

ACCORDO PER IL TRATTAMENTO E NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI (ai sensi e per gli effetti del GDPR U.E. n. 679/2016 e D.Lgs 196/2003 e ss. mod e int.)

* * *

1. Premesse

1.1 Il presente *Accordo per il Trattamento dei dati personali* (di seguito anche “*Accordo*”/“*Documento*”) costituisce allegato e parte integrante del Contratto per l’affidamento dell’appalto per il SERVIZIO DI PRONTO INTERVENTO SOCIALE PRIS METROPOLITANO DI BOLOGNA, (di seguito anche “*Contratto*”) sottoscritto tra:

- **ASP CITTÀ DI BOLOGNA**, con sede legale a Bologna - 40126, via Marsala, n. 7 e sede amministrativa in Bologna - 40139, via Roma, n. 21, P. IVA e C.F.: 03337111201, e-mail di contatto: asp@pec.aspbologna.it (di seguito denominato anche “*ASP*”/l’Azienda/“il Titolare del Trattamento”/“il Titolare”)

e

- il Fornitore designato quale *Responsabile del trattamento di dati personali* (di seguito anche “il Fornitore”/“il Responsabile”), che con la sottoscrizione del presente Documento accetta predetta nomina, ai sensi e per gli effetti dell’art. 28 del Regolamento Generale Europeo per la protezione dei dati 679/2016 e ss.mm.ii. (di seguito “*GDPR*”/“*Regolamento*”)

(entrambi di seguito denominati anche “*le Parti*”).

1.2 Il presente *Accordo* si compone delle clausole di seguito rappresentate e dai seguenti Allegati (tutti altresì parti integranti del *Contratto*) che ne formano parte costitutiva e sostanziale:

- APPENDICE 1: Glossario
- APPENDICE 2: Appendice “*Security*”

ed espressamente revoca e sostituisce ogni altro eventualmente intercorso tra le *Parti* inerente al *Trattamento dei Dati*.

1.3 Il presente *Accordo* decorre dalla data di sottoscrizione e resta in vigore per l’intera vigenza del *Contratto* e in ogni caso per tutto il periodo di *trattamento dei dati* da parte del *Responsabile del Trattamento*.

1.4 Il *Titolare dei trattamenti*, ai sensi e per gli effetti del *GDPR*, può individuare, proporre e nominare *Responsabile del trattamento dei dati personali* (di seguito anche “*Dati*”) una persona fisica, una persona giuridica, una Pubblica Amministrazione/o qualsiasi altri ente/associazione/organismo che per esperienza, capacità e affidabilità fornisca idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di *trattamento dei dati*, ivi compreso il profilo relativo alla sicurezza.

1.5 La natura del *Trattamento* è insita nello svolgimento da parte del *Fornitore* dei particolari obblighi e oneri di cui al *Contratto* e come nello stesso già dettagliati e la sua durata coincide con quella del predetto *Contratto*, come da precedente *sub* 1.3. e salvo quanto previsto nella successiva clausola **10.** del presente *Documento*.

1.6 *ASP* individua, designa e istruisce, anche per tramite di proprio *Sub-Delegato al Trattamento*, il *Fornitore* quale *Responsabile del Trattamento* in relazione ai *dati personali* trattati in relazione agli oneri e obblighi relativi e discendenti dal *Contratto* sottoscritto dalla *Parti* e sotteso alla presente *Nomina*.¹

¹ Come da Organigramma aziendale *privacy* consultabile presso il sito aziendale nella sezione dedicata (<https://www.aspbologna.it>)

1.7 Ai fini dell’espletamento degli obblighi in capo al *Responsabile*, il *Titolare* consente al predetto e altresì ai soggetti dallo stesso *Incaricati/Autorizzati* al *trattamento* l’accesso ai soli *dati personali* a

ciò necessari.

- 1.8 Il *Responsabile del trattamento* deve presentare garanzie sufficienti per metter in atto misure tecniche e organizzative adeguate a che il trattamento soddisfi i requisiti della normativa come vigente in materia complessivamente applicabile e garantisca i diritti dell'*Interessato*.
- 1.9 Il *Responsabile* deve procedere al *trattamento* secondo le istruzioni impartite dal *Titolare* per iscritto con il presente *Documento* e/o tramite accordi già intercorsi in sede di *Contratto* e altresì eventuali successivi.

Tutto quanto premesso, le *Parti* convengono quanto segue:

- 1.10 Le suestese **Premesse** costituiscono parte integrante del presente *Accordo*: le *Parti* confermano la veridicità e l'essenzialità di quanto nelle stesse dichiarato, anche ai fini dell'interpretazione del presente *Documento* nonché del *Contratto*.

2. Diritti e obblighi del Titolare del Trattamento

- 2.1. Il *Titolare del trattamento* ha la facoltà di apportare al presente *Accordo*, in qualunque momento ed *ex lege*, modifiche e integrazioni come necessarie e/o opportune ai fini dell'aggiornamento normativo, rispetto quindi a nuove prescrizioni che dovessero intervenire in materia in corso di validità dello stesso, con conseguente adeguamento, nel caso, altresì delle procedure aziendali e correlati adempimenti (es: aggiornamento del *Registro dei trattamenti*).
- 2.2. Le eventuali modifiche di cui alla precedente clausola 2.1. saranno debitamente comunicate dall'*Azienda* al *Responsabile* a mezzo P.E.C.
- 2.3. Il *Titolare* garantisce che i *Dati* da lui trasmessi al *Responsabile*:
- a) sono pertinenti e non eccedenti rispetto alle finalità per le quali sono state raccolte e successivamente trattati;
 - b) in ogni caso, i *dati personali* e/o le categorie particolari di *dati personali*, oggetto delle operazioni di *Trattamento* affidate al *Responsabile*, sono raccolti e trasmessi rispettando ogni prescrizione della normativa applicabile.
- 2.4. Il *Titolare* svolge attività di vigilanza e verifica nei confronti del *Fornitore* in relazione a:
- a) il rispetto delle istruzioni allo stesso impartite e degli obblighi tutti di cui al presente *Documento* e quindi assunti dal *Fornitore* con l'accettazione della correlata nomina a *Responsabile del trattamento*;
 - b) il permanere dei requisiti di esperienza, capacità e affidabilità di cui in *Premesse sub 1.4*.
- 2.5. *ASP* si riserva altresì il diritto di svolgere attività di *audit* come da successiva clausola **11.** del presente *Accordo*, cui si rinvia.

3. Obblighi del Responsabile: Trattamento dei dati nel rispetto delle istruzioni del Titolare

- 3.1. Il *Fornitore* nel dare corso all'esecuzione del *Contratto*, in qualità di *Responsabile*, si obbliga (per sé e per le persone autorizzate al *Trattamento* che collaborano con la sua organizzazione) al rispetto delle prescrizioni di cui:
- a) al *GDPR*;
 - b) all'interezza della normativa applicabile in materia;

- c) alle indicazioni del *Garante della Privacy*, adottando idonee misure preventive atte a salvaguardare la sicurezza dei *dati* trattati;

dando quindi attuazione alle misure di sicurezza previste dalla normativa *pro tempore* vigente in materia di *Trattamento di dati personali* e di cui anche alla clausola **4.** del presente *Atto* e fornendo assistenza al *Titolare* nel garantire il rispetto della medesima.

3.2. Il *Fornitore*, in conformità all'incarico assunto quale *Responsabile* e relativamente a tutti i *Dati personali* che tratta per conto di ASP si obbliga ad agire secondo modalità e ai fini atti a garantire che:

- a) tratta tali *Dati personali* solo ai fini dell'esecuzione dell'oggetto del *Contratto* e, successivamente, solo nel rispetto di quanto eventualmente concordato dalle *Parti* per iscritto, agendo pertanto, esclusivamente sulla base delle istruzioni documentate e fornite dall'*Azienda* come anche da successiva clausola **4.** del presente *Documento*;
- b) non trasferisce i *Dati personali* a soggetti terzi, se non nel rispetto delle condizioni di liceità assolute dal *Titolare* a fronte di quanto disciplinato nel presente *Accordo*;
- c) non tratta e/o utilizza i *Dati personali* per finalità diverse da quelle per cui è conferito l'incarico da ASP, financo per *trattamenti* aventi finalità compatibili con quelle originarie;
- d) prima di iniziare ogni *trattamento* e, ove occorra, in qualsiasi altro momento, informerà il *Titolare* se, a suo parere, una qualsiasi istruzione dal medesimo fornita si ponga in violazione di una o più prescrizioni di cui alla normativa applicabile in materia.

3.3. Il *Responsabile del trattamento* deve garantire e fornire all'*Azienda* cooperazione, assistenza e le informazioni che potrebbero essere ragionevolmente richieste dalla stessa, per consentirle di adempiere ai propri obblighi ai sensi della normativa applicabile, ivi compresi i provvedimenti e le specifiche decisioni del *Garante per la protezione dei dati personali* (di seguito anche "*Garante*" / "*GdP*").

3.4. Il *Responsabile del trattamento*, anche nel rispetto di quanto previsto all'art. 30 del *Regolamento*, deve mantenere, compilare e rendere disponibile a richiesta della stessa, un *Registro dei trattamenti dati personali* che riporti tutte le informazioni richieste dalla norma.

3.5. Il *Responsabile del trattamento* assicura la massima collaborazione al fine:

- a) dell'esperimento delle valutazioni d'impatto ex art. 35 del *GDPR* che ASP intenderà esperire sui *trattamenti* che rivelano, a Suo insindacabile giudizio, un rischio elevato per i diritti e le libertà delle persone fisiche;
- b) di garantire da parte del *Titolare* il rispetto degli obblighi relativi all'eventuale consultazione preventiva all'Autorità di Controllo.

3.6. Al fine di dare seguito alle eventuali richieste da parte degli *Interessati*, il *Fornitore* si obbliga:

- a) ad avvisare tempestivamente il *Titolare* di ogni istanza ricevuta da uno o più *Interessati* avente a oggetto l'esercizio dei diritti agli stessi riconosciuti dal *GDPR* (artt. 15-21) contestualmente assistendo ASP attraverso il reperimento e la resa di tutte le informazioni necessarie e opportune a sua disposizione;
- b) - in conformità al precedente punto *sub* 3.6.a) - a garantire la gestione delle richieste del *Titolare* e/o delle istanze degli *Interessati* entro il termine massimo di 30 (trenta) giorni dalla loro ricezione così da consentire l'esercizio diritti loro afferenti;
- c) - ove applicabile e in considerazione delle attività di *trattamento* affidategli - a fornire agli *Interessati* i propri *Dati* in un formato strutturato, di uso comune e leggibile da un dispositivo automatico, nonché a trasmettere i *dati* ad altro *Titolare*;
- d) a consentire al *Titolare* di garantire in tutto e/o in parte i diritti di opposizione e limitazione del *Trattamento*.

- 3.7. Il *Responsabile del trattamento* verifica, con cadenza almeno annuale, la permanenza dei requisiti di autorizzazione dei soggetti di cui al proprio organigramma aziendale in materia di *privacy* (quali a esempio *Incaricati, Amministratori di Sistema, Responsabili*, di cui anche alle successive clausole del presente *Accordo*).
- 3.8. Il *Responsabile del trattamento*, nei casi previsti *ex lege* e *Regolamento*, si obbliga a:
- a) rendere l'*Informativa* di cui all'art. 13 del *GDPR*;
 - b) richiedere il consenso informato *ex art. 6 GDPR*;
 - c) (nel caso) dare corso agli adempimenti necessari alla gestione delle casistiche inerenti il trasferimento dei *dati* all'estero, per il quale, in ogni caso vige il divieto come da clausola **9.** del presente *Accordo*.
- 3.9. Il *Fornitore* deve consentire al *Titolare* l'effettivo esercizio del potere di controllo di cui anche alla precedente clausola 2.4., rendendo quindi tutte le informazioni necessarie e utili a comprovare il rispetto degli obblighi assunti in qualità di *Responsabile del trattamento*.

4. Le misure di sicurezza

- 4.1. Il *Responsabile del trattamento* deve conservare i *dati personali* garantendone la separazione da quelli trattati per conto di terze parti e/o per proprio conto.
- 4.2. Il *Responsabile del trattamento*, tenendo conto dello stato dell'arte, della natura, dell'oggetto, del contesto, dei costi e delle finalità del *Trattamento*, nonché anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, deve adottare e mantenere, per sé e per le persone autorizzate al trattamento che collaborano con la sua organizzazione, appropriate misure di sicurezza, sia tecniche sia organizzative, per proteggere i *dati personali* trasmessi, conservati e/o comunque trattati da eventuali:
- a) distruzioni e/o perdite e/o modifiche e/o divulgazioni e/o accessi e/o danni di natura accidentale e/o colposa e/o illecita e/o illegale e in particolare, qualora il *trattamento* comporti trasmissioni di *dati* su una rete/sistema di comunicazione elettronico-informatico, da qualsiasi altra forma illecita di *trattamento*;
 - b) *trattamenti* di *dati* non consentiti e/o comune non conformi alle finalità di *trattamento* stesso come definite dal *Titolare*;
- e ciò in osservanza degli obblighi tutti derivanti dalle prescrizioni normative vigenti al fine, quindi, di garantire un livello di sicurezza adeguato al rischio.
- 4.3. Il *Responsabile del trattamento* implementerà, in relazione ai *trattamenti* di cui al *Contratto* misure di sicurezza idonee a garantire, se necessario e/o opportuno:
- a) la pseudonimizzazione e/o cifratura dei *dati*;
 - b) la permanenza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di *trattamento*;
 - c) la capacità di ripristinare in modo tempestivo la disponibilità e l'accesso dei *dati personali* in caso d'incidente tecnico, fisico, informatico e/o *data breach*.
- 4.4. Il *Responsabile del trattamento* fornisce al *Titolare*, nel caso di servizi di *Amministrazione di Sistema* forniti in *insourcing*, l'elenco con gli estremi identificativi delle persone fisiche che espletano, nell'ambito dell'incarico affidato funzioni di *Amministratori di Sistema* (di seguito anche "*A.d.S.*") unitamente all'attestazione delle conoscenze, dell'esperienza, della capacità e dell'affidabilità degli stessi soggetti, i quali devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di *trattamento*, ivi compreso il profilo relativo alla sicurezza come da valutazione propedeutica alla formale designazione ad *A.d.S.* da parte del *Titolare* il quale (in attuazione di quanto prescritto alla lettera f) del paragrafo 2 del Provvedimento del 28/11/2008 del *Garante* relativo agli *A.d.S.*) provvederà alla registrazione degli accessi logici ai sistemi da parte degli *A.d.S.* designati.

- 4.5. Il *Responsabile del trattamento* deve adottare misure tecniche e organizzative adeguate per salvaguardare la sicurezza di qualsiasi rete di comunicazione elettronica e/o dei servizi forniti all'*Azienda*, con specifico riferimento alle misure intese a prevenire l'intercettazione di comunicazioni e/o l'accesso non autorizzato a qualsiasi *computer* o *sistema*.
- 4.6. Il *Responsabile del trattamento* adotta e si attiene alle misure idonee di sicurezza al fine di massima salvaguardia del patrimonio informativo gestito da ASP come previste di cui all'Appendice "Security" allegata al presente *Accordo*: con la sottoscrizione del presente *Documento* e dei suoi allegati, pertanto, il *Fornitore* attesta e dichiara la conformità propria e della soluzione informatica prodotta/sviluppata, alle misure indicate nell'Appendice "Security".
- 4.7. In ogni caso, in ragione della riservatezza delle evidenze di analisi di conformità alle misure di cui alla suddetta Appendice "Security", il *Fornitore* condivide con ASP tali informazioni solo in caso di violazione e/o *data breach*.
- 4.8. Il *Responsabile del trattamento* dà esecuzione al contratto in aderenza alle politiche dell'*Azienda* in materia di *privacy* e sicurezza informatica, come anche risultanti dal proprio *Regolamento per l'utilizzo delle Risorse Informatiche* (di seguito anche "*Regolamento Informatico*") e ev. mm. ii .ss.: il *Regolamento Informatico* è reperibile e liberamente consultabile presso il sito *internet* aziendale ove pubblicato nell'apposita sezione e con la sottoscrizione del presente *Accordo* il *Responsabile del Trattamento* ne attesta la presa visione, comprensione e accettazione.

5. Misure tecniche, organizzative e da implementare

5.1. Il *Responsabile del Trattamento* garantisce:

- a) ove previsto, di aver nominato il D.P.O.;
- b) di mantenere aggiornato il proprio *Registro dei Trattamenti*;
- c) di ex art. 32 *GDPR*, di adeguatamente implementare le misure di sicurezza di cui alla precedente clausola 4. in considerazione dello stato e dell'evolversi della tecnologia sottesa al *trattamento dei dati*;
- d) di aver assunto e, se del caso, aggiornare una procedura di *data breach*;
- e) di aver assunto e, se del caso, aggiornare, procedure aziendali atte a garantire l'accesso ai sistemi aziendali e, nello specifico, ai *dati personali*, ai soli soggetti autorizzati e debitamente identificati e autenticati (con altresì previsione di sistemi di blocco in caso di errata reiterata autenticazione);
- f) di aver assunto e di aggiornare le misure tecniche e informatiche per la protezione dei sistemi IT/TN, garantendoli da accessi indesiderati;
- g) di non dare corso a conservazione di *dati* su supporti tecnici/informatici mobili, salvo casi eccezionali debitamente autorizzati e con contestuale applicazione di metodologie e tecniche di crittografia;
- h) (salvo esplicita autorizzazione del *Titolare* o se richiesto dall'esecuzione *Contratto*) di non collegare propri supporti informatici rimovibili esterni alle dotazioni e risorse informatiche di ASP;
- i) di non estrarre, eseguire, conservare, diffondere, comunicare copie analogiche e/o digitali dei *dati*;
- j) di aver previsto le opportune *policy* e/o procedure interne per la raccolta, lo smaltimento/distruzione/eliminazione dei supporti, analogici e informatici-digitali, contenenti *dati personali*;
- k) di dare corso a tutti gli obblighi previsti dalla normativa applicabile in materia.

6. Analisi dei rischi, *privacy by design* e *privacy by default*

- 6.1. Con riferimento agli esiti dell'analisi dei rischi effettuata dall'*Azienda* in merito ai *trattamenti di dati personali* cui concorre il *Fornitore*, lo stesso assicura massima cooperazione e assistenza al fine di dare effettività alle azioni di mitigazione previste dal *Titolare* per affrontare eventuali rischi identificati.
- 6.2. Il *Responsabile* dovrà consentire ad *ASP*, tenuto conto dello stato della tecnica, dei costi, della natura, dell'ambito e della finalità del relativo *trattamento*, di adottare, sia nella fase iniziale di determinazione dei mezzi di *trattamento*, che in costanza di trattamento stesso, ogni misura tecnica e organizzativa che al stessa riterrà opportuna per:
- a) garantire e attuare i principi previsti in materia di protezione *dati*;
 - b) tutelare i diritti degli *Interessati*.
- 6.3. In linea con i principi di *privacy by default*, dovranno essere trattati, per impostazione predefinita, esclusivamente quei *dati personali* necessari per ogni specifica finalità del *trattamento*; in particolare i *dati personali* non dovranno essere accessibili a un numero indefinito di soggetti senza l'intervento di una persona fisica.

7. Soggetti autorizzati ad effettuare i trattamenti

- 7.1. Il *Responsabile del trattamento* garantisce competenze e affidabilità dei propri dipendenti e collaboratori autorizzati al *trattamento dei dati personali* (di seguito anche "*Incaricati*") effettuati per conto di *ASP*.
- 7.2. Il *Responsabile del trattamento* garantisce che gli *Incaricati* abbiano ricevuto adeguata formazione in materia di protezione dei *dati personali* e sicurezza informatica, consegnando al *Titolare* le evidenze di tale formazione.
- 7.3. Il *Responsabile del trattamento* fornisce ai propri *Incaricati* le istruzioni necessarie alla conformità dei *trattamenti* dagli stessi effettuati alle prescrizioni del *GDPR* e della normativa italiana vigente in materia; a titolo esemplificativo e non esaustivo, il *Responsabile* dovrà:
- a) prescrivere che i soggetti autorizzati al *Trattamento* abbiano accesso ai soli *Dati* la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;
 - b) verificare che i soggetti autorizzati al *Trattamento* applichino tutte le disposizioni in materia di sicurezza informatica e organizzativa adeguate al rischio;
 - c) verificare che soggetti autorizzati al *Trattamento* conservino in luogo sicuro i supporti informatici e non contenenti atti e/o documenti con *categorie particolari* di *Dati* e/o la loro riproduzione, adottando contenitori con serratura (*trattamenti cartacei*);
 - d) - in conformità con quanto previsto nella suesposta clausola 4.4.: rispettare le previsioni *pro tempore* applicabili relative alla disciplina sugli *A.d.S.* contenute nel provvedimento del *Garante* del 27.11.2008 come modificato dal provvedimento del 25.06.2009 (impegnandosi a conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali *A.d.S.* e a fornirli prontamente al *Titolare*).
- 7.4. Con riferimento alla protezione e gestione dei *dati personali*, Il *Responsabile del trattamento*, impone ai soggetti autorizzati al *trattamento dei dati personali* obblighi di riservatezza e/o un adeguato obbligo legale di riservatezza, in ogni caso non meno onerosi di quelli previsti nel *Contratto* di cui il presente *Documento* costituisce parte integrante, vincolando detti soggetti anche per il periodo successivo all'estinzione del rapporto di collaborazione intrattenuto con il *Responsabile*.
- 7.5. In ogni caso il *Fornitore* sarà direttamente ritenuto responsabile per qualsiasi divulgazione di *dati personali* dovesse realizzarsi a opera dei soggetti dallo stesso autorizzati al *trattamento*.

8. Sub-Responsabili del trattamento di dati personali

- 8.1. Il *Fornitore*, nell'eventualità di subappalto occorso ai sensi della normativa vigente e applicabile in materia e, per tutte le evenienze, nei casi di conferimento di parte del *trattamento dei dati personali* a soggetti terzi *Sub-responsabili*:
- a) s'impegna a selezionarli tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti per la messa in atto di misure tecniche e organizzative adeguate a che il *Trattamento* soddisfi i requisiti di cui alla normativa *pro tempore* applicabile e garantisca la tutela dei diritti degli *Interessati*;
 - b) impone agli stessi condizioni vincolanti in materia di *trattamento dei dati personali* non meno onerose di quelle contenute nel presente *Accordo* indicando i loro compiti e richiedendoli di rispettare i medesimi obblighi, con riferimento alla disciplina sulla protezione dei *Dati*, imposti dal *Titolare* al *Responsabile* ai sensi della normativa *pro tempore* vigente e degli applicabili provvedimenti speciali del *G.d.P.*, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il *Trattamento* soddisfi i requisiti delle prescrizioni di legge e *Regolamento* come vigenti;
 - c) prescrive ai predetti i medesimi obblighi in materia e termini di riservatezza di cui alla pregressa clausola 7.4. del presente *Documento*.
- 8.2. Il *Responsabile* s'impegna altresì a informare il *Titolare* di eventuali modifiche previste riguardanti la sostituzione di altri *Sub-responsabili*, dandogli così la possibilità di opporsi a tali modifiche.
- 8.3. In via derogatoria rispetto alla prassi operativa prevista dal presente *Documento*, su precipua richiesta dell'*Azienda*, il *Fornitore* dovrà provvedere a che ogni *Sub-Responsabile* sottoscriva direttamente con il *Titolare* un accordo di *trattamento dei dati* che, a meno di ulteriori e specifiche esigenze, preveda sostanzialmente gli stessi termini del presente *Accordo*.
- 8.4. In ogni caso, il *Fornitore* si assume la responsabilità nei confronti di *ASP*, che mantiene quindi interamente indenne, per qualsiasi violazione e/o omissione e/o non conformità posta in essere da un *Sub-Responsabile* o da altri terzi soggetti dallo stesso incaricati e relative conseguenze tutte relative e discendenti (anche patrimoniali), indipendentemente dal fatto che il *Responsabile* abbia o meno rispettato i propri obblighi contrattuali, come anche da successiva clausola **14**.

9. Trattamento dei dati personali fuori dall'area economica europea

- 9.1. *ASP* non autorizza il trasferimento dei *dati personali* oggetto di *trattamento* al di fuori dell'Unione Europea, fatti salvi i casi di utilizzo da parte del Fornitori di *cloud* (es: *Google Suite/Workspace*) situati al di fuori dello SEE: in tale ipotesi i suoi *dati personali* dovranno necessariamente essere trasferiti anche al di fuori dell'UE e del relativo ambito di garanzia e di applicazione del suddetto Regolamento Europeo: in ogni caso il trattamento dei Suoi *dati* si baserà in conformità ai soli fini istituzionali².

² Nel caso di trasferimento *dati* verso fornitori aventi sede o *datacenter* negli USA, i fornitori USA sono soggetti ai poteri di regolamentazione della Federal Trade Commission degli Stati Uniti. In alcune situazioni, il fornitore USA potrebbe essere obbligato a comunicare i *dati personali* trasferiti, in risposta a richieste pervenutegli da autorità pubbliche per soddisfare i requisiti di sicurezza nazionale o di applicazione della legge locale (con conseguenti possibili accessi ai *dati*, di cui il fornitore *Co-Titolare* o *Responsabile* in base alla normativa locale potrebbe dover non dare avviso al *Titolare* e all'*Interessato*, i quali non potranno quindi esercitare i relativi diritti normalmente riconosciuti dal *GDPR*. Alla luce della normativa USA cui fa riferimento la Corte di Giustizia della Comunità Europea nella sentenza Schrems II del 16 luglio 2020 in astratto non si può escludere con assoluta certezza il rischio che in determinate occasionali situazioni legate a finalità di sicurezza nazionale (es. fini antiterrorismo) l'autorità pubblica americana operi un accesso ai dati. Tuttavia, fatta salve le ipotesi di natura eccezionale e frequenza improbabile di accesso da parte dell'autorità pubblica USA nei suddetti specifici e limitati casi, le condizioni applicati nel rapporto tra le parti ragionevolmente garantiscono in una tutela dei diritti degli interessati sostanzialmente identica a quella prevista dal *GDPR*.

10. Durata della nomina e obblighi di cancellazione dei dati personali

- 10.1. La nomina a *Responsabile del Trattamento* avrà efficacia fintanto che il *Fornitore* darà corso all'esecuzione del *Contratto*, fatti salvi gli specifici obblighi che per loro natura sono destinati a permanere anche successivamente.
- 10.2. Il *Fornitore* provvede alla cancellazione dei *dati personali* trattati:
 - a) in adempimento al presente *Documento* e per l'esecuzione del *Contratto*;
 - b) al termine del periodo di conservazione;
 - c) in qualsiasi circostanza in cui sia richiesto dal *Titolare*, compresa l'ipotesi in cui la stessa debba avvenire per dare seguito a specifica richiesta da parte di *Interessati*.
- 10.3. Qualora il rapporto tra le *Parti* venisse meno o perdesse efficacia per qualsiasi motivo o la fornitura/servizio di cui al *Contratto* non fosse più erogato, per qualsivoglia ragione, anche il presente *Accordo* verrà automaticamente meno senza bisogno di comunicazioni o revoche e il *Responsabile* non sarà più legittimato a trattare i *Dati* del *Titolare*.
- 10.4. In conformità alle clausole precedenti, alla cessazione del *Contratto* e, conseguentemente del presente *Accordo*, per qualsiasi causa intervenuta a discrezione di *ASP* i *dati personali* dovranno essere:
 - a) distrutti, salvi solo i casi in cui la loro conservazione sia richiesta da norme di legge e/o da altri fini (contabili, fiscali ecc.)
oppure
 - b) restituiti alla stessa, unitamente a qualsiasi supporto fisico e/o documento analogico e/o informatico contenente *dati personali* di proprietà del *Titolare*;
 in ogni caso non trattenendo il *Fornitore* presso di sé alcuna copia dei *Dati*.
- 10.5. Le previsioni di cui alle precedenti clausole fanno salvo quanto eventualmente e diversamente previsto dalla normativa vigente in relazione ai servizi/attività oggetto del *Contratto* intercorso fra le *Parti*.

11. Audit

- 11.1. Il *Fornitore* si rende disponibile, anche presso le proprie sedi, a specifici *audit* in tema di *privacy* e sicurezza informatica cui il *Titolare del trattamento* potrà dare corso direttamente e/o per tramite di terzi incaricati anche al fine di verificare la conformità delle procedure e delle attività poste in essere dal *Responsabile* a quanto previsto dal presente *Accordo* e dalla normativa vigente in materia come applicabile. A titolo esemplificativo, l'attività di *audit* potrà esplicarsi attraverso esame documentale, interviste, accesso ai locali e/o osservazioni dei mezzi, condizioni e/o procedure operative messi in opera, ai fini dell'esecuzione del *Contratto*, dal *Responsabile* e potrà altresì prevedere la richiesta di compilazione, da parte di quest'ultimo, dei questionari di autovalutazione.
- 11.2. In conseguenza di quanto alla precedente clausola 11.1. e previ accordi sul programma di *audit*, il *Responsabile* consente all'*Azienda* l'accesso ai propri locali e ai locali di qualsiasi *Sub-Responsabile*, ai *computer*, alla rete informatica aziendale e altri sistemi informativi, ad atti, documenti e a quanto ragionevolmente richiesto per verificare che i predetti *Responsabile* e/o *Sub-fornitori*, rispettino gli obblighi derivanti dalla normativa vigente in materia di protezione dei *dati personali* e dal presente *Accordo*.
- 11.3. L'esperimento di tali *audit* non deve avere a oggetto *dati* di terze parti e/o informazioni sottoposte ad obblighi di riservatezza degli interessi commerciali, salvo eccezioni eventualmente previste *ex lege* o *Regolamento*.

- 11.4. Nel caso in cui le risultanze dell'attività di *audit* forniscano evidenze di violazioni alla normativa in materia di protezione dei *dati personali* e al presente *Accordo*, quali ad esempio quelle indicate all'art. 83 comma 5 (con esclusione della lett. e) *del GDPR* ASP potrà risolvere il *Contratto* o chiedere una cospicua riduzione del prezzo pattuito in sede di *Contratto* quale corrispettivo della fornitura.
- 11.5. Nel caso in cui l'*audit* fornisca evidenze di violazioni gravi, quali ad esempio quelle indicate all'art. 83 comma 4 lett. a) *del GDPR*, l'Asp potrà chiedere una cospicua riduzione del prezzo pattuito in sede di *Contratto* quale corrispettivo della fornitura.
- 11.6. Il *Responsabile* si riserva la facoltà di rilevare e segnalare al *Titolare* eventuali istruzioni e/o procedure ritenute non conformi alla legge e/o *Regolamento*.
- 11.7. Il rifiuto del *Responsabile* a consentire al *Titolare* di svolgere l'attività di *audit* comporterà la risoluzione del *Contratto* per ingiustificato inadempimento del *Fornitore* e relative conseguenze anche sotto il profilo risarcitorio.
- 11.8. In conformità con quanto previsto dalla suesposta clausola **8.**, le *Parti* concordemente riconoscono i diritti e i doveri di cui alla presente clausola **11.** come *in toto* applicabili a qualsivoglia *Sub-fornitore* del *Responsabile*.
- 11.9. In ogni caso il *Titolare* s'impegna per sé e per i terzi dallo stesso incaricati, a che le informazioni fornite a fini di verifica/*audit* siano utilizzate unicamente per tali finalità.

12. Indagini dell'Autorità e reclami

- 12.1. Nei limiti della normativa applicabile, il *Responsabile* o qualsiasi *Sub-Responsabile* informa senza alcun indugio il *Titolare* in caso di ricevimento di qualsivoglia, a seconda del caso, reclamo/riciesta/comunicazione (di seguito complessivamente anche "*Istanze*") da parte:
 - a) del *Garante per la protezione dei dati personali*
 - b) delle Forze dell'Ordine e/o dall'Autorità Giudiziaria
 - c) di uno o più soggetti *Interessati*.

contestualmente fornendo, anche in esecuzione del *Contratto*, la dovuta assistenza ad ASP per garantire che l'*Azienda* possa dare riscontro alle predette *Istanze* nei termini previsti dalla normativa vigente applicabile.

13. Violazione dei dati personali e obblighi di notifica

- 13.1. Il *Fornitore*, in virtù di quanto previsto dall'art. 33 del *Regolamento*, dovrà comunicare a mezzo di posta elettronica certificata al *Titolare*, nel minor tempo possibile, senza giustificato ritardo e comunque non oltre 24 (ventiquattro) ore da quando ne abbia avuto notizia, qualsiasi violazione (c.d. "*data breach*") di sicurezza che abbia comportato accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata e/o l'accesso ai *dati personali* trasmessi, conservati e/o comunque trattati, ivi incluse quelle che abbiano riguardato i propri *Sub-Fornitori*.
- 13.2. La comunicazione di cui alla precedente clausola 13.1. dovrà contenere tutte le informazioni atte a esaurivamente:
 - a) descrivere la natura della violazione dei *dati personali*;
 - b) identificare le categorie e il numero approssimativo degli *Interessati* e delle registrazioni dei *dati personali* coinvolti dal *data breach*;
 - c) indicare i recapiti del D.P.O. nominato e/o del soggetto competente alla gestione del *data breach*;
 - d) descrivere le probabili conseguenze correlate attese alla violazione dei *dati personali*;

e) rappresentare le misure adottate o che s'intende adottare per affrontare la violazione della sicurezza, compreso, ove opportuno, quelle finalizzate a per mitigare i suoi possibili effetti negativi;

e sarà corredata da ogni altra indicazione e/o dato in ogni modo utile alla gestione del *data breach*.

13.3. Il *Responsabile* dovrà fornire all'*Azienda* tutto il supporto e collaborazione necessari e utili ai fini:

- a) dell'adempimento in capo al *Titolare* degli obblighi di notifica al *Garante* e/o agli *Interessati* di cui all'art. 34 del *GDPR*;
- b) delle indagini e sulle valutazioni in ordine alla violazione di *dati*, anche al fine di individuare, prevenire e limitare gli effetti negativi della stessa, conformemente ai suoi obblighi ai sensi del presente articolo e, previo accordo con il *Titolare*, per svolgere qualsiasi azione che si renda necessaria per porre rimedio alla violazione stessa.

13.4. Il *Fornitore* dovrà costituire e mantenere aggiornato un *Registro dei data breach* dettagliante le relative circostanze e le conseguenze, nonché i conseguenti provvedimenti adottati a fini risolutivi: invero, dette informazioni dovranno consentire al *Titolare* di dare corso alle verifiche relative al rispetto da parte del *Responsabile* delle prescrizioni di cui alla presente clausola **13**.

13.5. Il *Responsabile* non potrà e non dovrà rilasciare e/o pubblicare alcun comunicato stampa e/o relazione ecc., né dare notizia, attraverso qualsivoglia mezzo e/o modalità in relazione eventuali *data breach* e/o violazioni di *trattamento* senza aver ottenuto il previo consenso scritto del *Titolare del trattamento*.

14. Responsabilità e manleva

14.1. Il *Fornitore* tiene indenne e manleva l'*Azienda* da qualsivoglia perdita, costo, multa, sanzione, danno e/o responsabilità, di qualsiasi natura, connessa, relativa e/o conseguente, direttamente e/o indirettamente, a una qualsiasi violazione e/o non conformità da parte del *Responsabile* delle disposizioni contenute nel presente *Accordo* e/o comunque da prescrizioni imperative di legge o *Regolamento*.

14.2. In conformità con quanto previsto dalla precedente clausola 8.4., l'esenzione di responsabilità di cui alla precedente clausola 14.1. trova piena e sostanziale applicazione anche nel caso in cui la predetta violazione e/o non conformità sia riconducibile a *Sub-Responsabile del trattamento* come individuato e nominato dal *Responsabile*.

14.3. A fronte della ricezione di un reclamo o, più in generale, di una contestazione relativa alle attività oggetto del presente *Accordo*, il *Fornitore*:

- a) avverte, senza soluzione di continuità e in ogni caso a stretto giro, in forma scritta, l'*Azienda* del reclamo/contestazione;
- a) non fornisce dettagli al *soggetto* reclamante/contestante senza la preventiva interazione e confronto con il *Titolare*;
- b) non ha facoltà di transigere la controversia o in ogni modo accordarsi con la controparte, senza il previo consenso scritto di *ASP*;
- c) fornisce al *Titolare* tutta l'assistenza che potrebbe ragionevolmente richiedere nella gestione del reclamo/contestazione.

15. Oneri di Accordo

15.1. Il presente *Accordo* e l'adempimento degli obblighi e oneri conseguentemente derivanti da parte del *Responsabile del Trattamento* in relazione a detta sua nomina non comportano alcun diritto per lo stesso, che con la sottoscrizione del presente Documento espressamente vi rinunzia, a compensi e/o indennità e/o rimborsi e/o *benefit* e/o altra utilità, di qualsivoglia

natura, ulteriore, diversa, aggiuntiva e/o integrativa rispetto a quanto già definito in sede di *Contratto*.

16. Soppravvenienza dell'Accordo

- 16.1. Le *Parti* concordano che qualora una o più clausole del presente *Documento* vengano colpite da nullità o invalidità o si rendano inefficaci o inapplicabili in conseguenza dall'effetto di legge e/o *Regolamento* e/o sentenza e/o provvedimento del *G.d.P.*, un tanto non comporterà la nullità e/o l'invalidità e/o l'inefficacia e/o l'inapplicabilità dell'insieme del presente *Accordo*, né di altererà la validità, l'efficacia e il carattere obbligatorio dell'insieme delle restanti altre clausole.

17. Sottoscrizione e Rinvio

- 17.1. Con la sottoscrizione del presente *Documento*, le *Parti* attestano di averne interamente inteso il contenuto, gli obblighi, gli oneri, le finalità e le responsabilità tutte relative e conseguenti e di accettarle integralmente e senza riserva alcuna ai sensi e per gli effetti di cui al *GDPR* e, più in generale, della normativa applicabile in materia e di legge in generale.
- 17.2. Per tutto quanto non espressamente previsto e disciplinato nel presente *Accordo*, si rinvia alle disposizioni vigenti di cui al *GDPR* e alla normativa italiana applicabile in materia, nonché a quanto già eventualmente disposto in sede di *Contratto* e alla legge in generale.

Bologna ,

Il *Titolare del trattamento*
ASP CITTÀ DI BOLOGNA
F.to il *Sub-Delegato*

Il *Responsabile del Trattamento*

* *

APPENDICE 1 - GLOSSARIO

“Accesso”: diritto dell’*Interessato* al *trattamento* di richiedere e ottenere informazioni inerenti al trattamento dei propri *dati personali*.

“Accountability”: principio di responsabilizzazione dei *Titolari* e *Responsabili del trattamento* introdotto dal *GDPR* e che s’identifica con l’obbligo posto in capo agli stessi di adottare tutte le misure e procedure organizzative (nonché in determinati casi anche le corrette politiche in materia di protezione) tecniche e legali adeguate e necessarie a garantire l’uniformità ai principi sanciti dal *GDPR* e l’idonea protezione dei *dati personali* trattati. La responsabilizzazione si traduce altresì nella capacità di dimostrare la conformità delle modalità con cui si trattano i *dati personali* al *GDPR*.

“Amministratore di Sistema” o “A.d.S.”: soggetto esperto che presenta le qualifiche e le competenze tecniche-specialistiche in materia di gestione-trattazione informatica dei dati personali (con particolare riferimento alla sicurezza delle banche dati e delle reti telematiche riferibili all’organizzazione del *Titolare del trattamento*) e il cui intervento si pone come fondamentale sin dalle fasi di progettazione e protezione dei *Dati*. L’attività dell’*A.d.S.* comporta la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali e istituzionali: al medesimo viene quindi spesso co-affidato anche il compito di vigilare sul corretto utilizzo dei sistemi informatici di propri dell’organizzazione del *Titolare*. Non coincide con il *D.P.O.* rispetto al quale svolge funzioni e compiti di controllo e coauditazione.

“Appendice Security”: consiste nelle misure di sicurezza che il *Titolare* determina assicurando un livello minimo di sicurezza, e che possono essere aggiornate e implementate dal *Titolare*, di volta in volta, in conformità alle previsioni del presente *Accordo*.

“Autorità di controllo”: Autorità Pubblica indipendente individuata in ogni stato membro dell’Unione Europea incaricata di sorvegliare l’applicazione del *GDPR* al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all’interno dell’U.E.

“Compliance”: conformità rispetto alle regole e alle disposizioni imposte dal *GDPR* e dalle altre normative vigenti.

“Crittografia”: operazione con la quale un messaggio da inviare, un “messaggio semplice o in chiaro”, viene convertito in un “messaggio cifrato” che è incomprensibile per un terzo e diventa così confidenziale.

“Data breach”: violazione dei *Dati Personali* ossia un’infrazione di sicurezza che comporta (accidentalmente o in modo illecito/doloso) - la distruzione, la perdita, la modifica, la divulgazione non autorizzata e/o l’accesso ai *Dati Personali* trasmessi, conservati e/o comunque trattati e che può compromettere la riservatezza, l’integrità e/o la disponibilità degli stessi.

“Dati personali”: qualsiasi informazione riguardante una persona fisica identificata o identificabile («*Interessato*»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

“Data Protection Privacy Impact Assessment” o “DPIA”: Procedura di analisi finalizzata alla valutazione di tutti i processi e le banche dati in una determinata sezione/area/reparto/ecc. dell’organizzazione del *Titolare* (quali: scopo, periodo di conservazione diritti degli interessati ecc.), e dei relativi connessi rischi per la sicurezza dei dati (accesso ai dati, frodi ecc.) e il loro potenziale impatto in materia di *privacy* e alla conseguente determinazione delle misure tecniche e organizzative necessarie per affrontarli e proteggere i *Dati*. È obbligatoria per le tipologie di *trattamenti* che presentano rischi elevati in fatto di diritti e libertà delle persone fisiche.

“Data Protection Officer” o “D.P.O.”: Il D.P.O. è il garante del rispetto del *GDPR* in una Pubblica Amministrazione, Azienda, Ente, ecc. ; ha come principale responsabilità quella di osservare, valutare e organizzare la gestione del *trattamento di dati personali* nonché la loro protezione all'interno dell'organizzazione del titolare, per fare in modo che gli stessi vengano trattati *ex lege*. I suoi compiti comprendono: l'informazione e la consulenza sia al *Titolare* che ai dipendenti del predetto; la verifica del rispetto delle disposizioni normative e aziendali in materia di protezione dei *Dati*; assistenza e rilascio pareri in ambito di *DPIA* con conseguente validazione dei trattamenti registrati; monitoraggio dell'esecuzione; collaborazione con l'autorità di vigilanza. È obbligatorio nominare il *D.P.O.* qualora il *Trattamento* sia effettuato da un'autorità pubblica o da un organismo pubblico (ad eccezione delle autorità giurisdizionali nello svolgimento delle loro funzioni), nel caso in cui le attività del *trattamento* riguardano ambiti e/o finalità che, per loro natura, necessitano del monitoraggio regolare e sistematico degli interessati su larga scala e/o nel caso in cui le stesse riguardino, comunque su larga scala, categorie particolari di dati personali (*dati particolari*) nonché di dati relativi a condanne penali/misure di sicurezza/reati.

“Garante per la protezione dei dati personali” o “Garante”: è l'autorità di controllo responsabile per la protezione dei *dati personali* in Italia;

“GDPR” o “Regolamento”: si intende il *Regolamento UE 2016/679* sulla protezione delle persone fisiche relativamente al trattamento dei *dati personali* e della loro libera circolazione (*General Data Protection Regulation*) che sarà direttamente applicabile dal 25 maggio 2018.

“Interessato”: è la persona fisica, identificata e/o identificabile, cui si riferiscono i *dati personali* trattati.

“Minimizzazione dei dati”: principio per cui la raccolta e il *trattamento dei dati* devono essere effettuati solo se necessario per lo scopo per il quale vengono trattati, con contestuale obbligo in capo al titolare di non raccolta/eliminazione di tutti i restanti non essenziali per le operazioni di trattamento di ciascuna applicazione.

“Misure minime di sicurezza ICT”: emanate dall'AgID, sono un riferimento pratico per valutare, da parte delle Pubbliche Amministrazioni, in modo autonomo la propria situazione e avviare un percorso di monitoraggio e miglioramento per migliorare il livello di sicurezza informatica al fine di contrastare le minacce informatiche più frequente. Le misure minime: 1) forniscono un riferimento operativo direttamente utilizzabile (*checklist*); 2) stabiliscono una base comune di misure tecniche ed organizzative irrinunciabili; 3) forniscono uno strumento utile a verificare lo stato di protezione contro le minacce informatiche e poter tracciare un percorso di miglioramento; 4) responsabilizzano le P.A. sulla necessità di migliorare e mantenere adeguato il proprio livello di protezione cibernetica.

“Misure di sicurezza”: accorgimenti tecnici e organizzativi idonei a garantire un livello di sicurezza adeguato al rischio, adottati dal titolare e dal soggetto delegato attuatore al fine di assicurare e dimostrare che il trattamento dei dati è realizzato conformemente al *GDPR*. Le misure di sicurezza possono essere diverse tipologie; per esempio nell'ambito delle misure di sicurezza relative alle risorse informatiche si distinguono: 1) misure di sicurezza tecniche, cioè volte a proteggere le architetture di rete, gli applicativi e le banche *Dati* e la trasmissione dei *Dati* stessi (esempio: autenticazione informatica, uso delle password, sistema di autorizzazione e configurazione dei profili di accesso, *antivirus* e *antispam*, *backup*, pseudonimizzazione/anonimizzazione dei *Dati*, ecc.); 2) misure di sicurezza fisiche, cioè volte a proteggere le aree, i locali e gli archivi da accessi non autorizzati (esempio: armadi chiusi a chiave, controllo degli accessi con *badge* o altri sistemi di registrazione dei visitatori, vigilanza, ecc.); 3) misure di sicurezza organizzative, cioè individuate dal *Titolare* per l'assegnazione di compiti e responsabilità, per la costituzione di una cultura aziendale sulla tematica di protezione *Dati*, per garantire che i *trattamenti* avvengano per finalità autorizzate e consentite (esempio: informativa e consenso, deleghe di funzioni, autorizzazioni a trattare i *dati*, definizione dei termini di conservazione dei *dati*, gestione *data breach*, formazione dei dipendenti).

“Normativa Applicabile”: s’intende l’insieme delle norme rilevanti in materia protezione dei *dati personali*, incluso il Regolamento *Privacy* UE 2016/679 (GDPR) e ogni provvedimento del Garante per la protezione dei dati personali e del WP Art. 29.

“Principio *privacy by Default*”: principio per il quale il *Titolare* deve trattare i *dati personali* esclusivamente nella misura necessaria e sufficiente alle finalità previste e per il periodo strettamente necessario alle stesse e ciò per impostazione predefinita: egli pertanto deve mettere in atto misure organizzative e tecniche sin dalla fase della progettazione delle operazioni di trattamento al fine di salvaguardare *ab origine* la protezione dei *dati personali*.

“Principio *privacy by Design*”: Principio che impone al *titolare del trattamento* di agire nell’ottica della prevenzione del rischio e ponendo al centro l’interessato rispetto al quale dev’essere predisposto un sistema di tutela effettiva (e non solamente formale). La *privacy by design* prevede quindi: la prevenzione nella fase di progettazione, la *privacy by default*, sicurezza dei dati durante tutto il ciclo dei processi aziendali, la trasparenza.

“Pseudonimizzazione dei dati”: il *trattamento* dei *dati personali* in modo tale che i *dati personali* non possano più essere attribuiti a un *Interessato* specifico senza l’utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali *dati personali* non siano attribuiti a una persona fisica identificata o identificabile.

“Reclamo”: si intende ogni azione, reclamo, segnalazione presentata nei confronti del *Titolare* o di un *Suo Responsabile del trattamento*.

“Registro di trattamento dei dati”: *Registro* (generalmente informatico) nel quale devono essere riportate tutte le informazioni inerenti l’interesse delle operazioni di trattamento effettuate internamente a un’organizzazione (Pubblica Amministrazione, azienda privata o pubblica, Ente, ecc.). Nel *Registro dei Trattamenti* devono essere specificate le finalità degli stessi, le modalità di conservazione, le categorie degli interessati e dei dati personali, gli eventuali trasferimenti verso paesi terzi, eventuali misure di sicurezza applicate, ecc.

“Regolamento Informatico”: Regolamento che disciplina l’uso delle risorse informatiche (*hardware, software, device ecc.*) in uso all’interno dell’organizzazione cui fa capo il titolare e assegnate ai soggetti di cui all’organigramma *privacy* (esempio: *Responsabile, Sub-Responsabili, Incaricati al trattamento*, ecc.) che le utilizzano in costanza di *Trattamento*.

“Responsabile del trattamento”: soggetto esterno all’organizzazione del *Titolare del trattamento* (Persona fisica o giuridica o Autorità pubblica), tenuto (a seguito di convenzione, contratto, verbale di aggiudicazione e/o provvedimento di nomina a/o altro atto equivalente) a effettuare trattamenti di dati personali per conto del *Titolare del trattamento*.

“Riservatezza dei dati”: garanzia che i *dati* siano accessibili solo alle persone autorizzate, e quindi che le comunicazioni e/o i *dati* memorizzati non siano accessibili (e quindi intercettati, visionati, letti ecc.) da soggetti non autorizzati.

“Soggetto Sub Delegato Attuatore”: sono i soggetti interni all’organizzazione del *Titolare del trattamento* nominati, autorizzati e delegati dal soggetto delegato allo svolgimento di compiti in materia di *privacy*. I soggetti *Sub Delegati Attuatori* in ASP corrispondono ai profili-funzioni: dirigenziali e/o di responsabilità e/o di coordinamento e/o di riferimento interna dell’Area e/o Servizio e/o Unità Operativa e/o Ufficio secondo il modello organizzativo aziendale in vigore.

“Titolare del Trattamento”: la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di *dati personali*; quando le finalità e i mezzi di tale *trattamento* sono determinati dal diritto dell’Unione o degli Stati membri, il *Titolare del trattamento* o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell’Unione o degli Stati membri.

“Trattamento dei dati personali” o “Trattamento”: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a *dati personali* o insiemi di *dati personali*, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

* *

APPENDICE 2 - APPENDICE “SECURITY”

Al fine di definire le misure idonee di sicurezza si fa riferimento alle indicazioni *dell'Autorità nazionale per la cyber sicurezza*ⁱ e dell'*Agenzia per l'Italia Digitale*ⁱⁱ con particolare riferimento alle **misure minime per la sicurezza ICT** stabilite da questa agenzia con la circolare del 18 aprile 2017, n. 2/2017 pubblicata sulla Gazzetta Ufficialeⁱⁱⁱ, al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informativi.

Inoltre il Responsabile del Trattamento deve attenersi alle indicazioni del Regolamento per l'utilizzo delle Risorse Informatiche di ASP CITTÀ DI BOLOGNA – Azienda Pubblica di Servizi alla Persona reperibile presso il sito *internet* aziendale (<https://www.aspbologna.it>), come ivi pubblicato nell'apposita sezione, avendo cura di consultarlo all'atto della sottoscrizione del suesteso Documento nonché periodicamente in conseguenza e a fini di aggiornamento.

* *

ⁱ <https://www.acn.gov.it/>

ⁱⁱ <https://www.agid.gov.it/>

ⁱⁱⁱ <https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict>