque, qualora fosse indicata, non oltre la data di scadenza.
  6. L'etichetta identificativa da apporre su ciascun supporto magnetico od ottico per la copia deve riportare l'indicazione del giorno della settimana a cui corrisponde il salvataggio, la data di primo utilizzo e un numero progressivo univoco.
  7. Per effettuare la copia attenersi rigorosamente al manuale di istruzioni del dispositivo per quanto concerne le procedure di salvataggio
  8. E' consigliato controllare l'esito della copia con procedure automatiche per il controllo di esatta riproduzione rispetto ai dati originali.
  9. Per effettuare il ripristino in caso di danneggiamento degli archivi, attenersi scrupolosamente al manuale di istruzioni del dispositivo di copia o richiedere l'intervento di personale specializzato e qualificato.

L'Incaricato delle copie di sicurezza delle banche dati elettroniche dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato delle copie di sicurezza  
delle banche dati elettroniche  
per accettazione  
MAUTINO ROBERTO

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato delle copie di sicurezza delle banche dati elettroniche.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), premesso che le operazioni volte a garantire la disponibilità dei dati attraverso le copie di sicurezza delle banche dati elettroniche sono:

- definite a priori dal Responsabile della Gestione della Strumentazione Elettronica
- implementate per l'esecuzione automatica

si affida a:

**ROBERTO MAUTINO**

l'incarico di **Incaricato delle copie di sicurezza delle banche dati elettroniche**.

L'Incaricato ha il compito di gestire e sovrintendere **la custodia** delle copie di sicurezza delle banche dati elettroniche. In particolare :

- Assicurarsi della conservazione in luogo adatto e sicuro delle copie di sicurezza dei dati relativi alle banche dati elettroniche TUTTI, verificando che l'usura dei supporti utilizzati non possa pregiudicare il corretto salvataggio dei dati e la loro correttezza e consistenza
- Di provvedere a conservare con la massima cura e custodia le copie di sicurezza, impedendovi l'accesso da parte di personale non autorizzato.
- Una copia integrale dei salvataggi è conservata all'esterno della sede a cura dell'incaricato e sostituita periodicamente (almeno ogni 6 mesi)

L'Incaricato delle copie di sicurezza delle banche dati elettroniche dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato delle copie di sicurezza  
delle banche dati elettroniche  
per accettazione  
ROBERTO MAUTINO

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di incarico all'Incaricato delle copie di sicurezza delle banche dati elettroniche.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), premesso che le operazioni volte a garantire la disponibilità dei dati attraverso le copie di sicurezza delle banche dati elettroniche sono:

- implementate per l'esecuzione automatica

si affida a:

**MAUTINO ROBERTO**

l'incarico di **Incaricato delle copie di sicurezza delle banche dati elettroniche.**

L'Incaricato ha il compito di gestire e sovrintendere **la custodia** delle copie di sicurezza delle banche dati elettroniche. In particolare :

- Assicurarsi della conservazione in luogo adatto e sicuro delle copie di sicurezza dei dati relativi alle banche dati elettroniche TUTTI, verificando che l'usura dei supporti utilizzati non possa pregiudicare il corretto salvataggio dei dati e la loro correttezza e consistenza
- Di provvedere a conservare con la massima cura e custodia le copie di sicurezza, impedendovi l'accesso da parte di personale non autorizzato.
- Una copia integrale dei salvataggi è conservata all'esterno della sede a cura dell'incaricato e sostituita periodicamente (almeno ogni 6 mesi)

L'Incaricato delle copie di sicurezza delle banche dati elettroniche dichiara di aver preso conoscenza dei compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Incaricato delle copie di sicurezza  
delle banche dati elettroniche  
per accettazione  
MAUTINO ROBERTO

## Appendice E

# Facsimili per la gestione informatica

### E.1 Elaboratori informatici

Un soggetto fiscale che ha a carico uno o più elaboratori (PC, SERVER, NOTEBOOK) sul libro dei cespiti deve specificare che tipologia di attività il computer svolge all'interno della struttura. Un elaboratore può essere utilizzato per progettazione o per processare dati necessari alla produzione, in questo caso se non contiene dati personali e/o sensibili dei clienti, se non accede ad internet e non riceve posta non è soggetto alle procedure previste dalla vigente normativa in materia di privacy.

### E.2 Credenziali di autenticazione

Qualora un elaboratore contenga dati di clienti, fornitori, dipendenti, ecc.: - personali (anagrafiche, nome, cognome e indirizzo) - sensibili (informazioni contabili / dati giudiziari o riferimenti a contenziosi) deve essere dotato di password e, se non disponete di Server con Active Directory, assegnato unicamente ad una persona che diventerà responsabile dell'attività svolta dall'elaboratore stesso. La password deve essere di almeno 8 caratteri alfanumerici (es. R0s4n3r4); un suggerimento è utilizzare nomi facili da ricordare e sostituire alle A=4 E=3 I=1 O=0 (es. Carolina à C4r0l1n4). Le password devono essere trascritte in busta chiusa e conservate in luogo idoneo. Questo perché qualora il titolare o i dipendenti non potessero o decidessero di non utilizzare più l'elaboratore deve essere individuata una modalità per riappropriarsi dell'elaboratore senza effettuare un illecito (forzando una password). Qualora l'elaboratore venisse sottratto dalla vostra struttura dovrete provvedere ad allegare alla denuncia di furto la dichiarazione che al momento del furto l'elaboratore era dotato di password nel rispetto della normativa vigente.

### E.3 Antivirus

Il sistema AntiVirus serve a proteggere dal degrado e dal pericolo di perdita (dovuta a un'infezione del pc) i dati dei vostri clienti e fornitori. Tale sistema deve essere installato e aggiornato anche su pc non connessi alla rete per l'eventuale pericolo derivante dall'utilizzo di floppy / CD contenenti virus.

### E.4 Firewall

Il sistema Firewall deve essere installato o sulle singole postazioni (es. Norton Internet Security) o a monte della rete locale (tipo hardware) se presente una serie di pc in rete con possibilità di salvare ed utilizzare dati personali e sensibili dei clienti. Tale protezione serve inoltre per evitare l'intercettazione delle informazioni presenti nella vostra rete da parte di estranei. L'obiettivo dell'hacker

è sondare se nelle reti esistono protezioni e, trovata una via di accesso o un punto di debolezza, prendere i dati per utilizzarli e/o diffonderli in modo illecito.

## **E.5 Back-Up (salvataggio dei dati)**

I dati da salvare sono quelli che riguardano la contabilità dell'azienda o dati che vi possono essere richiesti da vostri clienti, fornitori e dalla Pubblica Autorità, che portano al contenzioso qualora non si rendano disponibili. Il salvataggio può essere effettuato su svariati supporti: CD, Floppy, nastro Dat, cassetta ZIP. Esso deve essere effettuato a seconda delle esigenze e logiche della vostra attività, preferibilmente una volta al giorno. Inoltre, almeno una volta al mese, copia dello stato dell'arte dell'azienda deve essere salvata in luogo idoneo preferibilmente all'esterno della struttura (portare un supporto cd/floppy/cassetta Dat all'esterno). Il motivo di tale procedura è semplice, in quanto se si verificassero incendi o eventi distruttivi l'azienda deve poter ricostruire la contabilità e recuperare dati che, se persi, potrebbero portare a contenziosi. Periodicamente verificate l'usura dei supporti: è inutile effettuare tanti salvataggi se il supporto non funziona!!! Provate ad effettuare operazioni di ripristino e verificate che i dati salvati siano poi riutilizzabili all'interno dei vostri elaboratori.

## **E.6 Banche Dati Autorizzate**

Trattare i dati vuol dire, oltre a conservarli, fare analisi, valutazioni, modificarli inserirli in preventivi, in e-mail etc etc. Esistono dei clienti che si vedono una sola volta, o fornitori non abituali, di cui non trattiamo i dati (loro non devono darci il consenso), ma ricordiamoci che molte attività sono collegate alla gestione abituale dei clienti e fornitori. Tali clienti e fornitori ci devono dare un'autorizzazione a trattare i loro dati in formato magnetico, elettronico e cartaceo. Avere banche dati non autorizzate ci rende colpevoli! Ogni cliente e fornitore di cui trattiamo i dati in maniera illegale può farci causa, valutiamo bene l'entità e il pericolo che si corre, memori del fatto che in ogni azienda si sarà sentito dire: Pensa se Tizio vedesse questo documento.... Alla luce di ciò, sarà sicuramente utile predisporre una metodologia di richiesta del consenso per il trattamento (Es invio via fax, attraverso raccomandata, durante visita o contatto diretto).

## **E.7 Navigazione in Internet e caselle di posta elettronica**

In seguito al Provvedimento del Garante per la protezione dei dati personali, n.13 del 1° marzo 2007, Linee guida per posta elettronica ed internet, si è reso necessario intraprendere particolari procedure di sicurezza al fine di garantire la liceità dei trattamenti, soprattutto nei riguardi dei dipendenti di qualunque tipo di attività che utilizzi strumentazioni elettroniche connesse alla rete di comunicazione pubblica Internet.

A tal fine, con lo scopo di recepire alcune delle nuove misure previste dal provvedimento, sono stati predisposti i modelli:

- MOD\_SITI - Elenco siti web correlati con l'attività lavorativa
- MOD\_EMAIL - Elenco caselle di posta elettronica

necessari per il Regolamento Informatico (RI).

### **E.7.1 Siti web correlati con l'attività lavorativa**

Il primo modello, MOD\_SITI - Elenco siti web correlati con l'attività lavorativa, deve essere compilato tenendo conto di tutti i siti web abitualmente consultati e utilizzati dagli incaricati del trattamento nello svolgimento delle attività loro affidate: tale elenco deve contenere l'indicazione della presenza di eventuali meccanismi di autenticazione (es. richiesta di login e password) e la

descrizione sintetica dei contenuti e delle operazioni eseguibili. La finalità di questo elenco è quella di censire i siti utili, tenere sotto controllo le operazioni di trattamento ed informare gli incaricati del trattamento al riguardo dei siti leciti.

Per una compilazione efficace e veritiera, si consiglia di distribuire a tutti gli incaricati il modulo in bianco, richiedendo di inserire gli indirizzi dei siti utilizzati abitualmente (anche quelli non strettamente connessi con il lavoro); raccolti i moduli, un responsabile dovrà razionalizzare i dati, scremando quei siti per i quali non sussiste un'attinenza con l'attività lavorativa. Un metodo diverso, se si possiede uno strumento firewall predisposto allo scopo, prevede di consultare le statistiche di navigazione della propria azienda e sulla base di tali dati compilare il modulo, senza coinvolgere gli incaricati.

## **E.7.2 Caselle di posta elettronica**

Il secondo modello, MOD\_EMAIL - Elenco caselle di posta elettronica, deve essere compilato riportando l'elenco di tutte le caselle di posta elettronica utilizzate dall'azienda e/o assegnate agli incaricati; per ogni casella deve essere indicato l'utilizzatore primario (colui che riceve ed invia comunicazioni) o, nel caso la casella sia condivisa tra più incaricati, devono essere indicati tutti gli utilizzatori; inoltre, deve essere indicato se la casella è da considerarsi personale dell'utilizzatore oppure lavorativa (non utilizzata per scambio di comunicazioni di carattere personale e riservato). Infine per ogni casella deve essere indicato un fiduciario, cioè un incaricato che possa accedere alla casella in caso di necessità ed in assenza dell'utilizzatore: a tale proposito e nel limite del possibile, conviene indicare come unico referente aziendale il Custode delle copie delle credenziali di autenticazione (nominato all'interno del DPS). La finalità di questo elenco è quella di censire le caselle, stabilendone la finalità, di prevedere un metodo lecito con cui accedere alle caselle lavorative in casi eccezionali.

Per la compilazione si consiglia di procedere, come suggerito in precedenza, richiedendo a tutti gli incaricati quali caselle di posta utilizzano, successivamente, razionalizzando i dati, stabilendo quali caselle debbano essere considerate come personali o lavorative ed infine eleggendo un fiduciario unico oppure indicando quello scelto da ciascuno.

## **E.8 Modelli**

Seguono i modelli per compilare

- l'elenco degli elaboratori
- l'elenco dei siti web correlati con l'attività lavorativa
- l'elenco delle caselle di posta elettronica
- il cambio delle credenziali di autenticazione
- le segnalazioni dei rischi hardware
- le segnalazioni dei rischi software
- il report dei virus e degli attacchi informatici rilevati
- l'autorizzazione temporanea all'uso di un personal computer
- l'autorizzazione alle operazioni di manutenzione/riparazione di un elaboratore elettronico da parte di ditte specializzate



ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

| # | Marca<br>Modello<br>S/N | Caratteristiche<br>CPU, RAM,<br>HD, ecc. | Sistema<br>Operativo | Indirizzo IP | Nome Host | Data<br>installazione | Utilizzatori |
|---|-------------------------|--|----------------------|--------------|-----------|-----------------------|--------------|
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |
|   |                         |  |                      |              |           |                       |              |

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

| # | Sito Web | Necessita<br>autenticazione | Descrizione contenuti e attività |
|---|----------|-----------------------------|----------------------------------|
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |
|   |          |                             |                                  |

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

| # | Casella | Lavorativa<br>o personale | Utilizzatore | Fiduciario |
|---|---------|---------------------------|--------------|------------|
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |
|   |         |                           |              |            |

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

Io sottoscritto (cognome e nome)

\_\_\_\_\_

Incaricato al trattamento, (spuntare di seguito il caso appropriato)

- autorizzato all'uso dell'autenticazione di rete
- autorizzato all'uso dell'elaboratore \_\_\_\_\_
- autorizzato all'uso del programma \_\_\_\_\_

e (spuntare di seguito il caso appropriato)

- mediante il nome utente \_\_\_\_\_
- mediante parola chiave su BIOS

dichiaro

che la parola chiave da me utilizzata

nel periodo \_\_\_\_\_ dal \_\_\_\_\_ al \_\_\_\_\_

è

\_\_\_\_\_

**NOTE**

La password deve essere di almeno 8 caratteri alfanumerici, possibilmente contenente anche caratteri minuscoli, maiuscoli e segni di punteggiatura

Nel caso di password su BIOS, utilizzare password lunghe pari al massimo numero di caratteri accettati dal sistema.

Inserire questo modulo compilato in una busta chiusa, recante all'esterno i seguenti dati: nome e cognome dell'incaricato, identificativo dell'elaboratore e data della modifica. Consegnare la busta all'incaricato della custodia delle credenziali.

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

| <b>Data</b> | <b>Apparecchiature</b> | <b>Reimpiego/Riciclaggio</b> | <b>Misure adottate</b> |
|-------------|------------------------|------------------------------|------------------------|
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |
|             |                        |                              |                        |

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

dal \_\_\_\_\_ al \_\_\_\_\_

| Data | Sistema di elaborazione | Parte coinvolta | Tipo di rischio | Gravità del rischio | Azioni correttive e preventive |
|------|-------------------------|-----------------|-----------------|---------------------|--------------------------------|
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |
|      |                         |                 |                 |                     |                                |

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

dal \_\_\_\_\_ al \_\_\_\_\_

| <b>Data</b> | <b>Sistema di elaborazione</b> | <b>Software coinvolto</b> | <b>Tipo di rischio</b> | <b>Gravità del rischio</b> | <b>Azioni correttive e preventive</b> |
|-------------|--------------------------------|---------------------------|------------------------|----------------------------|---------------------------------------|
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |
|             |                                |                           |                        |                            |                                       |

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

dal \_\_\_\_\_ al \_\_\_\_\_

|                            |                 |                              |  |
|----------------------------|-----------------|------------------------------|--|
| <b>Nome del firewall</b>   | <b>Versione</b> | <b>Data di installazione</b> | <b>Periodicità dell'aggiornamento</b><br><input type="radio"/> Giornaliera <input type="radio"/> Bimestrale<br><input type="radio"/> Settimanale <input type="radio"/> Trimestrale<br><input type="radio"/> Quindicinale <input type="radio"/> Semestrale<br><input type="radio"/> Mensile <input type="radio"/> Altro _____ |
| <b>Nome dell'antivirus</b> | <b>Versione</b> | <b>Data di installazione</b> | <b>Periodicità dell'aggiornamento</b><br><input type="radio"/> Giornaliera <input type="radio"/> Bimestrale<br><input type="radio"/> Settimanale <input type="radio"/> Trimestrale<br><input type="radio"/> Quindicinale <input type="radio"/> Semestrale<br><input type="radio"/> Mensile <input type="radio"/> Altro _____ |

| <b>Data</b> | <b>Tipologia (virus/attacco)</b> | <b>Nome del virus o dell'attacco</b> | <b>Provenienza</b> | <b>Danno</b> | <b>Azioni correttive e preventive</b> |
|-------------|----------------------------------|--------------------------------------|--------------------|--------------|---------------------------------------|
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |
|             |                                  |                                      |                    |              |                                       |



**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

**Oggetto: Incarico ed autorizzazione al trattamento ai sensi del D. Lgs. n. 196 del 30 giugno 2003 e Allegato B, disciplinare tecnico in materia di misure minime di sicurezza.**

Gent. Sig.ra / Egr. Sig.

Le comunichiamo che l'art. 30, D. Lgs. 30.6.2003, n. 196, evidenzia che il personale/collaboratore che effettua il trattamento di dati personali per conto della Società / Ente, assume il ruolo di incaricato del trattamento. Pertanto, nello svolgimento della Sua prestazione Ella potrà eseguire il trattamento dei dati personali, (ivi compresa la comunicazione), inerenti alle attività di Sua competenza. Con l'occasione Le ricordiamo che Ella dovrà usare la massima riservatezza e discrezione nella tenuta dei dati di cui sopra e nella conseguente loro protezione.

Le comunichiamo le seguenti misure di sicurezza a cui Ella dovrà scrupolosamente attenersi :

- Le è stata consegnata una password per l'accesso ai dati dall'incaricato dell'azienda \_\_\_\_\_; tale password è sotto la Sua responsabilità e dovrà essere tenuta strettamente riservata. Ella potrà autonomamente sostituirla, previa comunicazione in busta chiusa al custode delle password , il quale accederà a tale informazione solo in caso di assoluta necessità.
- Ella dovrà accedere ai soli dati personali la cui conoscenza è strettamente necessaria allo svolgimento dei compiti che Le sono assegnati;
- oltre alla password per l'accesso ai dati di cui sopra, Le viene attribuito un codice identificativo personale per l'utilizzazione dell'elaboratore stesso;
- sarà inoltre necessario inserire apposita password per la disattivazione dello screen saver, al fine di tutelare i dati in Sua assenza;
- con riferimento al trattamento di dati personali su supporto cartaceo, Le comunichiamo che essi devono essere conservati in archivi ad accesso selezionato.

Le comunichiamo che l'art. 26 individua particolari categorie di dati, denominati sensibili, che devono essere sottoposti ad una tutela particolare. In particolare sono da ritenersi sensibili i dati relativi a origine razziale ed etnica, le convinzioni religiose o filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o ad organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale. Nel caso di trattamento dei sopraindicati dati sensibili, Ella dovrà inoltre attenersi alle seguenti misure di sicurezza :

- eventuali supporti di memorizzazione riutilizzabili (floppy disks, nastri,) contenenti dati sensibili, possono essere riutilizzati solo se i dati precedentemente contenuti non sono più in alcun modo recuperabili (i dischetti quindi devono essere formattati ed i nastri riscritti), altrimenti vanno distrutti;
- per il trattamento di dati su supporto cartaceo, gli elenchi devono essere custoditi in contenitori chiusi a chiave;
- Ella è autorizzata ad effettuare il trattamento dei dati sensibili di cui sopra tramite l'uso dei programmi messi a Sua disposizione, sui computer a cui Ella ha accesso.

Le rammentiamo che l'inosservanza delle misure di sicurezza per i dati personali espone anche gli incaricati all'applicazione di sanzioni.

La preghiamo di restituirci copia della presente firmata per ricevuta.

Distinti saluti.

(luogo) \_\_\_\_\_, lì (data) \_\_\_\_\_

Il Responsabile della gestione della strumentazione elettronica  
EYNARD SIMONE FLAVIO

TIMBRO E FIRMA  
per accettazione

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

**Oggetto: Autorizzazione per addetti alla manutenzione e assistenza sugli elaboratori elettronici.**

Con la presente autorizziamo il personale, incaricato dalla Vostra Società, ad effettuare operazioni di manutenzione ed assistenza su elaboratori e programmi che contengono dati personali, oggetto della tutela di cui al D.Lgs. n. 196 del 30 giugno 2003, Codice in materia di protezione dei dati personali. L'autorizzazione all'accesso ai suddetti dati è limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di manutenzione.

Il Codice prevede la tutela delle persone fisiche e giuridiche e di altri soggetti rispetto al trattamento dei dati personali. In particolare esso impone che tali dati siano trattati in modo lecito, corretto e sicuro per ridurre al minimo i rischi di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito.

Nell'ambito dello svolgimento delle attività sugli elaboratori elettronici potrebbe accadere che gli addetti delle accedano a banche dati e/o a sistemi contenenti dati personali. Pertanto, si richiede di istruire gli addetti sui loro compiti non solo in relazione ai dati personali ma su tutti i dati aziendali. In particolare durante gli interventi essi sono tenuti a:

- trattare tutti i dati, di cui vengano a conoscenza durante l'esecuzione dell'intervento in modo lecito, corretto e sicuro per ridurre al minimo i rischi di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito da parte di terzi;
- accedere solamente ai dati necessari per l'esecuzione dell'intervento richiesto, con l'espresso divieto di aggiornare, modificare, correggere, cancellare o salvare i relativi dati senza una preventiva espressa autorizzazione da parte del titolare o di un responsabile;
- mantenere assoluto riserbo sui dati di cui vengano eventualmente a conoscenza durante l'esecuzione dell'intervento richiesto;
- non asportare supporti informatici o cartacei contenenti dei dati, senza una preventiva espressa autorizzazione da parte del titolare o di un responsabile;
- adottare, prima di allontanarsi dalla postazione di lavoro, le misure a disposizione per evitare l'accesso ai dati da parte di altri soggetti che non siano autorizzati.

Inoltre, nell'ipotesi di assistenza da remoto, al fine di poter effettuare un intervento gli addetti devono:

- essere preventivamente autorizzati;
- utilizzare un connessione sicura;
- segnalare al titolare o al responsabile sia l'inizio che la fine del collegamento.

Nel caso si rendesse necessario l'invio o la consegna di supporti magnetici oppure ottici contenenti dati per la verifica di eventuali anomalie utilizzando opportuni apparati hardware e/o software installati presso i vostri locali, gli addetti devono garantire la cancellazione dei dati ricevuti al termine della verifica. Qualora poi, emergesse l'esigenza di trasmettere i supporti a soggetti terzi per ulteriori verifiche, deve essere richiesta esplicita autorizzazione al titolare o al responsabile del trattamento.

Nel caso di ritiro di server, pc, hard disk, supporti magnetici o ottici, si devono evitare sia accessi non autorizzati, sia trattamenti non consentiti; si richiede altresì massima riservatezza e discrezione nel trattamento dei dati.

Distinti saluti.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

TIMBRO E FIRMA  
per accettazione

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTÀ' 1  
10122 - TORINO (TO)  
PIVA 08545970017

| Data | Amministr. di sistema | Note | Esito   |
|------|-----------------------|------|---|
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |
|      |                       |      | <input type="checkbox"/> Positivo <input type="checkbox"/> Negativo |

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

19/05/2014

**Oggetto: Lettera di assegnazione.**

In qualità di Responsabile della sicurezza dei dati personali, ai sensi del Codice in materia di dati personali (D.Lgs. 196/03) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. 196/03), si assegnano a:

\_\_\_\_\_

i seguenti dispositivi mobili personali con l'incarico di controllare e mantenere attive tutte le protezioni per la riservatezza e sicurezza dei dati personali trattati a nome per conto del titolare del trattamento.

- Tablet: \_\_\_\_\_  
S/N: \_\_\_\_\_
- Smartphone: \_\_\_\_\_  
IMEI: \_\_\_\_\_

L'utilizzatore e incaricato del trattamento dichiara di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza e si impegna ad adottare tutte le misure necessarie a proteggere gli strumenti da accessi non autorizzati e sottrazioni di informazioni.

L'utilizzatore si obbliga ad attenersi alle disposizioni di cui sopra, a quelle in materia di Privacy, contenute nel Codice in materia di dati personali e nel Regolamento del Sistema Informativo, per quanto concerne il trattamento di dati personali con strumenti elettronici e non.

Il mancato rispetto o la violazione del Regolamento potrebbe comportare provvedimenti disciplinari, anche gravi. In particolare si rileva come «l'abuso del telefono aziendale può costituire giustificato motivo soggettivo di licenziamento indipendentemente dall'entità del danno creato al datore di lavoro»(Cassazione, aprile 2002).

Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sui dispositivi saranno realizzate nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e dei regolamenti aziendali.

(luogo)\_\_\_\_\_, lì (data)\_\_\_\_\_

Il Responsabile della sicurezza dei dati personali  
LEON FRANCESCA

L'Utilizzatore per accettazione

# Appendice F

## Facsimili

Seguono i modelli per

- informativa, acquisizione del consenso e diritti dell'interessato
- contratti con collaboratori, dipendenti ed agenti
- lettere di incarico temporaneo e di cessazione dell'incarico
- dichiarazioni per il cambio o il trasferimento di sede
- postille e diciture per documenti contabili, di trasporto e comunicazioni varie
- lettere per fornitori non coinvolti direttamente nel trattamento dei dati, ma che accedono ai locali (es. imprese di pulizie)
- scarico di responsabilità in seguito al furto di elaboratori contenenti dati

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

**Informativa ed acquisizione di consenso per il trattamento di dati personali ai sensi del D. Lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali.**

**INFORMATIVA**

Ai sensi dell'art. 13, D. Lgs. 30 giugno 2003, n. 196, la Società ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA informa che, per l'instaurazione e per l'esecuzione dei rapporti contrattuali in corso con Voi, è in possesso di dati a Voi relativi qualificati dalla legge come personali o come identificativi.

Tali dati sono oggetto di trattamento per finalità gestionali e legate alle richieste della Pubblica Amministrazione e per ottemperare agli obblighi previsti dalle vigenti norme legislative mediante la consultazione, l'elaborazione, il raffronto, l'interconnessione, la comunicazione, (la diffusione) ed ogni altra opportuna operazione di trattamento. I dati sono trattati su supporto elettronico, magnetico, cartaceo.

Si precisa che il conferimento dei dati è obbligatorio per tutto quanto è inerente agli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli ovvero l'eventuale rifiuto al trattamento potrà determinare l'impossibilità della Società ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA a dar corso ai rapporti contrattuali.

I dati in questione potranno essere portati a conoscenza di persone fisiche o giuridiche quali responsabili della Società ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA ed a persone fisiche individuate dalla stessa quali incaricati a compiere operazioni di trattamento.

Essi potranno inoltre essere comunicati (in Italia e all'estero) a:

- agenti;
- società finanziarie, di leasing, di factoring, ecc.;
- banche ed istituti di credito;
- professionisti e consulenti;
- società operanti nel settore dei trasporti, spedizioni e comunicazioni

Si informa che, in relazione al trattamento dei dati che La riguardano, la Sua Azienda può esercitare i diritti di cui all'art. 7, D. Lgs. 196/2003.

Titolare del trattamento è: D'ACRI ANTONIO MARCO  
 Responsabile del trattamento è : LEON FRANCESCA

**ACQUISIZIONE DEL CONSENSO**

La Società \_\_\_\_\_ preso atto dell'informativa ricevuta e dell'art. 7 del D.Lgs. 196/03, esprime il proprio consenso al trattamento ed alla comunicazione dei propri dati per le finalità e nei limiti dell'informativa.

Inoltre, circa il trattamento dei propri dati, dichiara di  
concedere non concedere - l'autorizzazione per finalità statistiche;  
concedere non concedere - l'autorizzazione per finalità commerciali;  
concedere non concedere - l'autorizzazione per finalità promozionali e/o di marketing dirette;  
concedere non concedere - l'autorizzazione per finalità promozionali e/o di marketing di terzi;

(luogo) \_\_\_\_\_, lì (data) \_\_\_\_\_

TIMBRO E FIRMA  
per accettazione

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

**Informativa ed acquisizione di consenso per il trattamento di dati personali ai sensi del D. Lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali.**

**INFORMATIVA**

Ai sensi dell'art. 13, D. Lgs. 30 giugno 2003, n. 196, la Società ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA informa che, per l'instaurazione e per l'esecuzione dei rapporti contrattuali in corso con Voi, è in possesso di dati a Voi relativi qualificati dalla legge come personali o come identificativi.

Tali dati sono oggetto di trattamento per finalità gestionali e legate alle richieste della Pubblica Amministrazione e per ottemperare agli obblighi previsti dalle vigenti norme legislative mediante la consultazione, l'elaborazione, il raffronto, l'interconnessione, la comunicazione, (la diffusione) ed ogni altra opportuna operazione di trattamento. I dati sono trattati su supporto elettronico, magnetico, cartaceo.

Si precisa che il conferimento dei dati è obbligatorio per tutto quanto è inerente agli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli ovvero l'eventuale rifiuto al trattamento potrà determinare l'impossibilità della Società ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA a dar corso ai rapporti contrattuali.

I dati in questione potranno essere portati a conoscenza di persone fisiche o giuridiche quali responsabili della Società ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA ed a persone fisiche individuate dalla stessa quali incaricati a compiere operazioni di trattamento.

Essi potranno inoltre essere comunicati (in Italia e all'estero) a:

- agenti;
- società di assicurazione
- società di recupero del credito e cessionarie ai sensi degli artt.1260-1267 del Codice Civile;
- banche ed istituti di credito;
- professionisti e consulenti;
- società operanti nei settore dei trasporti, spedizioni e comunicazioni

Si informa che, in relazione al trattamento dei dati che La riguardano, la Sua Azienda può esercitare i diritti di cui all'art. 7, D. Lgs. 196/2003.

Titolare del trattamento è: D'ACRI ANTONIO MARCO

Responsabile del trattamento è : LEON FRANCESCA

**ACQUISIZIONE DEL CONSENSO**

L'interessato \_\_\_\_\_ preso atto dell'informativa ricevuta e dell'art. 7 del D.Lgs. 196/03, esprime il proprio consenso al trattamento ed alla comunicazione dei propri dati per le finalità e nei limiti dell'informativa.

Inoltre, circa il trattamento dei propri dati, dichiara di

concedere non concedere - l'autorizzazione per finalità statistiche;

concedere non concedere - l'autorizzazione per finalità commerciali;

concedere non concedere - l'autorizzazione per finalità promozionali e/o di marketing dirette;

concedere non concedere - l'autorizzazione per finalità promozionali e/o di marketing di terzi;

concedere non concedere - l'autorizzazione per finalità di gestione di finanziamenti, con comunicazioni a finanziarie;

(luogo) \_\_\_\_\_, lì (data) \_\_\_\_\_

TIMBRO E FIRMA  
per accettazione



**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

**Informativa per sito web vetrina, in cui non è prevista la creazione e l'utilizzo di banche dati**

**INFORMATIVA****Titolare del trattamento**

A seguito della consultazione di questo sito possono essere trattati dati relativi a persone identificate o identificabili. Il Titolare del trattamento è D'ACRI ANTONIO MARCO con sede in  
PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)

**Luogo di trattamento dei dati**

I trattamenti connessi ai servizi web di questo sito hanno luogo presso e presso i locali del Titolare del trattamento. Essi sono curati solo da personale incaricato al trattamento, oppure da eventuali incaricati per occasionali operazioni di manutenzione. Eccetto questi casi, nessun dato derivante dal servizio web viene comunicato o diffuso.

**Dati di navigazione**

I sistemi informatici e le procedure software preposte al funzionamento di questo sito web acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet.

Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti.

In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.

Questi dati vengono utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso del sito e per controllarne il corretto funzionamento e vengono cancellati immediatamente dopo l'elaborazione. I dati potrebbero essere utilizzati per l'accertamento di responsabilità in caso di ipotetici reati informatici ai danni del sito: fatto salva questa eventualità, i dati sui contatti web persistono per un periodo di tempo limitato (pari a circa \_\_\_\_\_ giorni).

**Dati forniti volontariamente dall'utente**

L'invio facoltativo, esplicito e volontario di posta elettronica agli indirizzi indicati su questo sito comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti nella missiva.

I dati personali forniti dagli utenti che inoltrano richieste di invio di materiale informativo (bollettini, Cd-rom, newsletter, relazioni annuali, risposte a quesiti, atti e provvedimenti, ecc.) sono utilizzati al solo fine di eseguire il servizio o la prestazione richiesta e sono comunicati a terzi nel solo caso in cui ciò sia a tal fine necessario.

### Cookies

Nessun dato personale degli utenti viene in proposito acquisito dal sito. Non viene fatto uso di cookies per la trasmissione di informazioni di carattere personale, né vengono utilizzati c.d. cookies persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti.

L'uso di c.d. cookies di sessione (che non vengono memorizzati in modo persistente sul computer dell'utente e svaniscono con la chiusura del browser) è strettamente limitato alla trasmissione di identificativi di sessione (costituiti da numeri casuali generati dal server) necessari per consentire l'esplorazione sicura ed efficiente del sito.

I c.d. cookies di sessione utilizzati in questo sito evitano il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di dati personali identificativi dell'utente.

### Facoltatività del conferimento dei dati

A parte quanto specificato per i dati di navigazione, l'utente è libero di fornire i dati personali attraverso mail e/o form negli appositi moduli per ottenere informazioni e/o il servizio richiesto. Il loro mancato conferimento può comportare l'impossibilità di ottenere quanto richiesto.

### Modalità del trattamento

I dati personali sono trattati con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti.

Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati. Specificare se la struttura è dotata di dispositivi anti-intrusione e quali.

### Diritti degli interessati

I soggetti cui si riferiscono i dati personali hanno il diritto in qualunque momento di ottenere la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento, oppure la rettificazione (art. 7 del d.lgs. n. 196/2003).

Ai sensi del medesimo articolo si ha il diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento.

Le richieste vanno rivolte al seguente indirizzo e-mail \_\_\_\_\_  
o al numero di telefono \_\_\_\_\_ o fax \_\_\_\_\_

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

**PRIVACY: DIRITTI DELL'INTERESSATO**

Si informa che, in relazione al trattamento dei dati, l'interessato (o gli aventi causa) possono esercitare i diritti di cui all'art. 7, D.Lgs. 196/2003. In particolare, l'interessato può ottenere la conferma dell'esistenza o meno dei propri dati personali e che tali dati siano messi a sua disposizione in forma intelligibile. L'interessato può altresì chiedere di conoscere l'origine dei suoi dati, nonché la logica e le finalità su cui si basa il trattamento; di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché l'aggiornamento, la rettificazione o, se vi è interesse, l'integrazione dei dati; di opporsi, per motivi legittimi, al trattamento.

**Estratto dal DLGS 196/2003****TITOLO II - DIRITTI DELL'INTERESSATO****Art. 7. Diritto di accesso ai dati personali ed altri diritti**

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
  - a) dell'origine dei dati personali;
  - b) delle finalità e modalità del trattamento;
  - c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
  - d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
  - e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
  - a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
  - b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
  - c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
  - a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
  - b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

**Oggetto: Informativa e acquisizioni del consenso per il trattamento dei dati personali ai sensi del D. Lgs. 30.6.2003, n. 196, Codice in materia di protezione dei dati personali.**

Gent. Sig.ra / Egr. Sig.

Il D.Lgs. n. 196/2003 ha la finalità di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato con particolare riferimento alla riservatezza e alla identità personale e al diritto alla protezione dei dati.

Ai sensi dell'art. 13, ed in relazione ai suoi dati personali che si intendono trattare, ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA La informa di quanto segue:

1. La normativa intende per trattamento qualunque operazione o complesso di operazioni, svolte con o senza l'aiuto di strumenti elettronici concernenti le operazioni di cui all'art. 4, comma 1, lett. a);
2. In relazione al rapporto di lavoro con Lei in atto alla data odierna, i dati personali comuni e sensibili raccolti e acquisiti preventivamente e durante il rapporto di lavoro, sono necessari per adempiere alla corretta gestione del rapporto di lavoro sotto tutti i profili: in particolare, per provvedere alla corresponsione delle paghe e ai connessi adempimenti previdenziali, assistenziali - anche integrativi - e fiscali; per assolvere ogni adempimento di legge, di regolamento e di contratto anche aziendale.
3. I dati in questione, per quanto attiene alla fase antecedente alla stipulazione del rapporto, sono stati acquisiti tramite il curriculum ricevuto e il questionario sottoscritto all'atto della assunzione. Nel loro complesso i dati inseriti nella banca dati interna del personale dipendente riguardano:
  - dati anagrafici (nome, cognome, data e luogo di nascita, residenza - via, cap, località, telefono, codice fiscale, stato civile);
  - dati di lavoro (n. di matricola, dati banca d'appoggio);
  - stato di famiglia, posizione militare, studi compiuti, lingue straniere conosciute e livello, esperienze di lavoro precedenti, formazione interna e/o esterna ricevuta.
4. Nel corso del rapporto, a seguito di eventuale segnalazione dell'interessato, e in occasione delle operazioni di trattamento dei dati personali, la Società titolare può venire a conoscenza di dati definiti dalla legge (art. 4, comma 1, lett. d) come sensibili, in quanto idonei a rivelare:
  - adesione a sindacato (es. assunzione cariche sindacali ed esercizio relativi diritti, versamento contributi sindacali);
  - lo stato di salute (es. certificati relativi ad assenze per malattia, maternità, infortunio, inidoneità a determinate prestazioni, avviamenti obbligatori, inabilità fisiche, nucleo familiare);
  - adesione a partiti politici (es. godimento permessi, aspettative, esercizio diritti per adempimento mandato);
  - convinzioni religiose;
  - obiezione di coscienza;
  - origine razziale ed etnica.

Tali dati - i quali potranno in taluni casi essere trattati per conto di Istituti previdenziali e assistenziali - saranno comunque trattati con il consenso degli interessati, nel rispetto del codice e nell'osservanza delle autorizzazioni del Garante al trattamento dei dati sensibili nei rapporti di lavoro.

5. I dati in questione potranno essere portati a conoscenza di persone fisiche o persone giuridiche, in qualità di responsabili designati dalla Società titolare e di persone fisiche in qualità di incaricati a compiere operazioni di trattamento. In particolare potranno essere comunicati:
  - alle pubbliche Amministrazioni per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge e dai regolamenti;
  - a Banche per accreditare le retribuzioni ed espletare altre operazioni di credito richieste dai dipendenti;

- a Società / Studio di consulenza del lavoro per l'adempimento degli obblighi contabili, retributivi, previdenziali, assistenziali e fiscali del personale dipendente;
  - a Compagnie e Broker Assicurativi per la gestione delle polizze;
  - a Istituti di credito e finanziarie per cessioni di stipendio, prestiti;
  - a Organizzazioni sindacali per l'esercizio dei diritti richiesti dagli interessati;
  - a Società collegate, organi collegiali e amministratori, delle medesime Società;
  - a Società terze per (certificazioni qualità, corsi di formazione);
  - a Società terze per espletamento degli obblighi inerenti contratti di appalto e fornitura;
  - a Società di trasporto, di noleggio auto;
  - all'estero in ambito CEE e Extra CEE, ad enti ed istituzioni per le finalità istituzionali del nostro Ente;
  - a Società terze per l'ottemperanza degli obblighi in materia di prevenzione, sicurezza e igiene del lavoro e per le finalità di security.
6. Tutti i dati personali, (identificativi, sensibili e giudiziari ove esistenti) in oggetto saranno trattati secondo le modalità e nel rispetto delle disposizioni di cui all'art. 11 D. Lgs. citato, con strumenti idonei a garantirne la sicurezza e la riservatezza. In particolare le operazioni saranno effettuate:
- su supporto cartaceo e/o su supporto informatico;
  - da soggetti autorizzati all'assolvimento di tali compiti opportunamente istruiti e resi edotti dei vincoli imposti dal Codice in materia di protezione dei dati personali;
  - in modo da impedire o ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
7. Si precisa che tanto il conferimento dei dati personali in oggetto, quanto il consenso a trattare i dati conferiti possono, a seconda dei casi, avere natura obbligatoria o facoltativa. Che il non conferimento totale o parziale dei dati, così come il mancato consenso, totale o parziale, al trattamento dei dati renderanno impossibile alla Società la effettuazione dei trattamenti corrispondenti e di quelli connessi.
8. Si rende noto che:
- titolare del trattamento dei dati personali (ex art. 4, comma 1, lett. F) è D'ACRI ANTONIO MARCO;
  - responsabile del trattamento è LEON FRANCESCA,
  - attraverso l'art. 7 del D. Lgs. n. 196/2003 si riconoscono il diritto di accesso ai dati personali ed altri diritti dell'interessato.

La preghiamo di restituirci con tempestività, firmata da Lei (e dai Suoi familiari e affini maggiorenni a carico, o comunque componenti del Suo nucleo familiare), la presente come attestazione di ricevuta dell'informativa e come espressione del consenso al trattamento e alla comunicazione di tutti i dati personali per le finalità e nei limiti indicati nella informativa ricevuta. Precisiamo che i familiari e affini interessati sono quelli che risultano a suo carico, per i quali Ella fruisce di detrazioni fiscali e/o assegni familiari, e/o altri trattamenti economici o normativi.

Distinti saluti.

(luogo) \_\_\_\_\_, lì (data) \_\_\_\_\_

Il Titolare del trattamento  
D'ACRI ANTONIO MARCO

FIRMA DELL'INTERESSATO  
per accettazione

**CLAUSOLA DI CONSENSO**

Preso atto dell'informativa di cui sopra e dell' art. 7 del D.Lgs. 196/03 i sottoscritti, familiari dell'interessato, di seguito identificati esprimono il consenso al trattamento dei dati personali comuni e sensibili che li riguardano e alla comunicazione dei medesimi dati.

Cognome e Nome \_\_\_\_\_ Firma \_\_\_\_\_  
 Cognome e Nome \_\_\_\_\_ Firma \_\_\_\_\_  
 Cognome e Nome \_\_\_\_\_ Firma \_\_\_\_\_  
 Cognome e Nome \_\_\_\_\_ Firma \_\_\_\_\_  
 Cognome e Nome \_\_\_\_\_ Firma \_\_\_\_\_  
 Cognome e Nome \_\_\_\_\_ Firma \_\_\_\_\_

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

**Oggetto: Informativa e acquisizioni del consenso per il trattamento dei dati personali ai sensi del D. Lgs. 30.6.2003, n. 196, Codice in materia di protezione dei dati personali.**

Gent. Sig.ra / Egr. Sig.

Il D. Lgs. 30.6.2003, n. 196, ha la finalità di garantire il trattamento dei dati personali identificativi e sensibili, con particolare riferimento alla riservatezza e alla identità dei soggetti interessati. Ai sensi dell'art. 13, ed in relazione ai suoi dati personali che si intendono trattare, la Società ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA La informa di quanto segue:

1. La normativa intende per trattamento qualunque operazione o complesso di operazioni, svolti con o senza l'aiuto di mezzi elettronici o comunque automatizzati concernenti le operazioni di cui all'art. 4, comma 1, lett. a), D. Lgs. 196/2003.
2. Il trattamento dei dati personali che La riguardano di cui la Società è in possesso e che Le saranno richiesti o che ci verranno da Lei comunicati è/sarà necessario per la corretta gestione del rapporto di collaborazione in qualità di agente sotto tutti i profili: in particolare, per provvedere alle scritture e registrazioni contabili obbligatorie, agli adempimenti fiscali e previdenziali, all'espletamento degli adempimenti di legge, di regolamento e di contratto relativi al mandato professionale, nonché alle relative modifiche e integrazioni.  
I dati in questione potranno essere comunicati:
  - alla/e Società \_\_\_\_\_
  - a Istituti bancari,
  - all'ENASARCO,
  - a \_\_\_\_\_
3. Nel corso del rapporto, a seguito di eventuale segnalazione dell'interessato, e in occasione delle operazioni di trattamento dei dati personali, la Società titolare può venire a conoscenza di dati definiti dalla legge come sensibili, in quanto idonei a rivelare lo stato di salute. Tali dati saranno comunque trattati con il consenso dell'interessato nel rispetto delle leggi vigenti e nell'osservanza delle autorizzazioni del Garante al trattamento dei dati sensibili.
4. I dati in questione potranno essere portati a conoscenza di persone fisiche o giuridiche in qualità di responsabili designati dalla Società titolare e di persone fisiche incaricate a compiere operazioni di trattamento.
5. I dati personali identificativi e sensibili in oggetto saranno trattati nel rispetto delle disposizioni di cui all'art. 11 D. Lgs. 196 del 2003, con strumenti idonei a garantirne la sicurezza e la riservatezza. In particolare le operazioni saranno effettuate:
  - su supporto cartaceo e/o su supporto magnetico;
  - da soggetti autorizzati all'assolvimento di tali compiti opportunamente istruiti e resi edotti dei vincoli imposti dal citato D. Lgs. 196/2003;
  - in modo da impedire l'indebito accesso a soggetti terzi e a personale non autorizzato; la distribuzione o la perdita, anche accidentale, dei dati stessi.
6. Si precisa che tanto il conferimento dei dati personali in oggetto, quanto il consenso a trattare i dati conferiti possono, a seconda dei casi, avere natura o obbligatoria o facoltativa. Che il non conferimento, totale o parziale, dei dati, così come il mancato consenso, totale o parziale, al trattamento degli stessi renderanno impossibile alla Società l'effettuazione dei trattamenti corrispondenti e di quelli connessi.
7. Si rende noto che:
  - Titolare del trattamento dei dati personali (ex art. 28 D. Lgs. 196/2003) è D'ACRI ANTONIO MARCO
  - Responsabile del trattamento (ex art. 29 D. Lgs. 196/2003) è LEON FRANCESCA
8. Si rende noto che l'art. 7, D. Lgs. 196/2003 riconosce i diritti dell'interessato nel trattamento dei dati.

Distinti saluti.

(luogo) \_\_\_\_\_, lì (data) \_\_\_\_\_

Il Titolare del trattamento  
D'ACRI ANTONIO MARCO

FIRMA DELL'INTERESSATO  
per accettazione

## ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

**Oggetto: Lettera di incarico per nuove assunzioni o collaborazioni e per trattamenti temporanei dei dati.**

Si dichiara che dalla data in calce, in seguito all'avvio del rapporto lavorativo / progetto, sono assegnati a

Cognome e Nome \_\_\_\_\_  
residente in (Luogo) \_\_\_\_\_  
provincia di \_\_\_\_\_  
presso (Indirizzo) \_\_\_\_\_  
Codice Fiscale \_\_\_\_\_

i permessi di accesso ai dati in formato cartaceo ed eventualmente elettronico per le seguenti banche dati:

|                  |                              |
|------------------|------------------------------|
| Banca Dati _____ | Permessi (I/C/M/A/T/D) _____ |
| Banca Dati _____ | Permessi (I/C/M/A/T/D) _____ |
| Banca Dati _____ | Permessi (I/C/M/A/T/D) _____ |
| Banca Dati _____ | Permessi (I/C/M/A/T/D) _____ |
| Banca Dati _____ | Permessi (I/C/M/A/T/D) _____ |
| Banca Dati _____ | Permessi (I/C/M/A/T/D) _____ |
| Banca Dati _____ | Permessi (I/C/M/A/T/D) _____ |
| Banca Dati _____ | Permessi (I/C/M/A/T/D) _____ |

Tali permessi ed eventuali responsabilità sui luoghi e sulla strumentazione elettronica saranno presentati nel Documento Programmatico sulla Sicurezza alla scadenza prevista dalla vigente normativa.  
(luogo) \_\_\_\_\_, lì (data) \_\_\_\_\_

Il Responsabile del trattamento  
LEON FRANCESCA

L'Incaricato al trattamento  
temporaneo per accettazione



**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

**Oggetto: Lettera di cessazione dell'incarico per incaricati e responsabili del trattamento dei dati.**

Si dichiara che dalla data in calce decadono le responsabilità inerenti ai permessi di accesso ai dati, ai luoghi e all'utilizzo degli elaboratori per

Cognome e Nome \_\_\_\_\_  
residente in (Luogo) \_\_\_\_\_  
provincia di \_\_\_\_\_  
presso (Indirizzo) \_\_\_\_\_  
Codice Fiscale \_\_\_\_\_

in seguito alla cessazione del rapporto di lavoro tra le parti, come da documentazione allegata.  
(luogo) \_\_\_\_\_, lì (data) \_\_\_\_\_

Il Responsabile del trattamento  
LEON FRANCESCA

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

**Oggetto: Lettera per cambio di sede.**

Si dichiara che dalla data in calce le attività di ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA sono trasferite dagli attuali locali ai locali di \_\_\_\_\_

I permessi di accesso ai dati, di utilizzo degli elaboratori e le responsabilità sui luoghi sono stati aggiornati e saranno presentati con il Documento Programmatico per la Sicurezza aggiornato secondo normativa vigente.

(luogo) \_\_\_\_\_, lì (data) \_\_\_\_\_

Il Responsabile del trattamento  
LEON FRANCESCA

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

---

Attraverso questa dicitura ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA autorizza al trattamento dei propri dati il cliente/fornitore che ha ricevuto la fattura/preventivo/ordine

**DA INSERIRE SULLE FATTURE, SUI PREVENTIVI O SUGLI ORDINI:**

Autorizzazione al trattamento dei dati personali e sensibili

Ai sensi del D. Lgs. 196/03 in materia di trattamento di dati personali e misure minime di sicurezza ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA con sede legale in PIAZZA PALAZZO DI CITTA' 1 10122 - TORINO (TO) - PIVA 08545970017 autorizza l'azienda sopra citata al trattamento mediante strumenti elettronici e non dei propri dati personali e sensibili secondo normativa vigente

(luogo) \_\_\_\_\_, lì (data) \_\_\_\_\_  
(timbro e firma) \_\_\_\_\_

---

Attraverso queste due diciture, ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA richiede il consenso al cliente/fornitore per trattarne i dati

**DA INSERIRE SU ORDINI A FORNITORI CHE DEVONO ESSERE RESTITUITI FIRMATI PER ACCETTAZIONE**

Autorizzazione al trattamento dei dati personali e sensibili

Ai sensi e nel rispetto del D. Lgs. 196/03 in materia di trattamento di dati personali e misure minime di sicurezza l'azienda (bisogna inserire il nome dell'azienda a cui si è fatto l'ordine o il preventivo) con sede legale (indicare la sede) e partita IVA (indicare la partita IVA) autorizza ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA al trattamento mediante strumenti elettronici e non dei propri dati personali e sensibili secondo normativa vigente

(luogo) \_\_\_\_\_, lì (data) \_\_\_\_\_  
(timbro e firma) \_\_\_\_\_

**DA INSERIRE SULLE FATTURE E/O DOCUMENTI DI TRASPORTO CHE DEVONO ESSERE RESTITUITI FIRMATI PER ACCETTAZIONE DAL CLIENTE**

Autorizzazione al trattamento dei dati personali e sensibili

Ai sensi e nel rispetto del D. Lgs. 196/03 in materia di trattamento di dati personali e misure minime di sicurezza si autorizza ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA al trattamento mediante strumenti elettronici e non dei nostri dati personali e sensibili secondo normativa vigente

(luogo) \_\_\_\_\_, lì (data) \_\_\_\_\_  
(timbro e firma) \_\_\_\_\_

**DA INSERIRE SULLE FATTURE PER LE QUALI IL CLIENTE NON APPONE LA PROPRIA FIRMA PER RICEVUTA**

Autorizzazione al trattamento dei dati personali e sensibili

Ai sensi del D.Lgs 196/03 in materia di trattamento di dati personali, la scrivente, titolare del trattamento, informa il cliente che i dati che lo riguardano sono trattati mediante strumenti elettronici e non, secondo normativa vigente e applicando le misure minime di sicurezza previste. Si precisa che il conferimento e il trattamento dei dati sono obbligatori per tutto quanto è inerente agli obblighi legali, contabili e contrattuali. Il cliente può esercitare i diritti di cui all'art.7 del predetto decreto.

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

---

**DICITURA DA INSERIRE SU COPERTINA FAX**

Spett.le \_\_\_\_\_

All'attenzione di \_\_\_\_\_

Il fax è rivolto all'interessato/i riportato/i nella dicitura sovrastante.

Si ricorda che per ottemperare a quanto previsto dal Decreto Legislativo n.196 del 30 giugno 2003 in materia di privacy, qualora persone diverse dall'interessato/i ricevessero il seguente fax, costoro sono pregate di non procedere alla lettura del contenuto.

Il fax dovrà essere consegnato all'interessato/i; qualora causa nostro errore o per diversi motivi non fosse possibile siete pregati di informarci tempestivamente.

Nostri riferimenti \_\_\_\_\_

---

**AVVERTENZA DA INSERIRE IN CALCE AL FAX**

Il contenuto del presente fax ed i suoi allegati sono diretti esclusivamente al destinatario e devono ritenersi riservati con divieto di diffusione e di uso nei giudizi salva espressa autorizzazione; nel caso di utilizzo senza espressa autorizzazione, verrà effettuata denuncia al competente organo giudiziario. La diffusione e la comunicazione da parte di soggetto diverso dal destinatario è vietata dall'art. 616 e ss. c.p. e dal d. l.vo n. 196/03. Se il fax e i suoi allegati sono stati ricevuti per errore da persona diversa dal destinatario siete pregati di distruggere tutto quanto ricevuto e di informare il mittente ai numeri telefonici in epigrafe.

**AVVERTENZA DA INSERIRE IN CALCE ALLE E-MAIL**

Le informazioni trasmesse attraverso la presente e-mail ed i suoi allegati sono diretti esclusivamente al destinatario e devono ritenersi riservati con divieto di diffusione e di uso salva espressa autorizzazione; nel caso di utilizzo senza espressa autorizzazione, verrà effettuata denuncia al competente organo giudiziario. La diffusione e la comunicazione da parte di soggetto diverso dal destinatario è vietata dall'art. 616 e ss. c.p. e dal d. l.vo n. 196/03. Se la presente e-mail ed i suoi allegati fossero stati ricevuti per errore da persona diversa dal destinatario siete pregati di distruggere tutto quanto ricevuto e di informare il mittente con lo stesso mezzo.

**AVVERTENZA DA INSERIRE IN CALCE ALLE LETTERE**

Il contenuto della presente ed i suoi allegati sono diretti esclusivamente al destinatario e devono ritenersi riservati con divieto di diffusione e di uso nei giudizi, salva espressa autorizzazione e, nel caso di utilizzo senza espressa autorizzazione, verrà effettuata denuncia al competente organo giudiziario. La diffusione e la comunicazione da parte di soggetto diverso dal destinatario è vietata dall'art. 616 e ss. c.p. e dal d. l.vo n. 196/03.

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

**Oggetto: Informazioni di condotta rispetto alla normativa sulla Privacy.**

Spettabile azienda,

Con l'entrata in vigore il D. Lgs. 30.6.2003, n. 196 sulla protezione dei dati personali, tra i nuovi obblighi previsti nel decreto (in particolare nel punto 29 del Disciplinare tecnico, allegato B) vi è anche quello - in determinate circostanze - dell'identificazione e registrazione dei soggetti ammessi nei locali contenenti archivi dopo l'orario di chiusura. Infatti, la protezione degli archivi contenenti dati personali è estesa alla custodia e conservazione di ogni atto e documento cartaceo contenente dati personali particolari, riferiti sia a persone fisiche che giuridiche.

Allo scopo di ottemperare alle suddette necessità, vogliate cortesemente fornirci i nominativi delle persone che la Vostra Ditta ha assegnato alle pulizie dei nostri locali al fine di poter considerare tali persone autorizzate all'accesso nella nostra struttura. In caso di assenza o impedimento delle persone che ci indicherete, sarà Vostra cortesia ed obbligo, comunicarci preventivamente i nominativi dei loro sostituti.

Ai fini dei necessari controlli e delle responsabilità civili e penali connessi alla violazione delle norme contenute nel D.Lgs. n. 196/2003 sarà opportuno che la Vostra Ditta organizzi un registro delle persone autorizzate ad accedere nei nostri locali.

Le persone autorizzate dovranno limitarsi alle sole attività di pulizia:

- non dovrà essere consultato nessun documento, né archivio;
- l'uso delle apparecchiature informatiche è vietato;
- il materiale cartaceo asportato, destinato allo smaltimento dei rifiuti, dovrà essere riposto con cura negli appositi sacchi di plastica e tali sacchi dovranno essere chiusi in maniera che gli atti e i documenti in essi contenuti non possano, nemmeno accidentalmente, fuoriuscire.

Tale condotta dovrà essere rispettata dal Vostro personale che, allo scopo, sarà da Voi informato.

Distinti saluti.

Il Responsabile della sicurezza del trattamento  
LEON FRANCESCA

TIMBRO E FIRMA  
per accettazione

**ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA**

PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
PIVA 08545970017

**Oggetto: Informazioni di condotta rispetto alla normativa sulla Privacy.**

Il sottoscritto \_\_\_\_\_  
legale rappresentante di ASSOCIAZIONE TORINO CITTÀ CAPITALE EUROPEA con sede in  
PIAZZA PALAZZO DI CITTA' 1  
10122 - TORINO (TO)  
nato a \_\_\_\_\_ il \_\_\_\_\_  
residente in \_\_\_\_\_  
codice fiscale \_\_\_\_\_

dichiara che:

- L'elaboratore identificato dal numero di serie \_\_\_\_\_ sottratto dai locali di \_\_\_\_\_  
in data \_\_\_\_\_, al momento del furto era dotato delle misure minime  
di sicurezza previste dall'Allegato B del D.Lgs. 196 del 30 giugno 2003, in particolare l'accesso per ogni  
utente è protetto mediante autenticazione con password di almeno 8 caratteri alfanumerici.
- All'interno del suddetto elaboratore sono presenti dati del seguente tipo:
  - Pertanto si dissocia da qualsiasi uso illecito che possa essere fatto in maniera fraudolenta, dagli autori  
del furto o da terzi, di tali dati.

(luogo) \_\_\_\_\_, lì (data) \_\_\_\_\_

LEON FRANCESCA

In fede

# Appendice G

## Elenco misure adottate

Segue l'elenco delle misure adottate al 19/05/2014 per ottemperare alla normativa in materia di privacy e trattamento di dati personali Decreto Legislativo n. 196 del 30 giugno 2003.

### G.1 Misure interne

- Realizzazione del Regolamento per la protezione dei dati personali, economici, sensibili e giuridici
- Lettera di incarico speciale con indicazione del titolare del trattamento
- Lettera di incarico speciale con indicazione del responsabile del trattamento
- Elenco di sedi e locali atti alla trattamento di dati personali, sensibili e giudiziari
- Lettere di incarico per gli addetti al controllo dei locali
- Elenco e descrizione dei trattamenti e delle banche dati con relativo registro con i permessi di accesso ai dati
- Lettere di incarico per gli incaricati interni del trattamento con relativi permessi di accesso ai dati
- Lettere di incarico per responsabili esterni del trattamento con relativi permessi di accesso ai dati e diritto di delega

### G.2 Misure atte al trattamento elettronico dell'informazione

- Elenco degli elaboratori
- Gestione e custodia delle credenziali di autenticazione come previsto da normativa vigente
- Sistema di salvataggio (back-up) dei dati come riportato nel documento programmatico sulla sicurezza previsto dalla normativa vigente
- Sistema firewall di protezione da intrusioni esterne e intercettazione delle informazioni presenti in rete (come da documentazione allegata)
- Sistema antivirus di protezione da attacchi e dal degrado dei dati contenuti sugli elaboratori
- Filtri e politiche antispam per il servizio di posta elettronica
- Metodologia per le segnalazioni dei rischi hardware e software, per la reportistica dei virus e degli attacchi informatici rilevati

### **G.3 Regolamenti e formazione**

- Formazione ed informazione dei Responsabili
- Formazione ed informazione degli incaricati
- Istituzione di regolamento interno sulla gestione e sul trattamento delle banche dati in formato elettronico e cartaceo
- Istituzione di regolamento interno sulla gestione e sulle modalità del recupero del credito
- Adozione delle misure previste dal Provvedimento del Garante del 27-11-2008 sulle funzioni degli amministratori di sistema

### **G.4 Ulteriori Misure**

- Predisposizione di informative per l'acquisizione al consenso del trattamento per dipendenti, collaboratori, clienti, fornitori, agenti e rappresentanti
- Lettere di responsabilizzazione per imprese di pulizia nell'accedere ai locali atti al trattamento
- Lettere di autorizzazione alle operazioni di manutenzione/riparazione di un elaboratore elettronico da parte di ditte specializzate

### **G.5 Analisi dei rischi**

Realizzazione del documento analisi rischi per i dati conservati all'interno della struttura riportante:

- Rischi dovuti agli operatori
- Misure adottate contro i rischi dovuti agli operatori
- Rischi dovuti al contesto
- Misure adottate contro i rischi dovuti al contesto
- Rischi dovuti agli strumenti
- Misure adottate contro i rischi dovuti agli strumenti

---

Il Titolare del trattamento  
D'ACRI ANTONIO MARCO



# Documento Confidenziale

Quanto segue è un documento confidenziale circa eventuali problematiche emerse dall'analisi condotta in merito all'applicazione degli obblighi e misure di sicurezza previste dalla normativa in materia di privacy e trattamento di dati personali Decreto Legislativo n. 196 del 30 giugno 2003.

Dall'analisi del questionario e dai dati raccolti risultano le seguenti evidenze:

- Occorre allegare la fattura di acquisto o il documento comprovante l'utilizzo di un firewall, eventualmente accompagnato da una relazione delle caratteristiche tecniche e delle configurazioni da esso adottate
- Occorre pianificare controlli periodici alla protezione offerta dai collegamenti telematici in uso
- Occorre adottare strumenti di protezione per i collegamenti telematico in uso
- Ricordarsi di allegare o aggiornare l'elenco delle apparecchiature elettroniche in vostro possesso con la descrizione delle caratteristiche hardware, delle configurazioni e delle persone che le utilizzano; potete utilizzare il modello MOD\_ELAB per predisporre la lista
- Occorre compilare e far firmare il modello MOD\_MTZ\_HWSW al responsabile dell'azienda informatica che fornisce assistenza hardware sugli elaboratori o conservare le schede degli interventi tecnici
- Occorre che alla scadenza stabilita, ogni utente provveda a modificare la propria password, registrandola sul modello MOD\_PWD, mettendola in una busta, sigillandola e consegnandola all'Incaricato della custodia delle password (ICCC), che dovrà provvedere alla raccolta e conservazione in luogo sicuro di tutte le buste
- Avendo disposto incarichi di trattamento dei dati con diversi privilegi di accesso ai dati e su differenti archivi, è necessario adottare un sistema che permetta di implementare tali politiche anche a livello informatico. In pratica occorre un server configurato opportunamente.
- Occorre adottare un adeguato sistema di logging che copra un periodo temporale di almeno 6 mesi per monitorare l'accesso degli amministratori di sistema alle banche dati
- Occorre registrare la verifica formale dell'attività degli amministratori di sistema, come stabilito dal provvedimento del Garante
- Occorre compilare l'elenco di tali dispositivi mobili all'interno del modello MOD\_ELAB dell'appendice A
- È necessario predisporre la documentazione relativa al sistema di videosorveglianza per evitare di incorrere in contestazioni per trattamento illecito di dati
- Occorre predisporre e affiggere gli appositi cartelli segnaletici contenenti l'informativa circa la presenza del sistema di videosorveglianza
- Occorre verificare periodicamente il comportamento degli addetti alle pulizie, ribadendo l'assoluto divieto di accedere ai dati presenti nei locali atti al trattamento; tutti i dati sensibili e/o giudiziari devono essere custoditi sotto chiave, a cura degli incaricati o dal responsabile.

- Occorre predisporre adeguati interventi formativi per gli incaricati al trattamento e per i responsabili

19/05/2014