



**Regione Lombardia**  
IL CONSIGLIO

---

**DD N. 170**

**del 05/06/2025**

---

**UFFICIO CONTRATTI E ICT**

**DECRETO DIRIGENZIALE**

Oggetto: ACQUISIZIONE DEL PERCORSO DI FORMAZIONE ONLINE SULLA SICUREZZA INFORMATICA, TERZA ANNUALITÀ, DESTINATO AI DIPENDENTI DEL CONSIGLIO REGIONALE DELLA LOMBARDIA TRAMITE ACCESSO ALLA PIATTAFORMA DI E-LEARNING "CYBER GURU AWARENESS" DI PROPRIETÀ DI CYBER GURU S.R.L. - AFFIDAMENTO DIRETTO, AI SENSI DELL'ARTICOLO 50, COMMA 1, LETTERA B) A CYBER GURU S.R.L. DI ROMA - DECISIONE DI CONTRARRE

---

Rep. 2023.XII.4.1.2.24

## IL DIRIGENTE

VISTA la legge regionale 7 luglio 2008, n. 20 *"Testo unico in materia di organizzazione e personale"*;

VISTO il regolamento contabile, approvato con deliberazione del Consiglio regionale 15 febbraio 2011, n. IX/143, e modificato con deliberazioni del Consiglio regionale 8 aprile 2014, n. X/356, e 28 luglio 2015, n. X/751;

VISTO il decreto legislativo 23 giugno 2011, n. 118 *"Disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi, a norma degli articoli 1 e 2 della legge 5 maggio 2009, n. 42"*, così come modificato e integrato dal decreto legislativo 10 agosto 2014, n. 126;

### RICHIAMATE:

- la deliberazione dell'Ufficio di presidenza 11 novembre 2024, n. 386 *"III Provvedimento organizzativo Anno 2024: conferimento incarichi dirigenziali"*, che ha, tra l'altro:
  - attribuito alla sottoscritta l'incarico triennale di dirigente dell'Ufficio Contratti e ICT, con decorrenza dal 1° gennaio 2025;
  - conferito al dott. Mario Di Stefano l'incarico di dirigente ad interim dell'Ufficio Comunicazione interna e Formazione, con decorrenza dal 1° gennaio 2025;
- la deliberazione del Consiglio regionale 17 dicembre 2024, n. XII/662, di approvazione del bilancio di previsione finanziario per gli anni 2025-2026-2027 per il funzionamento del Consiglio regionale;
- la deliberazione dell'Ufficio di presidenza 18 dicembre 2024, n. 423, di approvazione del documento tecnico di accompagnamento e di assegnazione delle quote di bilancio al segretario generale e al datore di lavoro, per gli anni 2025-2026-2027;
- la deliberazione dell'Ufficio di presidenza 3 febbraio 2025, n. 29 recante *"Piano Integrato di Attività e Organizzazione (PIAO) del Consiglio regionale della Lombardia, triennio 2025 - 2026 (anno 2025): approvazione"* e, in particolare, la tabella di cui al paragrafo 6.19 (Ulteriori misure di prevenzione della corruzione) della *"Sottosezione-Rischi corruttivi e trasparenza anni 2025-2027"*, in cui si prevede, tra l'altro, che *"Per i servizi e le forniture di importo inferiore a euro 40.000,00 il RUP procede all'affidamento all'operatore economico individuato, nella richiesta di acquisto (RDA) trasmessa via EDMA, dal dirigente cui afferisce il progetto e al quale fanno capo i relativi poteri di spesa anche senza previo interpello di altri operatori economici"*;
- la deliberazione dell'Ufficio di presidenza 28 luglio 2021, n. 184 *"Aggiornamento 2021 dell'assetto organizzativo privacy - modifiche alla deliberazione 1 aprile 2019, n. 111 'Definizione dell'assetto organizzativo privacy - Articolazione delle competenze in materia di protezione dei dati personali (Regolamento UE 2016/679 e d.lgs. 196/2003)'"*, come modificata dalla deliberazione 6 aprile 2020, n. 78, con cui è stata attribuita, tra l'altro, ai titolari di incarichi dirigenziali la competenza ad adottare gli atti di designazione del responsabile del trattamento di cui all'art. 28 Regolamento UE 2016/679 (RGPD) e di autorizzazione alla designazione di ulteriori sub responsabili del trattamento ai sensi dei paragrafi 2 e 4 dello stesso articolo, nell'ambito dei contratti pubblici per l'acquisizione di beni, servizi e forniture da loro stipulati per conto dell'Amministrazione;

VISTO il decreto del Segretario generale 23 dicembre 2024, n. 543, di approvazione del bilancio finanziario gestionale per gli anni 2025-2026-2027 per il funzionamento del Consiglio regionale e di assegnazione delle quote ai dirigenti;

VISTO il decreto legislativo 31 marzo 2023, n. 36 *"Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici"* (di seguito Codice), entrato in vigore il 1° aprile 2023, con efficacia dal 1° luglio 2023, come modificato dal decreto legislativo 31 dicembre 2024 n. 209, e, in particolare, le seguenti disposizioni:

- articolo 15, comma 1, secondo cui nel primo atto di avvio dell'intervento pubblico da realizzare mediante un contratto, le stazioni appaltanti nominano un responsabile unico del progetto per le fasi di programmazione, progettazione, affidamento e per l'esecuzione di ciascuna procedura soggetta al Codice;
- articolo 17, comma 2, ai sensi del quale le pubbliche amministrazioni, nell'atto con il quale adottano la decisione di contrarre per l'affidamento diretto, individuano l'oggetto, l'importo e il contraente, unitamente alle ragioni della sua scelta, ai requisiti di carattere generale e, se necessari, a quelli inerenti alla capacità economico-finanziaria e tecnico-professionale;
- articolo 50, comma 1, lettera b), ai sensi del quale *"le stazioni appaltanti procedono all'affidamento dei contratti di servizi di importo inferiore a 140.000 euro, anche senza consultazione di più operatori economici, mediante affidamento diretto, assicurando che siano scelti soggetti in possesso di documentate esperienze pregresse idonee all'esecuzione delle prestazioni contrattuali, anche individuati tra gli iscritti in elenchi o albi istituiti dalla stazione appaltante"*;
- articolo 52, comma 1 - primo periodo -, ai sensi del quale *"nelle procedure di affidamento di cui all'articolo 50, comma 1 lettere a) e b), di importo inferiore a 40.000,00 euro, gli operatori economici attestano con dichiarazione sostitutiva di atto di notorietà il possesso dei requisiti di partecipazione e qualificazione richiesti"*;
- Allegato I.1 che definisce, all'articolo 3, comma 1, lettera d), l'affidamento diretto come *"l'affidamento del contratto senza una procedura di gara, nel quale, anche nel caso di previo interpello di più operatori economici, la scelta è operata discrezionalmente dalla stazione appaltante o dall'ente concedente, nel rispetto dei criteri qualitativi e quantitativi di cui all'articolo 50, comma 1 lettere a) e b), del codice e dei requisiti generali o speciali previsti dal medesimo codice"*;
- articolo 226, comma 5, secondo cui *"ogni richiamo in disposizioni legislative, regolamentari o amministrative vigenti al decreto legislativo 18 aprile 2016, n. 50, o al codice dei contratti pubblici vigente alla data di entrata in vigore del codice, si intende riferito alle corrispondenti disposizioni del codice o, in mancanza, ai principi desumibili dal codice stesso"*;

DATO ATTO che il Segretario generale, con il suindicato decreto 543/2024, ha individuato, di norma e fatte salve le diverse disposizioni di singoli atti, per le procedure di affidamento ai sensi dell'articolo 50 del Codice e per le procedure di scelta del contraente ai sensi degli articoli 70 e ss. del Codice, nonché per le concessioni, come Responsabile unico del progetto (di seguito RUP) ai sensi dell'articolo 15 del Codice, il dirigente dell'ufficio contratti e ICT;

VISTO il decreto dirigenziale 8 febbraio 2024, n. 39, recante "*Linee guida per l'esecuzione dei controlli sulle dichiarazioni sostitutive di certificazione e di atto notorio ai sensi del D.P.R. 445/2000*";

VISTA la richiesta di acquisizione (RDA) n. 12 pervenuta all'U.O. Contratti ed economato, completa di pareri, tramite il sistema documentale EDMA, in data 9 aprile 2025, con la quale il Dirigente dell'Ufficio Comunicazione interna e formazione ha:

- esposto la necessità di provvedere all'affidamento del servizio in oggetto mediante acquisizione di credenziali per l'accesso alla piattaforma di e-learning "Cyber Guru Awareness", di proprietà della società Cyber Guru S.r.l., per l'erogazione della terza annualità e della terza parte dei corsi di formazione online sulla sicurezza informatica (moduli dal n. 25 al n. 36), destinati ai dipendenti del Consiglio regionale, per il periodo di durata di 13 mesi, comprensivi delle tempistiche di attivazione, decorrenti dalla data indicata nella comunicazione di stipulazione del contratto;
- stimato l'importo massimo del servizio in euro 8.775,00 (oltre IVA), calcolato moltiplicando l'importo unitario di ogni utenza, stimato in euro 29,25 (oltre IVA), per il numero massimo di utenze richiedibili dall'Amministrazione pari a n. 300;
- individuato le modalità di svolgimento del servizio e i relativi obblighi in capo al Fornitore stabilendo, in particolare, compresi nel corrispettivo contrattuale:
  1. la fruizione della terza parte del percorso di formazione, in modalità *e-learning*, sulla sicurezza informatica, suddiviso in 12 moduli (moduli da 25 a 36);
  2. l'erogazione dei precedenti moduli formativi predisposti per le precedenti annualità a favore dei dipendenti non presenti in Consiglio negli anni in cui erano state erogati la prima e la seconda annualità di corso o che, comunque, non abbiano seguito le annualità precedenti (moduli da 1 a 24);
  3. un servizio di CSM (Customer Success Management) volto a supportare l'Amministrazione nella corretta implementazione e gestione del servizio di training (al raggiungimento dell'attivazione di n. 251 utenze);
  4. un pacchetto composto da n. 16 ore di servizio di un team di supporto per le attività di set-up iniziale della piattaforma, per la fase di rendicontazione complessiva dei percorsi, per l'eventuale download massivo degli attestati e per l'invio ai referenti dell'Ufficio Comunicazione interna e formazione;
- chiesto di affidare il servizio alla società Cyber Guru S.r.l., con sede legale in Roma - codice fiscale e partita IVA 14324511006, per ragioni di natura tecnica in quanto titolare dell'uso esclusivo e del diritto di commercializzazione, in favore di soggetti pubblici e privati, della suddetta piattaforma e per garantire la continuità dei percorsi formativi già effettuati dai dipendenti del Consiglio;
- dichiarato che non vi sono convenzioni ARIA S.p.A. o Consip attive per l'erogazione del servizio in oggetto;
- indicato di assumere il ruolo di Direttore dell'Esecuzione del Contratto;

#### ACQUISITI AGLI ATTI:

- il parere del 3 aprile 2025, con cui l'Ufficio segreteria dell'Ufficio di presidenza, prevenzione della corruzione, trasparenza e privacy ha evidenziato, in base a quanto riportato nella RDA, che si rende necessaria la designazione del Fornitore come responsabile del trattamento dei dati ai sensi dell'articolo 28 del Regolamento UE 2016/679 (RGDP), trasmettendo a tal fine l'atto negoziale di designazione;
- il parere del 3 aprile 2025, con cui l'u.o. Prevenzione, protezione e sicurezza nei luoghi di lavoro e servizi ausiliari ha rilevato, in base a quanto riportato nella

RDA, che il servizio non rientra nelle fattispecie di cui all'articolo 26 del decreto legislativo 81/08 e pertanto non è prevista la redazione del DUVRI;

- il parere 9 aprile 2025, con cui il responsabile della unità organizzativa Amministrazione digitale, avendo valutato che i corsi possono essere fruiti attraverso i comuni browser web, con connessione protetta SSL, e che sono già stati utilizzati, senza problematiche, dagli utenti del Consiglio regionale per le due precedenti annualità, non ha rilevato incompatibilità con l'infrastruttura sistemistica del Consiglio regionale;
- le dichiarazioni sull'insussistenza di situazioni, anche potenziali, di conflitto di interesse ai sensi dell'articolo 16 del Codice, dei soggetti interessati dalla procedura di affidamento (prot. CRL 2025.0005939, prot. CRL.2025.0005953, entrambe del 7 aprile 2025 e prot. CRL.2025.0006123 del 9 aprile 2024);

RITENUTO di acquisire il servizio in argomento ai sensi dell'articolo 50, comma 1, lett. b), mediante affidamento diretto, come da richiesta del dirigente della struttura proponente, tramite la piattaforma di negoziazione telematica di Regione Lombardia *Sintel*;

DATO ATTO che:

- in data 6 maggio 2025 la sottoscritta, in qualità di RUP, ai sensi dell'articolo 15 del Codice, ha approvato, mediante sottoscrizione digitale, il Foglio patti e condizioni;
- in data 14 maggio 2025 è stata avviata la procedura sulla piattaforma telematica di negoziazione Sintel - avente ID 201524867, con invito rivolto all'operatore economico Cyber Guru S.r.l., con sede a Roma;
- in data 27 maggio 2025, verificata la regolarità della documentazione e delle dichiarazioni rese dall'operatore economico, anche a seguito di integrazione documentale, la sottoscritta, in qualità di RUP, ha proposto di affidare il servizio oggetto della presente procedura a Cyber Guru S.r.l., alle condizioni di cui al Foglio patti e condizioni e relativi allegati, al prezzo unitario per singola utenza pari a euro 29,25 (oltre IVA), per il numero massimo di utenze richiedibili dall'Amministrazione pari a n. 300, per un importo massimo spendibile pari a euro 8.775,00 (oltre IVA);

CONSIDERATO che il Fornitore:

- ha dichiarato il possesso dei requisiti di carattere generale e speciale per la partecipazione alla procedura;
- è iscritto alla Camera di Commercio, Industria e Artigianato per un'attività pertinente con quella oggetto di affidamento;
- è in possesso di adeguate esperienze pregresse idonee allo svolgimento del servizio, tra cui quelle accuratamente eseguite in favore del Consiglio regionale;

RILEVATO che:

- il servizio è da considerarsi di natura intellettuale, per cui l'operatore economico non è tenuto a indicare i costi della manodopera e i costi della sicurezza afferenti alla propria attività di impresa;
- l'oggetto del servizio è necessario per il completamento del percorso formativo in materia di cybersicurezza già svolto nelle prime parti dal personale dell'Amministrazione come indicato dal dirigente responsabile nella richiesta di acquisizione ed è fornito in esclusiva dall'Affidatario e che pertanto sussistono le condizioni di cui all'art. 49, comma 4, del Codice;

RITENUTO, pertanto:

- di affidare il servizio in argomento a Cyber Guru S.r.l., con sede legale a Roma - codice fiscale e partita IVA 14324511006, alle condizioni e modalità del Foglio patti e condizioni e relativi allegati, al prezzo unitario per singola utenza pari a euro 29,25 (oltre IVA), per il numero massimo di utenze richiedibili dall'Amministrazione pari a n. 300, per un importo massimo spendibile pari a euro 8.775,00 (oltre IVA), per le motivazioni sopra;
- di impegnare per il servizio la spesa complessiva di euro 10.705,50 (IVA inclusa), sull'annualità 2025 del bilancio finanziario gestionale per gli anni 2025-2026-2027, con imputazione sul capitolo 10406 "Formazione", codifica di V livello del piano dei conti finanziario U.1.03.02.04.999 "Acquisto di servizi per altre spese per formazione e addestramento n.a.c.";

DATO ATTO che l'eventuale differenza tra l'impegno assunto sull'annualità 2025 e l'importo complessivo dei servizi relativi alle utenze che saranno richieste nel corso del medesimo anno sarà reimputata sull'esercizio finanziario successivo, fermo il termine finale del contratto;

DATO ATTO, altresì, che:

- il Fornitore procederà alla fatturazione dei corrispettivi contrattuali secondo le modalità riportate all'articolo 5, comma 6, del Foglio patti e condizioni, a norma del quale la fatturazione delle utenze, effettivamente attivate e accertate dal direttore dell'esecuzione del contratto, avverrà come segue:
  - a seguito dell'avvenuta attivazione o riattivazione, con esito positivo, delle credenziali per n. 251 utenze;
  - a seguito dell'avvenuta attivazione, con esito positivo, delle utenze richieste a consumo per un massimo di 49 utenze;
- il pagamento del corrispettivo contrattuale è soggetto alla tracciabilità dei flussi finanziari secondo quanto previsto dall'articolo 3 della Legge 136/2010;
- trattandosi di servizi di importo inferiore a euro 40.000,00, la verifica del possesso dei requisiti dichiarati in sede di presentazione dell'offerta avverrà con le modalità di cui all'articolo 52, comma 1, del Codice e del decreto dirigenziale 39/2024, sopra richiamato, e pertanto il presente provvedimento è immediatamente efficace;
- ai sensi dell'articolo 18, comma 1, secondo periodo, del Codice, trattandosi di affidamento ai sensi dell'articolo 50 del Codice stesso, il contratto sarà stipulato mediante corrispondenza secondo l'uso commerciale e che lo stesso, trattandosi di servizi di importo inferiore a euro 40.000,00, è esente da imposta di bollo;
- il contratto è sottoposto a clausola risolutiva in caso di successivo accertamento di insussistenza dei requisiti dichiarati, come previsto all'articolo 52, comma 2, del Codice, con l'adozione in tal caso dei provvedimenti e delle comunicazioni ivi previsti;

RITENUTO:

- di nominare Cyber Guru S.r.l. quale Responsabile del trattamento dei dati ai sensi dell'articolo 28 RGPD, in conformità al parere espresso dal dirigente dell'Ufficio Segreteria dell'Ufficio di presidenza, prevenzione della corruzione, trasparenza e privacy, e come da atto di designazione allegato al Foglio patti e condizioni, sottoscritto dall'operatore economico per accettazione in sede di procedura;
- di individuare, come indicato nella sopracitata RDA, il Direttore dell'Esecuzione del Contratto nel Dirigente dell'Ufficio Comunicazione interna e formazione, competente anche per l'eventuale modifica dell'impegno di spesa nonché per la liquidazione delle fatture;

VERIFICATA la regolarità dell'istruttoria e della proposta di decreto, sia dal punto di vista tecnico sia sotto il profilo della legittimità;

ATTESTATA la rispondenza del contenuto del presente atto al principio della competenza finanziaria potenziata di cui al d.lgs. 118/2011, stante l'imputazione della spesa negli esercizi finanziari nei quali si prevede che l'obbligazione giuridica venga a scadenza;

VISTO il rapporto del Servizio Programmazione finanziaria e risorse strumentali sulla disponibilità dei fondi e la prenotazione della spesa ai sensi dell'articolo 15 del regolamento contabile,

### **DECRETA**

1. di affidare il servizio in oggetto a Cyber Guru S.r.l., con sede legale a Roma - codice fiscale e partita IVA 14324511006, alle condizioni e modalità del Foglio patti e condizioni e relativi allegati, al prezzo unitario per singola utenza pari a euro 29,25 (oltre IVA), per il numero massimo di utenze richiedibili dall'Amministrazione pari a n. 300, per un importo massimo spendibile pari a euro 8.775,00 (oltre IVA), come da offerta economica del 23 maggio 2025 avente ID Sintel 1748015309866, presentata dalla società medesima;
2. di impegnare in favore di Cyber Guru S.r.l. la spesa complessiva di euro 10.705,50 (IVA inclusa), sull'annualità 2025 del bilancio finanziario gestionale per gli anni 2025-2026-2027, con imputazione sul capitolo 10406 "*Formazione*", codifica di V livello del piano dei conti finanziario U.1.03.02.04.999 "*Acquisto di servizi per altre spese per formazione e addestramento n.a.c.*";
3. di dare atto che l'eventuale differenza tra l'impegno assunto sull'annualità 2025 e l'importo complessivo dei servizi relativi alle utenze che saranno richieste nel corso del medesimo anno, sarà reimputata sull'esercizio finanziario successivo, fermo il termine finale del contratto;
4. di annettere al presente decreto, quale parte integrante, il Foglio Patti e Condizioni disciplinante il servizio in oggetto, approvato dalla sottoscritta in qualità di responsabile unico del progetto, mediante sottoscrizione digitale, e accettato dal Fornitore tramite sottoscrizione digitale in sede di procedura;
5. di individuare quale direttore dell'esecuzione del contratto competente anche per le attività di cui in premessa, il Dirigente dell'Ufficio Comunicazione interna e formazione;
6. di nominare Cyber Guru S.r.l. quale Responsabile del trattamento dei dati ai sensi dell'articolo 28 RGPD, come da atto di disciplina dei trattamenti già sottoscritto dall'operatore economico in sede di procedura;
7. di stipulare il contratto, ai sensi dell'articolo 18, comma 1, del Codice, mediante corrispondenza secondo l'uso commerciale, previa acquisizione della garanzia definitiva di cui all'articolo 12 del Foglio patti e condizioni, stante l'immediata efficacia del presente decreto di affidamento;

8. di sottoporre il contratto alla condizione risolutiva del successivo accertamento negativo dei controlli sul possesso dei requisiti dichiarati, ferme le ulteriori conseguenze ai sensi dell'articolo 52, comma 2, del Codice.

**MARA GARGATAGLI**

Documento sottoscritto digitalmente, ai sensi dell'articolo 24  
del d.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale)

Foglio Patti e Condizioni

Acquisizione del percorso di formazione online sulla sicurezza informatica, terza annualità, destinato ai dipendenti del Consiglio regionale della Lombardia tramite accesso alla piattaforma di e-learning “Cyber Guru Awareness” di proprietà di Cyber Guru S.r.l.

**INDICE**

|                                                                                                                                                  |    |
|--------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Art. 1 - Definizione delle parti                                                                                                                 | 2  |
| Art. 2 - Oggetto, finalità, durata del contratto e opzioni contrattuali                                                                          | 2  |
| Art. 3 - Responsabile unico del progetto e Direttore dell’esecuzione del contratto                                                               | 2  |
| Art. 4 - Descrizione delle attività e delle tempistiche di esecuzione del servizio                                                               | 3  |
| Art. 5 - Corrispettivi, periodicità di fatturazione, contenuti della fatturazione elettronica e modalità di pagamento                            | 5  |
| Art. 6 - Revisione prezzi                                                                                                                        | 6  |
| Art. 7 - Penali                                                                                                                                  | 7  |
| Art. 8 - Clausola risolutiva ai sensi dell’articolo 1456 del Codice civile                                                                       | 8  |
| Art. 9 - Risoluzione ai sensi dell’articolo 122 d.lgs. 36/2023                                                                                   | 9  |
| Art. 10 - Recesso ai sensi dell’articolo 123 del d.lgs. 36/2023                                                                                  | 9  |
| Art. 11 - Tracciabilità dei flussi finanziari                                                                                                    | 9  |
| Art. 12 - Garanzia definitiva                                                                                                                    | 10 |
| Art. 13 - Divieto di cessione del contratto e subappalto                                                                                         | 11 |
| Art. 14 - Trattamento dei dati personali e designazione del Fornitore quale responsabile del trattamento                                         | 11 |
| Art. 15 - Patto di riservatezza                                                                                                                  | 14 |
| Art. 16 - Rispetto del codice di comportamento dei dipendenti pubblici e del personale del Consiglio regionale della Lombardia                   | 14 |
| Art. 17 - Divieto di “ <i>pantouflage</i> ” e relative sanzioni                                                                                  | 15 |
| Art. 18 - Segnalazione di violazioni nell’Amministrazione (c.d. whistleblowing) da parte dei lavoratori e collaboratori delle imprese fornitrici | 15 |
| Art. 19 - Stipulazione del contratto                                                                                                             | 16 |
| Art. 20 - Risoluzione delle controversie e Foro competente                                                                                       | 16 |

|                                                                                                                                                                           |    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Art. 21 - Indirizzo di posta elettronica certificata del Consiglio regionale                                                                                              | 16 |
| Art. 22 - Norma finale                                                                                                                                                    | 16 |
| Clausole del Foglio Patti e condizioni di cui all'art. 1341 c.c.                                                                                                          | 17 |
| Allegato D – Designazione del responsabile del trattamento dei dati personali                                                                                             | 18 |
| PREMESSA                                                                                                                                                                  | 19 |
| DURATA                                                                                                                                                                    | 20 |
| OBBLIGHI DEL TITOLARE DEL TRATTAMENTO                                                                                                                                     | 20 |
| OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO                                                                                                                                 | 21 |
| ATTIVITÀ DI VIGILANZA E VERIFICA DEL TRATTAMENTO                                                                                                                          | 34 |
| INDIVIDUAZIONE DI MAGGIORI LIVELLI DI SICUREZZA E ADEGUAMENTI ALLA NORMATIVA<br>PRIVACY SOPRAVVENUTA O A ESIGENZE CONTRATTUALI SOPRAVVENUTE                               | 35 |
| COMUNICAZIONI                                                                                                                                                             | 35 |
| DISPOSIZIONI FINALI                                                                                                                                                       | 36 |
| DATI DI CONTATTO DEI RESPONSABILI DELLA PROTEZIONE DEI DATI PERSONALI (RPD)                                                                                               | 36 |
| ALLEGATI                                                                                                                                                                  | 36 |
| <b>ALLEGATO A.1 - ELENCO DEI TRATTAMENTI DI DATI PERSONALI DI TITOLARITÀ DEL CONSIGLIO<br/>REGIONALE AFFIDATI AL FORNITORE IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO</b> | 37 |
| <b>ALLEGATO A.2 - ELENCO DELLE MISURE DI SICUREZZA</b>                                                                                                                    | 42 |

### **Art. 1 - Definizione delle parti**

1. Amministrazione Appaltante, nel prosieguo denominata anche 'Amministrazione' o 'Consiglio regionale' è il Consiglio regionale della Lombardia, codice fiscale 80053570158 e P. IVA 09201010965, con sede in via Fabio Filzi n. 22, CAP 20124, a Milano.
2. Fornitore, nel prosieguo denominato anche 'Affidatario', è l'operatore economico Cyber Guru S.r.l., codice fiscale e P.IVA 14324511006, con sede in Viale Della Grande Muraglia n. 284, C.A.P. 00144 - Roma.

### **Art. 2 - Oggetto, finalità, durata del contratto e opzioni contrattuali**

1. Il contratto ha per oggetto l'erogazione, della terza annualità, di un percorso di formazione online sulla sicurezza informatica, destinato ai dipendenti del Consiglio regionale, con fornitura di credenziali per l'accesso alla piattaforma di e-learning "Cyber Guru Awareness", di proprietà della società Cyber Guru S.r.l., per un numero minimo di 251 utenze e fino a un massimo di 300.
2. Il contratto ha una durata di 13 mesi, comprensivi delle tempistiche di attivazione, decorrenti dalla data indicata nella comunicazione di stipulazione del contratto. I dodici moduli formativi sono attivati nel corso della durata del contratto.
3. Nell'ipotesi in cui, alla scadenza del termine finale del contratto non sia esaurito l'importo massimo stabilito di cui all'articolo 5, tale termine potrà essere differito mediante decreto, a parità di corrispettivi e di massimale contrattuale, previa comunicazione scritta, da inviare al Fornitore tramite posta elettronica certificata con quindici giorni di anticipo rispetto alla scadenza.
4. Il Consiglio regionale, qualora in corso di esecuzione si renda necessario un aumento o una diminuzione delle prestazioni fino a concorrenza del quinto dell'importo del contratto, può imporne al Fornitore l'esecuzione, alle stesse condizioni previste nel contratto originario. In tal caso, il Fornitore non può far valere il diritto alla risoluzione del contratto.

### **Art. 3 - Responsabile unico del progetto e Direttore dell'esecuzione del contratto**

1. Ai sensi dell'articolo 15 e dell'articolo 2 dell'Allegato I.2 del d.lgs. 31 marzo 2023, n. 36 (di seguito, anche, Codice), il Consiglio regionale individua quale Responsabile Unico del progetto (RUP) il dirigente dell'Ufficio contratti e ICT.
2. Il Consiglio regionale individua quale Direttore dell'esecuzione del contratto (di seguito DEC) il Dirigente dell'Ufficio Comunicazione interna e formazione.
3. Fermo restando il rispetto delle disposizioni di servizio eventualmente impartite dal RUP, il DEC opera in autonomia in ordine al coordinamento, alla direzione e al controllo tecnico-contabile nell'esclusivo interesse all'efficiente e sollecita esecuzione del contratto.
4. Il DEC è competente altresì per l'eventuale modifica dell'impegno di spesa, per la liquidazione delle fatture e per il rilascio del certificato di regolare esecuzione.
5. È facoltà del DEC individuare uno o più referenti con funzioni operative, dandone comunicazione al Fornitore.

6. L'eventuale variazione del DEC è tempestivamente comunicata dal Consiglio regionale al Fornitore.
7. Le comunicazioni tra il DEC e il Fornitore avvengono per iscritto tramite posta elettronica istituzionale o posta elettronica certificata in modo da garantire la verifica dell'avvenuto recapito delle stesse, al seguente indirizzo:  

[protocollo.generale@pec.consiglio.regione.lombardia.it](mailto:protocollo.generale@pec.consiglio.regione.lombardia.it)
8. Il Consiglio regionale procederà, per il tramite del DEC, all'accertamento della conformità del servizio rispetto alle prescrizioni contrattuali.
9. L'eventuale variazione dei ruoli organizzativi è tempestivamente comunicata dal Consiglio regionale al Fornitore tramite PEC.

#### **Art. 4 - Descrizione delle attività e delle tempistiche di esecuzione del servizio**

1. Il servizio di cui all'articolo 2, comma 1, comprende:
  - a. la fruizione della terza parte del percorso di formazione, in modalità e-learning, sulla sicurezza informatica, suddiviso in 12 moduli (dal modulo n. 25 al modulo n. 36), secondo quanto previsto, al comma 8 del presente articolo, per i dipendenti che hanno già effettuato tutti i precedenti moduli dal n. 1 al n. 24;
  - b. l'erogazione dei seguenti moduli formativi concordati con l'amministrazione da far seguire ai dipendenti non presenti in Consiglio negli anni in cui erano state erogati la prima e la seconda annualità di corso o che, comunque, non abbiano seguito le annualità precedenti, indicativamente come segue:
    - dal modulo n. 1 al modulo n. 12, per i nuovi dipendenti;
    - dal modulo n. 13 al modulo n. 24, per i dipendenti che hanno già effettuato i moduli relativi alla prima annualità.
2. Ogni modulo ha una durata media di 15/20 minuti. I suddetti moduli sono erogati con cadenza mensile e caricati dal Fornitore sulla propria piattaforma entro la prima settimana di ogni mese, per una durata del percorso pari a n. 12 mesi.
3. Al termine del percorso formativo, ogni dipendente del Consiglio avrà concluso almeno una annualità, pari a 12 moduli.
4. Il Fornitore garantisce inoltre:
  - a. la fruizione illimitata del percorso, regolata secondo le scadenze di trasmissione di ogni segmento dello stesso, fino ad un massimo di 300 utenze, di cui n. 251 garantite;
  - b. il test finale previsto al termine di ciascuna sessione del corso, per ciascun utente;
  - c. l'attestato di partecipazione per ciascun utente, prodotto al termine del percorso nella sua interezza, scaricabile da ciascun utente.
5. La fruizione del corso avviene in modalità e-learning tramite l'utilizzo della piattaforma attiva 24 ore su 24. Il Fornitore deve garantire il servizio adeguandosi alla configurazione di lavoro del Consiglio regionale della Lombardia. Lo svolgimento di ogni sessione di corsi in modalità web e

tramite l'accesso al portale deve essere agevole, continuativa e senza ingiustificate interruzioni o sospensioni del servizio.

6. L'utilizzo della piattaforma del corso e-learning 24 ore su 24 deve essere resa possibile per la durata di un anno dal momento dell'attivazione del servizio. L'accesso alla piattaforma avviene tramite un nome utente (indirizzo e-mail del dipendente, fornito dall'Amministrazione) e una password creata dall'utente al primo accesso.
7. Le date e i tempi di attivazione e riattivazione delle credenziali devono essere concordate con il Fornitore e formalizzate a mezzo posta elettronica certificata dal Direttore dell'esecuzione del contratto. È comunque assicurata da parte del Fornitore la possibilità di attivare in qualsiasi momento ulteriori utenze sino ad un massimo di 300, entro il periodo di validità del contratto. Le date di attivazione sono comunicate al Fornitore, mediante posta elettronica certificata, dal Direttore dell'esecuzione del contratto unitamente ai nominativi dei dipendenti da attivare. Il Fornitore trasmette via e-mail, entro sette giorni precedenti la data fissata per ciascun corso, le credenziali di autenticazione per l'accesso alla piattaforma web che rimarranno sempre valide anche per l'accesso ai successivi moduli.
8. La periodicità dell'erogazione del corso sarà mensile, suddiviso in 12 moduli della durata di 12 mesi, come previsto dal comma 2. Una volta fissata la data di attivazione del corso, il calendario della piattaforma Cyber GURU, programma di conseguenza il calendario dei successivi moduli. A fronte di specifiche esigenze organizzative e con un preavviso di almeno cinque giorni lavorativi, il Direttore dell'esecuzione ha facoltà di richiedere delle variazioni alla programmazione stabilita di cui al comma precedente.
9. Al termine del percorso formativo la piattaforma deve rilasciare ai partecipanti gli attestati di partecipazione, di cui al comma 4, lettera c), e il relativo materiale didattico, in formato elettronico.
10. L'intero percorso formativo deve essere tracciato, in termini di argomenti trattati e di effettiva presenza dei dipendenti, attraverso una registrazione online, definita congiuntamente al Direttore dell'esecuzione e inviata al termine delle sessioni di formazione svolte.
11. Al raggiungimento dell'attivazione di n. 251 utenze, è compreso nel corrispettivo:
  - a. un servizio di CSM (Customer Success Management) volto a supportare l'Amministrazione nella corretta implementazione del servizio di training, sia nella fase di avviamento del piano formativo (on boarding degli utenti, supporto alla suddivisione in team, ausilio alla comunicazione agli utenti, scelta dei template per phishing mail, analisi primi risultati, etc.), sia nel corso dell'esecuzione dello stesso, attraverso riunioni mensili in videoconferenza con uno specialista.
  - b. un pacchetto composto da n. 16 ore di servizio di un team di supporto per le attività di set-up iniziale della piattaforma, per la fase di rendicontazione complessiva dei percorsi, per l'eventuale download massivo degli attestati e per l'invio ai referenti dell'Ufficio Comunicazione interna e formazione. Le attività e le ore di servizio effettuate dal team di

supporto devono essere trasmesse e rendicontate dal Direttore dell'esecuzione del contratto.

**Art. 5 - Corrispettivi, periodicità di fatturazione, contenuti della fatturazione elettronica e modalità di pagamento**

1. Al fornitore è riconosciuto il corrispettivo offerto in sede di procedura, formulato sulla base dell'importo stimato massimo stimato dall'amministrazione e indicato nella richiesta di preventivo. Il corrispettivo contrattuale è determinato dal costo unitario di ogni utenza offerto dal fornitore moltiplicato per il numero massimo di utenze richiedibili (n. 300).
2. Il corrispettivo è erogato in base alle utenze effettivamente richieste e rendicontate dal DEC. Sono garantite n. 251 utenze minime. Il Fornitore non può pertanto vantare l'erogazione dell'intero corrispettivo contrattuale.
3. Il valore contrattuale è pari al corrispettivo unitario di aggiudicazione moltiplicato per il numero di utenze regolarmente attivate.
4. Gli oneri per la sicurezza per rischi da interferenza sono pari a zero euro.
5. I corrispettivi si riferiscono al servizio oggetto dell'affidamento eseguito a perfetta regola d'arte e nel pieno adempimento delle modalità e delle prescrizioni contrattuali e includono tutti gli oneri derivanti al Fornitore dall'esecuzione del contratto e dall'osservanza di leggi e regolamenti. È escluso il rimborso di eventuali spese sostenute dal Fornitore a qualsiasi titolo.
6. Il Fornitore procede alla fatturazione delle utenze, effettivamente attivate e accertate dal direttore dell'esecuzione del contratto, come segue:
  - a seguito dell'avvenuta attivazione o riattivazione, con esito positivo, delle credenziali per n. 251 utenze;
  - a seguito dell'avvenuta attivazione, con esito positivo, delle utenze richieste a consumo per un massimo di 49 utenze.
7. L'Amministrazione provvede al pagamento del corrispettivo, previa verifica da parte del DEC della regolarità della fatturazione, entro trenta (30) giorni dal ricevimento di regolare fattura in favore del conto corrente indicato dal Fornitore nel modulo di cui all'articolo 11.
8. La fattura deve essere emessa secondo le prescrizioni del decreto del Ministro dell'economia e delle finanze del 23 gennaio 2015 "Modalità e termini per il versamento dell'imposta sul valore aggiunto da parte delle pubbliche amministrazioni", e deve riportare obbligatoriamente i seguenti dati:
  - Intestazione: **Consiglio regionale della Lombardia;**
  - Sede: via Fabio Filzi, 22 – Milano (MI);
  - Codice Univoco Ufficio di IPA (campo 1.1.4): **UFIRHM;**
  - Codice fiscale del Consiglio regionale (campo 1.4.1.2): **80053570158;**
  - Repertorio contratto (campo 2.1.3.2): **2023.XII.4.1.2.24;**
  - CIG contratto (campo 2.1.2.7), **comunicato in seguito all'affidamento;**
  - Esigibilità IVA (campo 2.2.2.7): **S "Scissione dei pagamenti"**.

9. Nel caso in cui la fattura sia priva dei dati richiesti al comma precedente, l'Amministrazione non procede con la liquidazione e chiede al Fornitore l'emissione di una nota di credito a completo storno della fattura irregolare e la contestuale emissione di una fattura contenente i dati richiesti.
10. Eventuali contestazioni o irregolarità di fatturazione, anche diverse da quelle richiamate al comma precedente, sospendono comunque il termine di pagamento, con facoltà per l'Amministrazione di procedere ai sensi del medesimo comma.
11. Ai sensi dell'articolo 31 del decreto-legge 21 giugno 2013, n. 69, convertito con modificazioni dalla legge 9 agosto 2013, n. 98, al fine di procedere al pagamento delle prestazioni contrattuali, il Consiglio regionale acquisisce d'ufficio il Documento Unico di Regolarità Contributiva (di seguito DURC).
12. In caso di inadempienza contributiva risultante dal DURC e di ritardato pagamento delle retribuzioni dovute al personale impiegato nell'esecuzione dell'appalto, si procederà ai sensi dell'articolo 11, comma 6, del Codice.
13. In ogni caso, sull'importo netto progressivo delle prestazioni contrattuali è operata una ritenuta dello 0,50 per cento. Le ritenute possono essere svincolate soltanto in sede di liquidazione del saldo finale, dopo la verifica della regolare esecuzione del contratto, previo rilascio del DURC. L'IVA esposta nella fattura deve comunque essere calcolata sul corrispettivo pieno.
14. Il Consiglio regionale, prima di effettuare il pagamento, procede inoltre alla verifica prevista dall'articolo 48-bis del D.P.R. 29 settembre 1973, n. 602, così come modificata dall'articolo 1, commi 986 e 987, lettere a) e b), della legge 27 dicembre 2017, n. 205, secondo le modalità stabilite dal D.M. 18/01/2008, n. 40.

#### **Art. 6 - Revisione prezzi**

1. Ai sensi degli articoli 9 e 60 del Codice, qualora nel corso di esecuzione del contratto si verificino particolari condizioni di natura oggettiva, che determinano una variazione, in aumento o in diminuzione, del costo del servizio superiore al cinque per cento dell'importo complessivo, i prezzi sono aggiornati, nella misura dell'ottanta per cento della variazione stessa, in relazione alle prestazioni da eseguire.
2. Ai fini della determinazione della variazione dei prezzi l'Amministrazione, ai sensi dall'Allegato II.2 bis al Codice, utilizzerà l'indice dei prezzi al consumo, nel caso specifico l'indice ISTAT 105 "Corsi d'istruzione e di formazione", corrispondente ai CPV 80500000-9 "Servizi di formazione", pubblicati, unitamente alla relativa metodologia di calcolo, sul portale istituzionale dell'ISTAT in conformità alle pertinenti disposizioni normative europee e nazionali in materia di comunicazione e diffusione dell'informazione statistica ufficiale.
3. I nuovi prezzi determinati a seguito della revisione sono applicati alle prestazioni contrattuali svolte dopo la revisione a partire dalla prima fatturazione utile. In nessun caso la revisione dei prezzi potrà avere effetto sulle prestazioni già eseguite.

## **Art. 7 - Penali**

1. Il DEC ha facoltà di contestare le prestazioni contrattuali, entro il termine di quindici (15) giorni, qualora a seguito di controlli ravvisi inadempienze, difformità e ritardo negli adempimenti rispetto alle attività e alle modalità di esecuzione indicate all'articolo 4. La contestazione viene formulata al Fornitore dal DEC per il tramite di PEC. Il Fornitore ha facoltà di formulare controdeduzioni, per il tramite di PEC, entro il termine perentorio di cinque (5) giorni dal ricevimento della formale contestazione.
2. Il DEC, valutate le ragioni addotte dal Fornitore, può procedere all'applicazione delle seguenti penali:
  - a) attivazione del servizio: qualora non venga rispettato l'orario e il calendario concordato con il Direttore dell'esecuzione del contratto, ai sensi dell'articolo 4, comma 7: l'1,5 per mille dell'importo netto contrattuale, per ogni giorno di ritardo;
  - b) contenuti e argomenti trattati: in caso di inosservanze accertate e difformità rispetto a quanto concordato ai sensi dell'articolo 4, commi 7 e 8: euro 20,00 per ogni inosservanza e difformità accertata;
  - c) utilizzo piattaforma: nel caso in cui non sia garantito l'utilizzo come previsto dall'articolo 4, comma 5: euro 30,00 per ogni caso di impossibilità di utilizzo;
  - d) materiale didattico e attestati: in caso di mancato rilascio, inosservanze accertate e difformità nella distribuzione del materiale e nel rilascio degli attestati, di cui all'articolo 4, comma 9: euro 20,00 per ogni inosservanza e difformità accertata;
  - e) ingiustificata sospensione del servizio: euro 50,00 per ogni episodio accertato;
  - f) mancata esecuzione delle attività o violazioni non gravi degli obblighi di cui agli articoli 14 e 15 e di cui all'atto di designazione del responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679 (Allegato D): euro 100,00 per ogni violazione.
3. Le fattispecie riportate al comma 2 non hanno carattere di tassatività. In caso di disservizio, ritardo o inadempimento diverso da quelli contemplati al comma 2, il DEC può irrogare al Fornitore, in relazione alla gravità del fatto, una penale compresa tra lo 0,5 per mille e l'1,5 per mille dell'importo contrattuale netto.
4. Le penali espresse in percentuale sono arrotondate alla seconda cifra decimale per eccesso.
5. Le penali per il ritardo non possono comunque superare, complessivamente, il 10 per cento dell'importo netto contrattuale.
6. In caso di applicazione di penali, è fatto salvo il risarcimento dell'eventuale maggior danno subito dal Consiglio regionale ai sensi dell'articolo 1382 del Codice civile.
7. Per la riscossione delle penali e la rifusione degli eventuali ulteriori danni il Consiglio regionale potrà rivalersi anche tramite trattenuta, per compensazione, sui crediti vantati dal Fornitore nei confronti del Consiglio regionale, nonché sulla garanzia definitiva prestata che, in tal caso, dovrà essere reintegrata secondo quanto previsto all'articolo 12.
8. La richiesta o il pagamento delle penali di cui al presente articolo non esonera in nessun caso il Fornitore dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto

sorgere la penale. In caso di mancata esecuzione delle attività o di esecuzione gravemente imperfetta non è dovuto alcun corrispettivo.

9. Fatta salva l'applicazione delle penali, nei casi in cui il Fornitore ometta di eseguire, anche parzialmente, la prestazione oggetto del contratto con le modalità ed entro i termini previsti, il Consiglio regionale si riserva la facoltà di ordinare ad altro soggetto l'esecuzione parziale o totale di quanto omesso dal Fornitore, cui saranno addebitati i relativi costi e i danni eventualmente derivati al Consiglio regionale, dandone comunicazione al Fornitore via PEC, con un preavviso di sette giorni di calendario.
10. Qualora l'inesatto adempimento o il ritardo siano determinati da cause di forza maggiore, il Fornitore dovrà notificare immediatamente tale circostanza alla competente struttura tramite PEC, fornendo le necessarie motivazioni a comprova.
11. In caso di applicazione delle penali, l'Amministrazione provvederà a darne comunicazione all'ANAC, in osservanza della normativa vigente in materia.

#### **Art. 8 - Clausola risolutiva ai sensi dell'articolo 1456 del Codice civile**

1. Fatta salva l'applicazione delle penali di cui all'articolo 7, il Consiglio regionale ha facoltà, previa comunicazione scritta da inviare al Fornitore a mezzo PEC con cui dichiara che intende avvalersi della presente clausola, di risolvere il contratto ai sensi dell'articolo 1456 del Codice civile, con incameramento della garanzia al verificarsi delle seguenti ipotesi:
  - a) in caso di applicazione di penali per un ammontare totale almeno pari al dieci per cento del corrispettivo contrattuale netto, comprensivo dell'eventuale corrispettivo del periodo di proroga qualora esercitata tale facoltà;
  - b) in caso di violazione degli obblighi di tracciabilità finanziaria richiamati all'articolo 11;
  - c) in caso di mancata completa reintegrazione della garanzia definitiva di cui all'articolo 12, eventualmente escussa, entro il termine di dieci giorni naturali e consecutivi dal ricevimento della relativa richiesta tramite PEC da parte del Consiglio regionale;
  - d) in caso di violazione del divieto di cessione del contratto di cui all'articolo 13;
  - e) in caso di gravi violazioni delle norme in materia di protezione dei dati personali e degli obblighi assunti in qualità di responsabile del trattamento e delle norme relative al patto di riservatezza di cui rispettivamente agli articoli 14 e 15;
  - f) in caso di violazione dei codici di condotta di cui all'articolo 16;
  - g) in caso di mancato rispetto della normativa vigente in materia di lavoro, d'infortuni sul lavoro, d'igiene, di previdenza sociale e di tutti gli obblighi previsti dal d.lgs. 9 aprile 2008, n. 81, oppure inosservanza degli obblighi previsti dai contratti collettivi di categoria, nazionali e regionali, anche dopo la loro scadenza fino alla loro sostituzione;
  - h) in caso di verifiche con esito negativo in merito al possesso dei requisiti generali e speciali di partecipazione dichiarati in sede di procedura, fatte salve le ulteriori conseguenze previste ai sensi dell'articolo 52, comma 2, del Codice.

2. L'Amministrazione può dichiarare risolto il contratto a proprio insindacabile giudizio e potrà provvedere a stipulare un nuovo contratto, addebitando le maggiori spese che dovessero derivare da prezzi meno favorevoli per l'Amministrazione stessa e fatto salvo il risarcimento del maggior danno.

**Art. 9 - Risoluzione ai sensi dell'articolo 122 d.lgs. 36/2023**

1. L'Amministrazione può risolvere il contratto di appalto ai sensi dell'articolo 122 del Codice.
2. In tutti i casi di risoluzione del contratto il Fornitore ha diritto soltanto al pagamento delle prestazioni relative al servizio regolarmente eseguito, decurtato degli oneri aggiuntivi derivanti dallo scioglimento del contratto, fatto salvo quanto previsto al comma 6 del medesimo articolo.

**Art. 10 - Recesso ai sensi dell'articolo 123 del d.lgs. 36/2023**

1. L'Amministrazione può recedere dal contratto in qualunque momento ai sensi dell'articolo 123 del Codice. All'Affidatario è riconosciuta un'indennità, pari al decimo dei servizi non eseguiti, calcolata sulla differenza tra l'importo dei quattro quinti del prezzo posto a base dell'affidamento, depurato del ribasso d'asta, e l'ammontare netto dei servizi eseguiti, secondo quanto previsto all'articolo 11 dell'allegato II.14, del Codice.
2. L'esercizio del diritto di recesso è manifestato dall'Amministrazione appaltante mediante una formale comunicazione all'Affidatario da darsi per iscritto con un preavviso non inferiore a venti giorni, decorsi i quali il Consiglio regionale prende in consegna i servizi ed effettua la verifica della regolare esecuzione degli stessi.

**Art. 11 - Tracciabilità dei flussi finanziari**

1. Il Fornitore assume tutti gli obblighi di tracciabilità finanziaria di cui all'articolo 3 della legge 13 agosto 2010, n. 136, così come interpretato e modificato dagli articoli 6 e 7 del decreto-legge 12 novembre 2010, n. 187, convertito dalla legge 17 dicembre 2010 n. 217. A tal fine, il Fornitore sottoscrive, su richiesta del Consiglio regionale, la dichiarazione di tracciabilità dei flussi finanziari, contenente tra l'altro gli estremi del conto corrente dedicato ai pagamenti relativi al presente contratto e la aggiorna tempestivamente in caso di modifica dei dati ivi dichiarati.
2. Il Fornitore si impegna a notificare tempestivamente eventuali variazioni che si verificassero nelle modalità di pagamento e, in difetto di tale notificazione, esonera il Consiglio regionale da ogni responsabilità per i pagamenti eseguiti.
3. I subappaltatori e i subcontraenti, a qualunque titolo coinvolti nella esecuzione del contratto, sono tenuti, unitamente al Fornitore, al rispetto della normativa sulla tracciabilità dei flussi finanziari (articolo 3, comma 1, legge 136/2010).
4. Ai sensi dell'articolo 119, comma 2, ultimo periodo, del d.lgs. 36/2023, "L'affidatario comunica alla stazione appaltante, prima dell'inizio della prestazione, per tutti i sub-contratti che non sono subappalti, stipulati per l'esecuzione dell'appalto, il nome del sub-contraente, l'importo del subcontratto, l'oggetto del lavoro, servizio o fornitura affidati. Sono, altresì, comunicate alla stazione appaltante eventuali modifiche a tali informazioni avvenute nel corso del sub-

contratto. È altresì fatto obbligo di acquisire autorizzazione integrativa qualora l'oggetto del subappalto subisca variazioni e l'importo dello stesso sia incrementato".

5. Come previsto all'articolo 3, comma 1, della legge n. 136/2010 "La stazione appaltante verifica che nei contratti sottoscritti con i subappaltatori e i subcontraenti della filiera delle imprese a qualsiasi titolo interessate ai lavori, ai servizi e alle forniture di cui al comma 1 sia inserita, a pena di nullità assoluta, un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla presente legge".
6. L'appaltatore, il subappaltatore o il subcontraente che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria è tenuto a darne immediata comunicazione alla stazione appaltante e alla prefettura - ufficio territoriale del Governo della provincia di Milano.

## **Art. 12 - Garanzia definitiva**

1. Ai sensi dell'articolo 53, comma 4, del Codice, il Fornitore per la sottoscrizione del contratto deve costituire una garanzia definitiva a sua scelta sotto forma di cauzione o fideiussione, pari al 5% dell'importo contrattuale netto, non si applicano le riduzioni di cui all'articolo 106, comma 8, del Codice e gli aumenti previsti dall'articolo 117, comma 2.
2. La cauzione è costituita con versamento della somma garantita presso l'istituto incaricato del servizio di tesoreria, a titolo di pegno a favore dell'amministrazione, esclusivamente tramite il sistema Pago PA.
3. La garanzia fideiussoria può essere rilasciata da imprese bancarie o assicurative che rispondano ai requisiti di solvibilità previsti dalle leggi che ne disciplinano le rispettive attività ovvero dagli intermediari finanziari iscritti nell'albo di cui all'articolo 106 del d.lgs. 1 settembre 1993, n. 385, che svolgono in via esclusiva o prevalente attività di rilascio di garanzie e che sono sottoposti a revisione contabile da parte di una società di revisione iscritta nell'apposito albo e che abbiano i requisiti minimi di solvibilità richiesti dalla vigente normativa bancaria assicurativa. La garanzia fideiussoria deve essere emessa e firmata digitalmente; essa deve essere altresì verificabile telematicamente presso L'emittente ovvero gestita in tutte le fasi mediante ricorso a piattaforme operanti con tecnologie basate su registri distribuiti ai sensi dell'articolo 8-ter, comma 1, del decreto-legge 14 dicembre 2018, n. 135, convertito, con modificazioni, dalla legge 11 febbraio 2019, n. 12, o su registri elettronici qualificati ai sensi del Regolamento (UE) n. 910/2014. Le piattaforme, operanti con tecnologie basate su registri distribuiti o su registri elettronici, sono conformi alle caratteristiche stabilite dall'AGID con il provvedimento di cui all'articolo 26, comma 1.
4. Il beneficiario della polizza fideiussoria è il Consiglio regionale della Lombardia.
5. La cauzione (o fideiussione) è prestata a garanzia dell'adempimento di tutte le obbligazioni del contratto e del risarcimento dei danni derivanti dall'eventuale inadempimento delle obbligazioni stesse, salva comunque la risarcibilità del maggior danno.
6. Il Consiglio regionale ha il diritto di valersi della garanzia, nei limiti dell'importo massimo garantito, per l'eventuale maggiore spesa sostenuta per il completamento del servizio nel caso

di risoluzione del contratto disposta in danno dell'esecutore e ha il diritto di valersi della cauzione per provvedere al pagamento di quanto dovuto dall'esecutore per le inadempienze derivanti dalla inosservanza di norme e prescrizioni dei contratti collettivi, delle leggi e dei regolamenti sulla tutela, protezione, assicurazione, assistenza e sicurezza fisica dei lavoratori comunque presenti nei luoghi dove viene prestata il servizio.

7. La garanzia cessa di avere effetto solo alla data di emissione del certificato di regolare esecuzione. Il Consiglio regionale può richiedere al soggetto affidatario la reintegrazione della garanzia ove questa sia venuta meno in tutto o in parte. Diversamente, il Consiglio regionale si riserva la facoltà di avvalersi della clausola di cui all'articolo 9 comma 1, lettera c).
8. Ai sensi di legge la garanzia è svincolata dopo l'accertamento, da parte del DEC, della completa ottemperanza alle clausole contrattuali.
9. Alla garanzia di cui al presente articolo si applicano le disposizioni in materia di garanzia provvisoria dell'articolo 106 del Codice, ove richiamate dall'articolo 117 del medesimo Codice, salvo quanto previsto al comma 1.

#### **Art. 13 - Divieto di cessione del contratto e subappalto**

1. La cessione del contratto è nulla, fatte salve le ipotesi previste dall'articolo 120, comma 1, lett. d) del Codice.
2. Il ricorso al subappalto è ammesso nei limiti e con le modalità di cui all'articolo 119 del Codice. Non può essere affidata in subappalto la prevalente esecuzione delle prestazioni oggetto del contratto. Il subappalto è autorizzato dall'Amministrazione qualora ricorrano le condizioni di cui al comma 4 del suindicato articolo.
3. Ai sensi dell'articolo 119, comma 3, qualora il Fornitore affidi a terze parti prestazioni secondarie, accessorie o sussidiarie in forza di contratti continuativi di cooperazione, servizio o fornitura sottoscritti in epoca anteriore alla indizione della procedura finalizzata all'affidamento del presente servizio è tenuto a trasmettere i relativi contratti al Consiglio regionale prima o contestualmente alla sottoscrizione del contratto di appalto.
4. Nei contratti di subappalto o nei subcontratti comunicati alla stazione appaltante è obbligatorio l'inserimento di clausole di revisione prezzi riferite alle prestazioni o lavorazioni oggetto del subappalto o del subcontratto e determinate incoerenza con quanto previsto degli articoli 8 e 14 dell'allegato II.2-bis, del Codice, che si attivano al verificarsi delle particolari condizioni di natura oggettiva di cui all'articolo 60, comma 2, dello stesso Codice.

#### **Art. 14 - Trattamento dei dati personali e designazione del Fornitore quale responsabile del trattamento**

1. Ai fini del presente capitolato e dei suoi allegati, s'intende per "Normativa privacy", il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito, "RGPD"), il d.lgs. 30 giugno 2003, n. 196, recante

“Codice in materia di protezione dei dati personali recante disposizioni per l’adeguamento dell’ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE” (di seguito “Codice privacy”), nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile in Italia, ivi compresi i provvedimenti dell’Autorità Garante per la Protezione dei dati personali.

2. Le prestazioni contrattuali comportano l’affidamento al Fornitore di attività di trattamento, con l’ausilio di strumenti elettronici, di dati personali di cui è titolare il Consiglio regionale. Ai sensi dell’art. 28 RGPD, il Fornitore, nella persona del legale rappresentante pro tempore, in qualità di aggiudicatario, assume la qualifica di Responsabile del trattamento dei dati personali trattati, per conto del Consiglio regionale (Titolare del trattamento), nell’ambito dell’esecuzione delle prestazioni di cui al presente capitolato ed è tenuto alla piena e diligente esecuzione dei compiti indicati nell’allegato D, che costituisce parte integrante e sostanziale del Foglio patti e condizioni stesso.
3. Il Fornitore tratta esclusivamente i dati personali necessari per lo svolgimento delle operazioni elettroniche funzionali a garantire l’accesso alla piattaforma web utilizzata per l’erogazione del servizio, attivazione, mantenimento, aggiornamento e gestione della stessa, assistenza e supporto tecnico, formazione degli utenti, garantendo la funzionalità e la sicurezza degli applicativi e dei dati ivi presenti, nonché la conformità alla normativa sui cookies e alla Normativa privacy. In ogni caso, tutti i dati personali possono essere trattati dal Fornitore nell’ambito e solo nei limiti in cui sia indispensabile per effettuare le prestazioni contrattuali, garantendo la tutela della riservatezza, l’integrità e la disponibilità dei dati.
4. Il Fornitore garantisce, per l’ambito di trattamento affidato, la messa in atto delle misure tecniche ed organizzative necessarie affinché il trattamento di dati personali avvenga in conformità con le prescrizioni della Normativa Privacy vigente, impegnandosi a consentire al Consiglio regionale le attività di verifica ai sensi dell’art. 28, par. 3, RGPD.
5. Il Fornitore è obbligato a conservare i dati personali esclusivamente per i tempi stabiliti dal presente contratto e dalle norme di legge applicabili in materia.
6. Il Fornitore è tenuto a presentare all’Amministrazione garanzie in termini di conoscenza specialistica, affidabilità, risorse, anche in ordine all’adozione di misure tecniche, logiche ed organizzative idonee per assicurare che i trattamenti dei dati personali affidatigli avvengano in conformità alla normativa Privacy; a tale fine il Fornitore è tenuto a trasmettere, su richiesta, una relazione in cui descrive il proprio sistema di gestione dei dati personali in conformità al RGPD anche in termini di adeguatezza al rispetto delle previsioni dell’allegato di designazione come responsabile del trattamento, nonché le misure tecniche e di sicurezza implementate con riferimento all’applicativo. Il Fornitore deve mantenere, per tutta la durata dell’affidamento, un’organizzazione adeguata all’esecuzione dell’incarico di trattamento dei dati personali connesso alle prestazioni contrattuali, garantendo il pieno rispetto, per sé e per i propri

dipendenti e collaboratori, delle istruzioni sul trattamento dei dati personali dell'allegato D, oltre che di tutte le norme di legge in materia applicabili.

7. Il Fornitore garantisce, per l'ambito di trattamento affidato, che i dati del Titolare del trattamento sono trattati nel territorio dell'Unione Europea o dello Spazio Economico Europeo ovvero nel territorio di Paesi non appartenenti allo Spazio Economico Europeo ritenuti adeguati tramite decisione della Commissione europea ai sensi degli art. 45 e 46 del Regolamento UE 2016/679.
8. Il Fornitore è obbligato a collaborare con il Titolare del trattamento per il rispetto delle norme sulla protezione dei dati personali e deve fornire al Consiglio regionale la documentazione e le informazioni necessarie in relazione ai servizi svolti e alle misure di sicurezza applicate e garantire l'assistenza necessaria per garantire il rispetto della Normativa privacy, compresa, se richiesta, l'assistenza alla redazione dell'analisi del rischio per la protezione dei dati personali (art. 32 e 35 RGPD) secondo le procedure di cui alla deliberazione Ufficio di presidenza 4.11.2019, n. 423 recante "Metodologia per l'analisi del rischio e la valutazione di impatto per la protezione dei dati personali da applicare ai trattamenti di dati personali del Consiglio regionale della Lombardia" e ss.mm.ii. allegata alla documentazione di gara.
9. Il Fornitore ha l'obbligo di comunicare un recapito per comunicazioni relative al trattamento dei dati personali e, salva la deroga di cui all'art. 20, par. 5, RGPD, di tenere il registro delle attività di trattamento dei dati personali effettuate per conto del Titolare e, su richiesta, di mettere tale registro a disposizione del Titolare e/o del Garante per la protezione dei dati personali.
10. In ragione delle attività affidate, il Fornitore s'impegna a redigere e mantenere aggiornato un elenco con gli estremi identificativi delle persone fisiche, appositamente designate, che svolgeranno le attività con privilegi di amministratore di sistema, definendone le funzioni e gli ambiti operativi di intervento, e garantisce ogni misura per l'assolvimento delle prescrizioni e degli obblighi di cui al provvedimento del Garante per la protezione dei dati personali del 27.11.2008 sugli amministratori di sistema, dandone conferma annuale al Consiglio regionale.
11. La designazione come responsabile del trattamento è efficace per tutta la durata del rapporto contrattuale, fino alla scadenza dello stesso e conserva la sua efficacia in caso di rinnovo, ripetizione o proroga. Il Fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti o collaboratori impegnati nell'esecuzione delle prestazioni contrattuali, che devono essere vincolati legalmente ai medesimi obblighi di riservatezza.
12. In caso di revoca della designazione come responsabile del trattamento oppure al termine del contratto, anche anticipato per recesso o risoluzione, il Fornitore s'impegna a seguire le istruzioni impartite dal Titolare, provvedendo alle operazioni richieste dal Titolare stesso, salva la conservazione di eventuali dati che il Fornitore deve conservare per obbligo di legge.
13. È in ogni caso fatto divieto al Fornitore di eseguire trattamenti non finalizzati all'esecuzione delle attività affidate e in particolare è fatto divieto di pubblicare, cedere, donare o altrimenti disporre dei dati, senza la preventiva ed espressa richiesta o autorizzazione dell'Amministrazione consiliare.

14. L'individuazione di ulteriori Responsabili del trattamento dovrà essere effettuata in conformità dell'art. 28, par. 2 e 4, RGPD.
15. In conformità agli articoli 82 e 83, il Responsabile del trattamento risponde di ogni perdita, costo, spesa, multa e/o sanzione, danno derivante da o in connessione con una qualsiasi violazione delle disposizioni del presente capitolato, della Normativa privacy e dei compiti e istruzioni di cui all'allegato D, da parte sua, dei suoi dipendenti o collaboratori o degli eventuali altri responsabili del trattamento di sua designazione.
16. Ogni altra attività di trattamento ulteriore rispetto quella di cui al comma 3 rientra nella titolarità autonoma del Fornitore, che in tale veste risponde della liceità del trattamento e del rispetto delle disposizioni in materia di protezione dei dati personali.

#### **Art. 15 - Patto di riservatezza**

1. Ferme le disposizioni di cui al precedente articolo, i dati economici, finanziari, patrimoniali o di qualunque altro genere, che vengano a conoscenza del Fornitore, in ragione dei servizi resi per il Consiglio regionale, sono riservati. I dati e le informazioni, non oggetto di pubblicazione in base alla legge, fermo il divieto di cui al comma 13 dell'articolo precedente, venute a conoscenza del Fornitore in relazione all'esecuzione del presente contratto e le informazioni che transitano attraverso le apparecchiature di rilevazione, elaborazione, trasferimento, archiviazione dei dati del Fornitore non debbono in alcun modo e in nessuna forma essere comunicate e divulgate a terzi, né debbono essere utilizzate da parte del Fornitore o da parte di chiunque collabori alle sue attività per fini diversi da quelli contemplati nel presente capitolato/contratto.
2. Il Fornitore è tenuto a mantenere riservati tali dati, a non divulgarli in alcun modo e a non utilizzarli per scopi diversi da quelli relativi all'esecuzione del contratto. Il Fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti o collaboratori impegnati nell'esecuzione delle prestazioni contrattuali dei suddetti obblighi di riservatezza.
3. Tale clausola deve intendersi vincolante anche dopo la cessazione del presente contratto.
4. Il Consiglio regionale s'impegna a trattare, in conformità al d.lgs. 196/2003 e al RGPD, i dati personali conferiti dal Fornitore per le sole finalità di definizione e gestione del contratto e dei relativi pagamenti, provvedendo alle comunicazioni e alle pubblicazioni dei dati relativi all'affidamento secondo quanto previsto dal d.lgs. 36/2023, dal d.lgs. 33/2013 e dalle altre norme in materia come descritto nell'informativa sul trattamento dei dati personali di cui all'art. 13 e 14 RGPD, allegata alla documentazione di procedura.

#### **Art. 16 - Rispetto del codice di comportamento dei dipendenti pubblici e del personale del Consiglio regionale della Lombardia**

1. Il Fornitore, con la sottoscrizione del presente Foglio Patti e condizioni, si impegna a osservare e a far osservare ai propri dipendenti e collaboratori a qualsiasi titolo gli obblighi di condotta previsti dal d.p.r. 16 aprile 2013, n. 62 "Codice di comportamento dei dipendenti pubblici" pubblicato nella Gazzetta Ufficiale n. 129 del 4.06.2013 e dal Codice di Comportamento del

personale del Consiglio regionale della Lombardia adottato con Deliberazione dell'Ufficio di Presidenza 24.10.2022 n. 356, allegata alla documentazione di procedura e comunque disponibile sul sito istituzionale del Consiglio regionale.

#### **Art. 17 - Divieto di “*pantouflage*” e relative sanzioni**

1. Ai sensi dell'articolo 53, comma 16-ter, del d.lgs. 30 marzo 2001, n. 165, i dipendenti che, negli ultimi tre anni di servizio, hanno esercitato poteri autoritativi o negoziali per conto delle pubbliche amministrazioni di cui all'articolo 1, comma 2, del medesimo decreto legislativo, non possono svolgere, nei tre anni successivi alla cessazione del rapporto di pubblico impiego, attività lavorativa o professionale presso i soggetti privati destinatari dell'attività della pubblica amministrazione svolta attraverso i medesimi poteri.
2. I contratti conclusi e gli incarichi conferiti in violazione di tale divieto sono nulli ed è fatto divieto ai soggetti privati che li hanno conclusi o conferiti di contrattare con le pubbliche amministrazioni per i successivi tre anni, con obbligo di restituzione dei compensi eventualmente percepiti e accertati ad essi riferiti.

#### **Art. 18 - Segnalazione di violazioni nell'Amministrazione (c.d. whistleblowing) da parte dei lavoratori e collaboratori delle imprese fornitrici**

1. Ai sensi del d.lgs. 24/2023, i lavoratori e i collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'Amministrazione consiliare che, nell'interesse pubblico e dell'integrità del Consiglio regionale, segnalano al Responsabile della prevenzione della corruzione e della trasparenza (RPCT) del Consiglio regionale le violazioni di norme nazionali ed europee che consistono in illeciti penali, civili, contabili e amministrativi, di cui siano venuti a conoscenza in ragione del rapporto di lavoro/collaborazione, non possono essere sanzionati, demansionati, licenziati, trasferiti, o sottoposti ad altra misura, determinata dalla segnalazione, avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro. L'adozione di misure ritenute ritorsive nei confronti del segnalante può essere segnalata all'ANAC per i provvedimenti di competenza. Sono previste forme di garanzia della riservatezza dell'identità del segnalante il cui nominativo non può essere comunicato se non con il consenso del segnalante o in caso di legittima richiesta dell'Autorità giudiziaria e contabile.
2. Il Fornitore è tenuto a informare i propri dipendenti o collaboratori a qualsiasi titolo impegnati in prestazioni o servizi per l'Amministrazione consiliare della tutela di cui al comma 1 e a renderli edotti che sul portale del Consiglio regionale è messa a disposizione, nella sezione “Segnalazione di violazioni nell'amministrazione (whistleblowing)”, la “Procedura per la segnalazione di violazioni nell'Amministrazione (c.d. whistleblowing) ai sensi del decreto legislativo 24/2023”, con i dati di contatto del RPCT, le istruzioni e il link alla piattaforma web “Segnalazione illeciti”, nonché l'informativa sul trattamento dei dati personali.

**Art. 19 - Stipulazione del contratto**

1. Il contratto è stipulato ai sensi dell'articolo 18, comma 1, del Codice, mediante corrispondenza secondo l'uso commerciale.
2. Come disciplinato dall'Allegato I.4 del Codice, il contratto è esente dall'imposta di bollo.

**Art. 20 - Risoluzione delle controversie e Foro competente**

1. In caso di controversie di qualsiasi natura inerenti al contratto e alla sua esecuzione, le parti concordano nel riconoscere la competenza esclusiva del Foro di Milano.

**Art. 21 - Indirizzo di posta elettronica certificata del Consiglio regionale**

1. Le comunicazioni a mezzo di posta elettronica certificata destinate al Consiglio regionale devono essere spedite al seguente l'indirizzo:  
[protocollo.generale@pec.consiglio.regione.lombardia.it](mailto:protocollo.generale@pec.consiglio.regione.lombardia.it).

**Art. 22 - Norma finale**

1. Per tutto quanto non espressamente previsto nel presente Foglio Patti e condizioni si applica la normativa vigente in materia. Tutti i riferimenti a disposizioni legislative e regolamentari sono da intendersi riferite alla formulazione della norma in vigore al momento dell'affidamento.

Firma digitale per accettazione

## **Clausole del Foglio Patti e condizioni di cui all'art. 1341 c.c.**

### **CLAUSOLE DEL FOGLIO PATTI E CONDIZIONI DI CUI ALL'ART. 1341 C.C.**

Ai sensi e per gli effetti dell'articolo 1341 del Codice civile, sono individuate le clausole di cui agli articoli 6 (Revisione dei prezzi), 7 (Penali), 8 (Clausola risolutiva ai sensi dell'art. 1456 del Codice civile), 10 (Recesso ai sensi dell'art. 123 del d.lgs. 36/2023), 14 (Trattamento dei dati personali e designazione del Fornitore quale responsabile del trattamento dei dati), 15 (Patto di riservatezza), 16 (Rispetto del codice di comportamento dei dipendenti pubblici e del personale del Consiglio regionale della Lombardia) e 20 (Risoluzione delle controversie e Foro competente), del presente Foglio Patti e condizioni.

## Allegato D – Designazione del responsabile del trattamento dei dati personali

**Atto di designazione come responsabile del trattamento dei dati personali e individuazione dei trattamenti consentiti, delle finalità, della tipologia dei dati personali e dei compiti del responsabile del trattamento, ai sensi dell'art. 28 del Regolamento UE 2016/679 del 27 aprile 2016, per l'acquisizione di credenziali per l'accesso alla piattaforma di e-learning "Cyber Guru Awareness" per l'erogazione di una annualità di corsi di formazione online sulla sicurezza informatica, destinati ai dipendenti del Consiglio regionale della Lombardia.**

### Sommario

|                                                                                                                                                                                 |           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| PREMESSA .....                                                                                                                                                                  | 19        |
| DURATA.....                                                                                                                                                                     | 20        |
| OBBLIGHI DEL TITOLARE DEL TRATTAMENTO .....                                                                                                                                     | 20        |
| OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO.....                                                                                                                                  | 21        |
| ATTIVITÀ DI VIGILANZA E VERIFICA DEL TRATTAMENTO .....                                                                                                                          | 34        |
| INDIVIDUAZIONE DI MAGGIORI LIVELLI DI SICUREZZA E ADEGUAMENTI ALLA NORMATIVA<br>PRIVACY SOPRAVVENUTA O A ESIGENZE CONTRATTUALI SOPRAVVENUTE .....                               | 35        |
| COMUNICAZIONI.....                                                                                                                                                              | 35        |
| DISPOSIZIONI FINALI.....                                                                                                                                                        | 36        |
| DATI DI CONTATTO DEI RESPONSABILI DELLA PROTEZIONE DEI DATI PERSONALI (RPD) ...                                                                                                 | 36        |
| ALLEGATI.....                                                                                                                                                                   | 36        |
| <b>ALLEGATO A.1 - ELENCO DEI TRATTAMENTI DI DATI PERSONALI DI TITOLARITÀ DEL CONSIGLIO<br/>REGIONALE AFFIDATI AL FORNITORE IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO .....</b> | <b>37</b> |
| <b>ALLEGATO A.2 - ELENCO DELLE MISURE DI SICUREZZA .....</b>                                                                                                                    | <b>42</b> |

## **PREMESSA**

Ai fini del presente Atto, s'intende per:

- **Titolare del trattamento**, ai sensi dell'articolo 4, n. 7, RGPD, il Consiglio regionale della Lombardia [di seguito denominato anche "Consiglio regionale" o "Titolare del trattamento"], C.F. 80053570158, nella persona del dirigente pro tempore dell'Ufficio Contratti e ICT, domiciliato per la carica presso la sede del Consiglio regionale della Lombardia in Milano, via Fabio Filzi n. 22, in conformità alla deliberazione dell'Ufficio di presidenza 1 aprile 2019, n. 111 (Definizione dell'assetto organizzativo privacy – Articolazione delle competenze in materia di protezione in materia di protezione di dati personali (Regolamento (UE) 2016/679 e d.lgs. 2003 come modificato dal d.lgs. 101/2018) e alla deliberazione dell'Ufficio di Presidenza 28 luglio 2021, n. 184 (Aggiornamento 2021 dell'assetto organizzativo privacy) e ss.mm.ii;
- **Responsabile del trattamento**, ai sensi dell'articolo 4, n. 8, RGPD, è il Fornitore, aggiudicatario del servizio, in persona del proprio Legale Rappresentante pro tempore, domiciliato presso la società che rappresenta;
- **Normativa privacy**, il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), di seguito denominato RGPD, il d.lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, [di seguito denominato: Codice Privacy] e ogni altra disposizione di contenuto normativo sulla protezione dei dati personali applicabile sul territorio nazionale, ivi compresi i provvedimenti dell'Autorità Garante per la Protezione dei dati personali;
- "sub-responsabile del trattamento", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, soggetto terzo, al quale il Responsabile del trattamento abbia affidato l'esecuzione di specifiche attività di trattamento ai sensi dell'art. 28, par. 2 e 4, RGPD;
- "affidamento", il capitolato/contratto definito nel decreto di aggiudicazione e/o in ogni altro atto contrattuale tra il Consiglio regionale e il Fornitore;
- per le altre definizioni si rinvia all'art. 4 RGPD.

Il presente atto è stato predisposto al fine di specificare, ai sensi dell'art. 28 del Regolamento (UE) 2016/679, i trattamenti di dati personali affidati dal Consiglio regionale al Fornitore definendo la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi gravanti sul Titolare e sul Responsabile del trattamento.

Il **Titolare del trattamento** e il **Responsabile del trattamento** dichiarano reciprocamente di essere informati e di acconsentire che i dati personali forniti o raccolti in conseguenza dell'affidamento sono trattati esclusivamente per le finalità ivi indicate ed in conformità a quanto previsto dalla vigente normativa in materia di protezione dei dati personali.

A tal fine il **Responsabile del trattamento** è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto dell'affidamento e si impegna ad effettuare, per conto del Titolare del trattamento, le sole operazioni di trattamento necessarie a tal fine, nei limiti delle finalità ivi specificate, nel rispetto della Normativa privacy e delle istruzioni fornite, come definitivi nell'Allegato A.1.

Le premesse e gli allegati **A.1** (Elenco dei trattamenti dei dati personali di titolarità del Consiglio regionale della Lombardia effettuati dal Fornitore in qualità di Responsabile del trattamento) e **A.2** (Elenco delle misure di sicurezza applicate dal Fornitore) costituiscono parte integrante e sostanziale del presente Atto.

Rimangono valide le prescrizioni e gli obblighi, anche relativi alle misure di sicurezza applicate, definiti nell'affidamento richiamato in premessa e negli eventuali altri atti allegati allo stesso, nonché in eventuali altri atti successivi stipulati tra le parti.

I dati economici, finanziari, patrimoniali o di qualunque altro genere, che vengano a conoscenza del Fornitore, in ragione dei servizi resi per il Consiglio regionale, sono riservati. Il Consiglio regionale s'impegna a trattare, in conformità al Codice privacy e al RGPD, i dati personali conferiti dal Fornitore per le sole finalità di definizione e gestione del servizio e dei relativi pagamenti, provvedendo alle comunicazioni e alle pubblicazioni dei dati relativi all'affidamento secondo quanto previsto dal d.lgs. 36/2023, dal d.lgs. 33/2013 e dalle altre norme in materia.

## **DURATA**

La designazione a **Responsabile del trattamento** e le clausole del presente Atto hanno durata pari a quella dell'Affidamento.

La designazione e il presente Atto cesseranno automaticamente di avere efficacia in ipotesi di risoluzione, recesso o perdita di efficacia dell'Affidamento, salvo il tempo eventualmente necessario a consentire al Consiglio regionale di recuperare i dati personali, come contrattualmente definito.

Parimenti, in caso di rinnovo, proroga e differimento a ogni titolo della durata dell'Affidamento, la designazione e il presente Atto continueranno a produrre i propri effetti senza necessità di ulteriori atti delle parti.

Il **Responsabile del trattamento** s'impegna a mantenere riservati i dati e le informazioni personali conosciute in ragione dei servizi resi e della presente designazione, anche dopo la cessazione di efficacia del presente Atto.

## **OBBLIGHI DEL TITOLARE DEL TRATTAMENTO**

Con riguardo alle tipologie di dati personali e categorie di interessati indicati nell'allegato A.1 del presente Atto, il Consiglio regionale verifica e garantisce, per quanto di competenza in qualità di Titolare del trattamento, la liceità del trattamento e il rispetto dei principi applicabili al trattamento di dati personali, ai sensi della Normativa Privacy, delle norme dello Statuto della Regione Lombardia, del Regolamento generale del Consiglio regionale e delle disposizioni della legge regionale e della legge statale applicabili alle diverse fattispecie e della deliberazione del Consiglio regionale 6 maggio 2014, n. X/378 (Regolamento per il trattamento dei dati personali sensibili e giudiziari

di cui è Titolare il Consiglio Regionale della Lombardia (pubblicato sul BURL n. 20 serie ordinaria del 15 maggio 2014).

Il **Titolare del trattamento** s'impegna a fare un uso appropriato dei servizi forniti dal **Responsabile del trattamento** per garantire un livello di sicurezza adeguato e fare un uso responsabile delle credenziali, dei sistemi e dei dispositivi utilizzati per accedere ai servizi forniti dal **Responsabile del trattamento**.

Il **Titolare del trattamento** s'impegna a rispettare i termini per le comunicazioni, le autorizzazioni e le richieste di informazioni e di attivazione dei poteri di verifica di cui al presente Atto.

## **OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO**

Il **Responsabile del trattamento** dichiara di avere una struttura e un'organizzazione adeguata all'esecuzione dell'incarico di trattamento dei dati personali del Titolare del trattamento e s'impegna a mantenerla adeguata alla rilevanza dell'incarico stesso, garantendo il pieno rispetto per sé e per i propri dipendenti e collaboratori a qualunque titolo della Normativa Privacy e di quanto prescritto nel presente Atto.

Il **Responsabile del trattamento** esegue esclusivamente i trattamenti di cui all'Allegato A.1, richiesti dal Titolare del trattamento e indispensabili per l'esecuzione delle prestazioni contrattuali in modo lecito e secondo correttezza, per scopi legittimi e determinati assicurando l'esattezza e la completezza dei dati e garantendo il rispetto dei principi di necessità, proporzionalità, pertinenza e non eccedenza, e garantisce lo svolgimento dei compiti sottoindicati.

Il **Responsabile del trattamento** si attiene alle istruzioni del Titolare, tra cui rientrano anche le prescrizioni di cui al provvedimento recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni" di cui alla circolare del 18 aprile 2017, n. 2/2017, recante "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»" e, in quanto compatibili, le Linee guida sulla sicurezza nel procurement ICT (Determinazione n. 220/2020 del 17 maggio 2020 Agid), le circolari AgID n. 2 "Criteri per la qualificazione dei Cloud Service Provider per la PA" e n. 3 "Criteri per la qualificazione di servizi SaaS per il Cloud della PA" del 2018, la Determinazione AgID n. 628/2021 del 15 dicembre 2021 - Adozione del "Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione" e i provvedimenti di ACN (ad es. in materia di infrastrutture e servizi cloud per le PPAA, Linee guida per la conservazione delle password, atti regolamentari della disciplina cyber).

Il **Responsabile del trattamento** si attiene altresì, per quanto compatibile, alle istruzioni e alle misure di cui al Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale adottato dal Garante per la protezione dei dati personali in data 7 ottobre 2024.

Il **Responsabile del trattamento** è autorizzato a svolgere le attività di trattamento indispensabili per lo svolgimento del servizio affidato, come descritto nell'Affidamento o concordate con il **Titolare** con altro valido atto scritto, attenendosi alla Normativa Privacy e rispettando gli obblighi di cui al presente Atto e alle istruzioni impartite dal Titolare del trattamento, in modo lecito e secondo correttezza, per scopi legittimi e determinati assicurando l'esattezza e la completezza dei dati e garantendo il rispetto dei principi di necessità, proporzionalità, pertinenza e non eccedenza.

Senza specifica autorizzazione del Titolare, il **Responsabile del trattamento** non può effettuare trattamenti di dati personali ulteriori rispetto a quelli indicati nel presente Atto e nei suoi allegati e comunque non finalizzati all'adempimento delle prestazioni contrattuali o di obblighi di legge connessi alle prestazioni contrattuali stesse.

Il **Responsabile del trattamento** non è autorizzato a effettuare copie permanenti dei dati personali, se non su espressa autorizzazione scritta del **Titolare del trattamento** e deve in ogni caso conservare i dati personali temporaneamente acquisiti, solo per il tempo strettamente necessario alle esigenze e agli adempimenti contrattuali con il Consiglio regionale e agli altri obblighi di legge, se previsti; tali dati devono essere cancellati con modalità che ne garantiscano la certa non recuperabilità, documentando per iscritto le operazioni a tal fine eseguite decorso un mese dalla conclusione dell'affidamento, salvo diversa richiesta del Titolare.

Le operazioni di cancellazione sicura e a norma dei dati dai supporti, sistemi e reti del **Responsabile del trattamento** devono essere documentate e in merito dell'avvenuta effettuazione e conclusione positiva delle stesse il Responsabile del trattamento deve rilasciare apposita dichiarazione ai sensi del D.P.R. 445/2000.

Il **Titolare del trattamento** può autorizzare il **Responsabile del trattamento** a copiare, duplicare, riprodurre o registrare i dati indispensabili per l'esecuzione dell'attività affidata, solo per il tempo strettamente necessario allo svolgimento della stessa e mettendo in atto le necessarie precauzioni da concordare con il Titolare del trattamento per la trasmissione/trasferimento e ogni misura di sicurezza necessaria a garantire la riservatezza dei dati tenendo conto dei rischi correlati e della natura anche sensibile dei dati stessi. In ogni caso, il **Responsabile del trattamento** garantisce che la trasmissione/trasferimento dei dati avvenga su canali sicuri o in forma criptata (per esempio, HTTPS e SSH v2; file criptati con password comunicata con altro canale), salvo che sia diversamente richiesto e autorizzato dal Titolare del trattamento.

Salvo con riguardo ai dati e ai documenti resi pubblici dal Titolare del trattamento o che siano tali per natura (per esempio provvedimenti normativi), è fatto assoluto divieto al **Responsabile del trattamento** di diffondere i dati e di comunicarli a terzi, senza previa, espressa e scritta autorizzazione del Titolare del trattamento.

Il **Responsabile del trattamento** non è autorizzato a comunicare a terzi, pubblicare, cedere, donare o altrimenti disporre dei dati personali di titolarità del Consiglio regionale, senza la preventiva ed espressa richiesta o autorizzazione dell'Amministrazione consiliare, salvo non sia richiesto da disposizioni di legge e con riguardo ai dati e ai documenti resi pubblici dal Titolare o che siano tali per natura (per esempio provvedimenti normativi).

Il **Responsabile del trattamento** informa immediatamente il **Titolare del trattamento** qualora a suo parere un'istruzione del Titolare violi la Normativa Privacy.

### **Personale e altri collaboratori**

Il **Responsabile del trattamento** adotta le misure appropriate per garantire la conformità al presente Atto delle attività e dei comportamenti dei suoi dipendenti ed eventuali appaltatori e sub-responsabili relativamente al loro ambito di prestazione.

Il **Responsabile del trattamento** provvede in particolare a che gli operatori assegnati al trattamento sotto la sua autorità, compresi gli amministratori di sistema, siano autorizzati per iscritto o con modalità tracciabile agli specifici trattamenti necessari per lo svolgimento delle loro mansioni e siano adeguatamente istruiti e formati in materia di protezione dei dati personali, predisponendo e attuando un piano di formazione, nonché vincolati legalmente al rispetto degli obblighi di riservatezza di cui al presente Atto (art. 29 RGPD e art. 2-*quaterdecies* d.lgs. 196/2003) mediante la sottoscrizione di apposite dichiarazioni, le cui copie saranno messe a disposizione del Titolare del trattamento su richiesta per l'esercizio delle attività di controllo e vigilanza di propria competenza.

Il **Responsabile del trattamento** provvede altresì affinché ai dati personali accedano solo gli operatori incaricati obbligandoli a conformare il proprio comportamento alle seguenti prescrizioni: a) i dati personali possono essere utilizzati soltanto per gli scopi previsti nell'Affidamento; b) i dati personali devono essere conservati in modo da evitarne la dispersione, la sottrazione e ogni altro uso non conforme alla legge e alle istruzioni ricevute; c) i dati personali di cui si venga a conoscenza in occasione dello svolgimento della prestazione principale o di attività a essa strumentali non possono essere diffusi, né altrimenti utilizzati per interessi privati, propri o altrui; d) i comportamenti non conformi alle norme sulla protezione dei dati personali o l'eventuale smarrimento o perdita dei dati o delle credenziali di autenticazione sono immediatamente comunicati ai referenti del Titolare del trattamento. e) i dati personali sono custoditi fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate; f) nel caso di comunicazioni telefoniche o vocali scambiate durante lo svolgimento delle proprie attività in merito a dati personali del Titolare i comportamenti tenuti si conformano alla necessità di garantire la riservatezza delle informazioni trattate.

Il **Responsabile del trattamento** risponde per l'esatta osservanza degli obblighi di riservatezza e per l'esatta e diligente applicazione dei compiti e delle istruzioni di cui al presente atto, da parte dei propri dipendenti o collaboratori o altre persone fisiche impegnati, su suo incarico, nell'esecuzione delle prestazioni contrattuali.

In relazione ai soggetti incaricati al trattamento che agiscono sotto la sua autorità, il **Responsabile del trattamento** è tenuto a istruirli sulla normativa privacy e sugli obblighi di cui presente Atto, predisponendo ed attuando un piano di formazione destinato ai soggetti incaricati autorizzati al trattamento.

### **Sistema di autenticazione per gli incaricati del Responsabile e per i dipendenti del Consiglio regionale**

Il **Responsabile del trattamento** è tenuto a predisporre un sistema di autenticazione per gli applicativi/postazioni di lavoro/piattaforme telematiche e analoghi strumenti che consentono l'accesso ai dati personali del **Titolare del trattamento**, che garantisca la riservatezza.

Il **Responsabile del trattamento**, con riguardo al sistema di autenticazione, è tenuto alle seguenti misure minime:

- a) prevedere profili di autorizzazione di accesso per ogni singolo soggetto incaricato/autorizzato al trattamento o gruppo omogeneo e configurarli prima dell'inizio dei trattamenti in modo adeguato alle mansioni svolte e agli ambiti di trattamento affidati;
- b) assicurarsi che a ogni soggetto incaricato/autorizzato sia assegnata una credenziale di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione del soggetto autorizzato al trattamento associato a una parola chiave (*password*) riservata e conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e a uso esclusivo dell'incaricato/autorizzato, eventualmente associato a un codice identificativo o a una parola chiave. Non è ammessa la creazione di credenziali non nominative, salvo specifica richiesta del Titolare;
- c) prescrivere necessarie cautele per assicurare la segretezza della componente riservata della credenziale e/o la diligente custodia del dispositivo in possesso a uso esclusivo del soggetto incaricato/autorizzato al trattamento;
- d) assicurare che per la componente riservata della credenziale di autenticazione siano previste adeguate misure di sicurezza;
- e) richiedere al soggetto interessato di utilizzare sempre le proprie credenziali personali mantenendole riservate, evitando di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire l'individuazione dell'autore del trattamento;
- f) assicurare che la parola chiave, quando prevista sia composta da almeno quattordici (14) caratteri misti alfanumerici; essa non deve contenere riferimenti agevolmente riconducibili all'Incaricato e deve essere modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni tre mesi, ove non presente un ulteriore fattore di autenticazione oltre al codice di identificazione e alla password;
- g) assicurare che l'utenza venga bloccata dopo un numero di tentativi falliti di accesso pari a tre;
- h) assicurare un sistema di reset della password che consenta l'identificazione del richiedente;
- i) assicurare che il codice per l'identificazione, laddove utilizzato, non possa essere assegnato ad altri incaricati, neppure in tempi diversi e assicurare che sia operata la disattivazione delle credenziali di autenticazione o delle abilitazioni di accesso del personale in caso venga a cessare la necessità di accesso da parte del soggetto incaricato autorizzato al trattamento o intervenga un'inattività per più di tre mesi;

- j) predisporre le necessarie procedure affinché, in caso di prolungata assenza o impedimento dell'incaricato/autorizzato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, si possa comunque assicurare la disponibilità di dati o strumenti elettronici;
- k) verificare a intervalli almeno annuali le autorizzazioni in essere;
- l) implementare un sistema di autenticazione a due fattori su richiesta del Titolare in base al livello di rischio dei trattamenti di dati personali e alle prescrizioni delle norme di riferimento;
- m) adottare misure per prevenire e contrastare attacchi informatici di tipo credential stuffing (testing username/password pairs obtained from the breach of another site), brute force (testing multiple passwords from dictionary or other source against a single account) e password spraying (testing a single weak password against)

Su richiesta del direttore dell'esecuzione o di suo delegato, il **Responsabile del trattamento** è tenuto ad operare l'attivazione e la disattivazione delle credenziali di autenticazione per i soggetti indicati dal Titolare in caso venga a cessare la necessità di accesso.

È consentita l'implementazione di ulteriori o diverse misure di sicurezza rispetto a quanto sopra solo qualora le misure garantiscano un maggior livello di sicurezza.

Il **Responsabile del trattamento** è tenuto ad applicare le prescrizioni minime di sicurezza sopra riportate anche alle credenziali di autenticazione fornite ai dipendenti e agli incaricati/autorizzati del Titolare del trattamento per accedere alla piattaforma web utilizzate per l'erogazione del servizio. Diverse misure di sicurezza applicate al sistema di autenticazione possono essere autorizzate per iscritto dal Titolare del trattamento, previa verifica della loro adeguatezza rispetto ai rischi per i dati personali.

Il **Responsabile del trattamento** mette a disposizione un inventario delle utenze presenti nel sistema con i relativi profili di autorizzazione assegnati, disponibile al Titolare per sua rendicontazione e analisi degli accessi.

Il **Responsabile del trattamento** è tenuto ad adottare un sistema di salvataggio dei log di accesso al sistema in modo che il Titolare possa esportarli.

Il **Responsabile del trattamento** adotta, per la conservazione delle password degli utenti, di adeguate tecniche crittografiche quali le funzioni di derivazione di chiavi crittografiche (Key Derivation Function) che offrono garanzie in caso di loro esfiltrazione dai sistemi informatici del Produttore (cfr. OWASP Password Storage Cheat Sheet, NIST 800-63B Digital Identity Guidelines).

### **Amministratori di sistema**

Per quanto riguarda le attività degli amministratori di sistema svolti su infrastrutture e reti proprie il **Responsabile del trattamento** deve redigere e mantenere aggiornato un elenco con gli estremi identificativi delle persone fisiche, appositamente designate, dal Responsabile stesso, che espleteranno nell'ambito delle attività previste dal contratto, funzioni di Amministratori di Sistema (AdS), con la definizione delle funzioni e dell'ambito operativo a ciascuno assegnato, e garantire ogni altra misura per l'assolvimento delle prescrizioni e degli obblighi di cui al provvedimento del Garante per

la protezione dei dati personali del 27.11.2008 sugli amministratori di sistema e successive modifiche e integrazioni.

Il **Responsabile del trattamento** garantisce l'applicazione delle misure previste dal citato Provvedimento del Garante dandone conferma scritta al Titolare su richiesta.

### **Rispetto della normativa sui cookies**

Il **Responsabile del trattamento** si impegna a garantire che l'applicativo web utilizzato per il servizio sia configurato al fine di garantire il trattamento dei soli dati degli utenti indispensabili, nel rispetto di quanto definito dal provvedimento del Garante per la protezione dei dati personali n. 231 del 10 giugno 2021 recante "Linee guida cookie e altri strumenti di tracciamento" pubblicato sulla Gazzetta Ufficiale n. 163 del 9 luglio 2021 e di quanto definito nell'allegato A.1. del presente atto.

Il **Responsabile del trattamento** fornisce al Titolare del trattamento le informazioni e il supporto necessari per assicurare la corretta informazione degli interessati circa il rispetto e la conformità del portale alla normativa sui cookies e ai provvedimenti anche futuri del Garante, assistendolo nella redazione dell'informativa, mettendo in atto le misure tecniche e organizzative che si rendano all'uopo necessarie e garantendo l'effettuazione di un monitoraggio circa la rispondenza del servizio web alla normativa e la trasmissione di apposito report al Titolare.

Le eventuali difformità rilevate devono essere immediatamente comunicate al Titolare affinché assuma le necessarie determinazioni.

### **Misure di sicurezza tecniche e organizzative**

Il **Responsabile del trattamento** deve assicurare, per le componenti di sua competenza e per tutta la durata dell'Affidamento, in ogni momento, che la sicurezza fisica e logica dei dati oggetto di trattamento sia conforme alle norme vigenti. Le misure di sicurezza adottate, ai sensi dell'art. 32 del RGPD, devono in ogni situazione uniformarsi allo "standard" di maggiore sicurezza fra le disposizioni di legge e gli elementi contrattuali e/o progettuali.

Le misure di sicurezza adottate devono in ogni situazione uniformarsi allo "standard" di maggiore sicurezza fra le disposizioni di legge e gli elementi contrattuali/progettuali indicati nell'Atto di affidamento, tra cui le misure di cui al provvedimento recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni" di cui alla circolare del 18 aprile 2017, n. 2/2017, recante "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»", alle Linee guida sulla sicurezza nel procurement ICT (Determinazione n. 220/2020 del 17 maggio 2020 Agid) e, se applicabili, alle circolari AgID n. 2 "Criteri per la qualificazione dei Cloud Service Provider per la PA" e n. 3 "Criteri per la qualificazione di servizi SaaS per il Cloud della PA" del 2018 e la Determinazione AgID n. 628/2021 del 15 dicembre 2021 - Adozione del "Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di

qualificazione dei servizi cloud per la pubblica amministrazione”, i provvedimenti di ACN (ad es. in materia di infrastrutture e servizi cloud per le PPAA, Linee guida per la conservazione delle password, atti regolamentari della disciplina cyber) e il Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale.

Il **Responsabile del trattamento** è tenuto a implementare e mantenere efficaci le misure tecniche e organizzative, per proteggere i dati del Titolare del trattamento da distruzione, perdita, alterazione, divulgazione o accesso non autorizzati o accidentali

Il **Responsabile del trattamento** si impegna a individuare e adottare misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, tenendo conto, fra l'altro, della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche nonché della tecnologia applicabile e dei costi di attuazione. Tali misure comprendono, ove opportuno:

- i) la cifratura dei dati personali;
- ii) i mezzi che permettono di garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
- iii) i mezzi che permettono di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso d'incidente fisico o tecnico;
- iv) una procedura (messa a disposizione del titolare su richiesta) mirata a testare, verificare e valutare regolarmente l'efficacia delle misure di sicurezza tecniche e organizzative al fine di garantire la sicurezza del trattamento.

I sistemi del **Responsabile del trattamento** devono in particolare essere dotati di misure di protezione perimetrali logico-fisiche e i sistemi software, i programmi utilizzati e la protezione antivirus devono essere costantemente aggiornati sia sui server sia sulle postazioni di lavoro. L'adeguamento alle misure minime di sicurezza implica, tra l'altro, la presenza di un adeguato sistema informatico che renda possibile:

- l'accesso ai dati tramite sistema di autenticazione;
- la protezione del computer tramite programmi contro il rischio di intrusione e l'accesso abusivo in accordo ai requisiti di legge aggiornati almeno semestralmente e comunque in occasione di ogni versione disponibile dalla casa costruttrice, anche per i sistemi non connessi in rete o che non accedono a Internet;
- la modifica e l'aggiornamento, ogni qualvolta vi sia la disponibilità e comunque entro un congruo periodo di tempo non superiore a sei mesi, dei programmi utilizzati, o almeno alla valutazione degli impatti sull'aggiornamento.

Il **Responsabile del trattamento** adotta sistemi di back up, di continuità operative e disaster recovery e s'impegna a garantire che l'accesso in rete ai dati personali avvenga su canali sicuri o in forma criptata.

Il **Responsabile del trattamento** s'impegna a garantire l'accesso in rete ai dati personali e la comunicazione degli stessi avvenga su canali sicuri o in forma criptata (per esempio. HTTPS, SSH v2), salvo che sia diversamente richiesto e autorizzato dal **Titolare del trattamento**.

Il **Responsabile del trattamento** effettua test di penetrazione con cadenza periodica (quantomeno al rilascio di ogni major release), adotta un piano di miglioramento che

analizzi le vulnerabilità emerse dai VA e PT e dai bollettini di sicurezza pubblici e di fornitori terzi e ne preveda una adeguata gestione/risoluzione, svolgendo periodicamente test di vulnerabilità sugli applicativi messi a disposizione del Titolare.

Il **Responsabile del trattamento** assicura la separazione degli ambienti di test e sviluppo rispetto ad ambienti di produzione e la previsione di misure di accesso mediante credenziali e privilegi diversi in modo da ridurre al minimo i rischi.

Il **Responsabile del trattamento** può aggiornare o modificare le misure di sicurezza garantite al momento dell’Affidamento e/o stabilite nel decreto di incarico o atto successivo a condizione che tali aggiornamenti e modifiche non comportino il degrado della sicurezza complessiva dei servizi e dei sistemi, dandone comunicazione al **Titolare del trattamento**.

Il **Responsabile del trattamento** è tenuto, in caso di modifiche e di implementazioni di nuovi servizi o di regole afferenti ai dispositivi utilizzati nell’ambito dell’incarico richiamato nelle premesse, a condividere con il **Titolare del trattamento** le informazioni che abbiano rilievo sul trattamento dei dati personali ed è tenuto, prima di procedere alla messa in uso di tali implementazioni sui dati stessi a ottenerne l’autorizzazione scritta.

Salvo l’impegno del **Responsabile del trattamento** a fornire tutte le informazioni necessarie al **Titolare del trattamento** per rispettare la Normativa Privacy, gli interventi di modifica e le innovazioni necessarie per la sicurezza dei servizi telematici che non investono la fruizione del servizio e non modificano le modalità di trattamento dei dati né la tipologia dei dati trattati, come interventi sul codice e sulla gestione tecnica della infrastruttura, non sono soggetti a preventiva autorizzazione da parte del **Titolare del trattamento**.

Nello stesso modo, non necessitano di preventiva autorizzazione gli interventi urgenti per la sicurezza e la garanzia di continuità del servizio, per i quali il **Responsabile del trattamento** si impegna a fornire successivamente le informazioni sulle modifiche effettuate al Titolare.

Il **Responsabile del trattamento** garantisce di applicare le misure minime di sicurezza individuate nell’allegato A.2. e le altre misure di sicurezza definite nell’Affidamento.

Tra queste rientrano anche le misure di sicurezza definite nel Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale qualora l’applicativo utilizzato sia su Data Center del Responsabile, oppure su Data Center esterni resi disponibili da sub-fornitori del Responsabile.

Il **Responsabile del trattamento** è tenuto a fornire, su richiesta del **Titolare del trattamento**, informazioni di dettaglio sulle misure di sicurezza adottate in relazione al trattamento dei dati personali, secondo quanto previsto dal presente atto e dall’art. 32 del RGDP, nonché a documentare l’adozione delle stesse e la valutazione della loro idoneità ai sensi del già menzionato articolo e, in genere, della normativa Privacy.

Il **Responsabile del trattamento** è tenuto a predisporre e mettere a disposizione la documentazione degli strumenti utilizzati per trattare i dati (indicazione del DB utilizzato, strumento di scrittura del codice, sistema di conservazione dei documenti prodotti), definendo le misure di sicurezza poste a tutela dei dati (profili di accesso al DB, crittografia del DB, dialogo tra applicazione e DB e protezione delle password, ecc.).

Il **Responsabile del trattamento** è tenuto altresì a informare immediatamente il **Titolare del trattamento**, nel caso in cui riscontri carenze in relazione alla sicurezza del trattamento, nell'ambito delle verifiche sulle misure di sicurezza adottate nel trattamento dei dati personali, che il **Responsabile del trattamento** è tenuto a effettuare regolarmente.

Con riguardo ai trattamenti di dati personali svolti occasionalmente senza ausilio di strumenti elettronici e informatici, il **Responsabile del trattamento** se nel caso deve provvedere a che gli archivi fisici siano adeguatamente custoditi e l'accesso sia riservato solo ai soggetti autorizzati. Devono essere definite le procedure di deposito, custodia, consegna, restituzione e compartimentazione dei documenti contenenti dati personali e, in ragione della particolare natura dei dati personali, predisposti contenitori separati e serrati con appositi strumenti e definita una procedura di gestione delle chiavi.

### **Assistenza per l'utilizzo degli applicativi del Responsabile**

L'erogazione del servizio di assistenza e di accesso alle piattaforme da remoto devono avvenire mediante connessione VPN con MFA.

Le attività svolte dagli operatori con utenze privilegiate devono essere tracciate e monitorate.

Gli operatori incaricati dell'assistenza devono accertarsi che le richieste di assistenza provengano da un soggetto identificato e preventivamente autorizzato dal Titolare (ad esempio tramite autenticazione sulla piattaforma di ticketing).

Gli operatori incaricati dell'assistenza devono richiedere al Titolare in modo tracciabile le autorizzazioni necessarie ai fini dell'erogazione del servizio di assistenza (ad esempio, la condivisione dello schermo, il controllo condiviso dell'applicativo, il trasferimento dei file e la registrazione delle attività).

L'eventuale copia o trasferimento di archivi o base dati del Titolare per finalità di assistenza o manutenzione deve essere preventivamente ed espressamente autorizzata dal Titolare stesso.

I DB/archivi del Titolare devono essere conservati per il tempo strettamente necessario all'esecuzione dell'attività di assistenza e immediatamente cancellati qualora non più necessari per l'esecuzione delle operazioni di assistenza.

Le copie dei DB/archivi del Titolare prelevati per finalità di assistenza devono essere trasferite tramite canali sicuri e protetti, salvate in ambienti dotati delle opportune misure di sicurezza e non devono essere sottoposti a backup allo scopo di minimizzare il trattamento.

Qualora durante le attività di assistenza fosse necessario stampare documenti o informazioni, tali documenti devono rimanere nell'esclusiva disponibilità dell'operatore e da questi devono essere protetti contro accessi non autorizzati. Al termine dell'attività, i documenti dovranno essere distrutti.

Sono adottati processi e strumenti di assistenza che assicurino la tracciabilità degli interventi richiesti ed eseguiti (piattaforma di ticketing).

### **Operazioni da eseguire sui dati personali al termine dell'affidamento, anche anticipato**

In caso di revoca della designazione come **Responsabile del trattamento** oppure al termine dell'affidamento, anche anticipato per recesso o risoluzione, il **Responsabile del trattamento**, in accordo con il Titolare, è tenuto:

- alla restituzione completa dei dati personali di titolarità del Consiglio regionale, di cui abbia disponibilità;
- alla distruzione di eventuale documentazione contenente i dati personali di cui all'allegato A.1, salvo sia obbligatorio conservare alcuni documenti in ragione degli adempimenti amministrativi e contabili stabiliti dalla legge o di specifica richiesta da parte del Titolare del trattamento;
- alle altre operazioni richieste dal Titolare del trattamento stesso o previste dall'Affidamento, compresa la cancellazione dei dati personali di cui all'allegato A.1. dai supporti elettronici e informatici utilizzati con modalità che non ne consentano il recupero, in conformità al provvedimento del Garante per la protezione dei dati personali 13 ottobre 2008 in materia di rifiuti di apparecchiature elettriche ed elettroniche (RAEE) e misure di sicurezza dei dati personali.

In questo ambito risulta necessario procedere a: a) emanare adeguate istruzioni di comportamento a tutti i soggetti incaricati autorizzati al trattamento; b) effettuare una ricognizione completa di tutti i supporti di memoria che possano essere riutilizzabili (sia su parti di tipo asportabile sia di quelli presenti in aree di memoria interne al sistema operativo od in programmi), ove possano trovarsi dati; c) esaminare tutti i nuovi supporti, sistema operativo e programmi, che vengono inseriti nel sistema di trattamento dei dati, analizzando i possibili rischi ed impartendo specifiche istruzioni ai soggetti incaricati autorizzati al trattamento.

In caso di occasionali trattamenti svolti senza ausilio di strumenti elettronici e informatici, è necessario procedere con la triturazione del supporto al fine di non consentire l'identificazione degli interessati.

Delle operazioni di cancellazione compiute e degli obblighi di conservazione ulteriori, il **Responsabile del trattamento** è tenuto a rilasciare apposita dichiarazione scritta e firmata dal legale rappresentante al **Titolare del trattamento**.

Rimangono ferme le eventuali specificazioni definite nell'Affidamento.

### **Obblighi di informazione e collaborazione**

Il **Responsabile del trattamento** deve fornire la documentazione e le informazioni necessarie in relazione ai servizi svolti e alle misure di sicurezza applicate e dare l'assistenza necessaria per garantire il rispetto della Normativa privacy.

In particolare, il **Responsabile del trattamento** deve dare assistenza e collaborare, fornendo la documentazione e le informazioni necessarie anche con riguardo alle misure di sicurezza, nello svolgimento e nella redazione dei documenti relativi all'analisi del rischio per la protezione dei dati personali e alla valutazione di impatto sulla protezione dei dati personali (art. 32 e 35 RGPD), secondo le procedure di cui alla deliberazione dell'Ufficio di Presidenza 4.11.2019, n. 423 recante "Metodologia per l'analisi del rischio e la valutazione di impatto per la protezione dei dati personali da applicare ai trattamenti di dati personali del Consiglio regionale della Lombardia" e ss.mm.ii.

Il **Responsabile del trattamento**, ai sensi dell'art. 30, par. 2, del RGPD, salva la deroga di cui al medesimo articolo, tiene il registro delle attività relative al trattamento dei dati personali effettuate per conto del Titolare e, su richiesta, mette tale registro a disposizione del Titolare e/o del Garante per la protezione dei dati personali.

Il **Responsabile del trattamento** è comunque tenuto a fornire al Titolare le informazioni necessarie alla compilazione del "Registro delle attività di trattamento" e delle informative sul trattamento dei dati personali per gli interessati, come previsto dalla Normativa privacy, anche curando ogni necessario rapporto con gli eventuali sub responsabili e a mettere a disposizione del **Titolare del trattamento** le informazioni necessarie all'espletamento delle attività di revisione, comprese le ispezioni richieste dallo stesso **Titolare del trattamento** o da altro soggetto da esso autorizzato, al fine di rilevare il rispetto degli obblighi previsti dalla Normativa privacy e dal contenuto specifico dell'Affidamento del servizio richiamato nel presente Atto.

Il **Responsabile del trattamento** deve evadere tempestivamente le richieste del Titolare e impegnarsi alla collaborazione necessaria in modo da consentire l'esercizio dei diritti da parte degli interessati, richiamati dalla Normativa privacy. Nel caso in cui il **Responsabile del trattamento** riceva, da parte dell'interessato, un'istanza per l'esercizio dei suoi diritti ai sensi degli artt. da 15 a 22 RGPD è tenuto a inoltrarla prontamente al **Titolare del trattamento**.

Il Titolare provvederà a informare gli interessati ai sensi della Normativa privacy (articoli 13 e 14 RGPD); al fine di consentire tale attività, il **Responsabile del trattamento** deve fornire tutte le informazioni richieste dal Titolare.

Il **Responsabile del trattamento** deve collaborare attivamente con l'Autorità Garante per la Protezione dei dati personali e le Autorità Pubbliche, per consentire a queste ultime l'esercizio delle proprie attività istituzionali, quali richieste di informazioni, attività di controllo mediante accessi e ispezioni, relativamente ai trattamenti oggetto del presente Atto, informando immediatamente il Titolare di qualsiasi richiesta e/o comunicazione relativa ai dati personali pervenutagli dal Garante e da qualsiasi Autorità. Qualora il **Titolare** debba svolgere una revisione della valutazione del rischio ai sensi degli articoli 32 e 35 RGPD, il **Responsabile del trattamento** si impegna a fornire le informazioni necessarie anche in merito alle misure di sicurezza applicate.

Il **Responsabile del trattamento** è tenuto a redigere e rendere consultabile agli interessati sulla piattaforma web utilizzata per erogare il servizio le informazioni di cui agli articoli 13 e 14 RGPD in accordo con il Titolare del trattamento, fornendone copia previamente all'inizio dell'erogazione del servizio. Il testo definitivo comunque deve essere disponibile al momento dell'accesso agli applicativi utilizzati dal Responsabile del trattamento per erogare il servizio.

#### **Designazione di sub-responsabili (art. 28, par. 2 e 4, RGPD)**

Il **Responsabile del trattamento** ha la facoltà di ricorrere ad altri responsabili del trattamento di dati personali (sub - responsabili del trattamento) nell'ambito delle attività di trattamento di dati personali per conto del Consiglio regionale della Lombardia. Ai sensi dell'art. 28, par. 2, del RGPD, tale facoltà è da intendersi quale autorizzazione scritta generale da parte del Consiglio regionale della Lombardia,

**Titolare del trattamento**, nei confronti del **Responsabile del trattamento** per le attività sopra menzionate, salvo l'obbligo di comunicazione nei termini sotto specificati. Il **Responsabile del trattamento**, in sede di designazione di sub-Responsabili, deve informare il **Titolare del trattamento**, al fine di consentire, come previsto dall'art. 28 par. 2 RGPD, di poter manifestare eventuale formale opposizione a tale designazione entro e non oltre il termine di quindici giorni dalla ricezione della comunicazione; decorso il termine quest'ultima potrà procedere all'effettuazione delle designazioni nei confronti dei sub-responsabili del trattamento individuati.

In ogni caso, la designazione di un sub-responsabile del trattamento da parte del **Responsabile del trattamento** è possibile a condizione che su tale soggetto siano imposti gli stessi obblighi in materia di protezione dei dati contenuti nel presente Atto, incluse garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti richiesti dalla Normativa privacy e dal rischio correlato al trattamento e che sia la garanzia che il trattamento sia svolto nel territorio dell'Unione Europea o nel territorio di Paesi non appartenenti allo Spazio Economico Europeo ritenuti adeguati tramite decisione della Commissione europea ai sensi degli art. 45 e 46 del Regolamento UE 2016/679.

Il **Responsabile del trattamento** deve inviare al **Titolare del trattamento**, su richiesta di quest'ultimo, la documentazione relativa alla designazione del sub-responsabile del trattamento per l'esercizio delle prerogative stabilite dall'art. 28 RGPD.

Il **Responsabile del trattamento** rimane comunque interamente responsabile nei confronti del Consiglio regionale della Lombardia con riguardo all'adempimento degli obblighi in materia di protezione dei dati da parte del sub-responsabile del trattamento, ai sensi dell'art. 28, par. 4, RGPD ed è tenuto alla gestione di ogni rapporto con tale soggetto a garanzia della protezione dei dati personali di titolarità del Consiglio regionale e al rispetto della Normativa Privacy.

Il **Titolare del trattamento** può in qualsiasi momento verificare le garanzie e le misure tecniche e organizzative del sub-responsabile del trattamento, tramite audit e ispezioni, anche avvalendosi di soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti o inadeguate, il Titolare del trattamento può chiedere la presentazione di garanzie sufficienti entro un termine congruo.

Nel caso in cui all'esito delle verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inadeguate ad assicurare l'applicazione del RGPD o risulti che il sub-responsabile agisca in modo difforme o contrario alle istruzioni fornite dal Titolare del trattamento, quest'ultimo applicherà al **Responsabile del trattamento** le penali e le ulteriori conseguenze sul contratto previste nell'Affidamento e diffiderà lo stesso a far adottare al sub-responsabile del trattamento tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato.

Il **Responsabile del trattamento** garantisce che i dati personali non siano utilizzati dagli altri sub – responsabili per finalità non connesse allo svolgimento delle prestazioni di cui all'Affidamento, salvo che l'interessato non esprima, in autonomia e in aggiunta

a quanto previsto nel presente Atto, valido consenso agli ulteriori trattamenti nel rispetto della Normativa privacy e previa informativa.

Il **Responsabile del trattamento** è tenuto a fornire la DPIA o l'analisi dei rischi svolta sul servizio erogato, a richiesta del Titolare.

Il **Responsabile del trattamento** è tenuto ad informare il Titolare, mediante relazione scritta, di tutte le attività svolte in conformità a quanto previsto dal Contratto almeno una volta all'anno e, comunque, ogni qualvolta sia ritenuto necessario dal Titolare.

### **Gestione degli incidenti di sicurezza informatica e violazioni di dati personali (data breach)**

Il **Responsabile del trattamento** è tenuto ad adottare un piano di gestione degli incidenti di sicurezza, conforme alla Normativa Privacy e ai provvedimenti del Garante per la protezione dei dati personali.

Fermo quanto previsto nell'Affidamento, il **Responsabile del trattamento** è tenuto a comunicare al Titolare, senza ingiustificato ritardo, ogni violazione dei dati o di incidenti informatici o altro accadimento che possa aver comportato un impatto sui dati personali del Consiglio regionale della Lombardia, **Titolare del trattamento**, violandone la riservatezza, integrità, disponibilità o comunque esponendoli a rischio, secondo quanto richiesto dalla Normativa privacy vigente.

Il **Responsabile del trattamento** è dotato di un modello di comunicazione al **Titolare del trattamento** per i casi di violazione dei dati personali conforme alla Normativa Privacy e ai provvedimenti del Garante per la protezione dei dati personali.

La comunicazione deve contenere almeno le seguenti informazioni:

- i) la descrizione della natura del *data breach* compresi, ove possibile, le categorie e il numero approssimativo d'interessati colpiti dalla violazione nonché le categorie e il numero approssimativo di registrazioni dei dati personali oggetto della violazione;
- ii) il nome e i dati di contatto del responsabile per la protezione dei dati o di altro punto di contatto del responsabile, presso cui ottenere informazioni ulteriori;
- iii) la descrizione delle probabili conseguenze del *data breach*;
- iv) se del caso, tenendo conto della natura del trattamento, dei servizi e del contratto, la descrizione delle misure adottate dal responsabile o di quelle di cui propone l'adozione per porre rimedio al *data breach* ovvero attenuarne i possibili effetti negativi.

La comunicazione deve avvenire anche qualora la violazione sia solo presunta o esista un sospetto, pur in assenza di certezze.

La comunicazione deve essere rivolta al Dirigente dell'Ufficio Contratti e ICT all'indirizzo: [protocollo.generale@pec.consiglio.regione.lombardia.it](mailto:protocollo.generale@pec.consiglio.regione.lombardia.it) e [sistema.informativo@consiglio.regione.lombardia.it](mailto:sistema.informativo@consiglio.regione.lombardia.it), nonché per conoscenza all'indirizzo [rp@consiglio.regione.lombardia.it](mailto:rp@consiglio.regione.lombardia.it).

Eventuali modifiche o precisazioni sulla procedura possono essere oggetto di separato accordo con il Titolare del trattamento.

Le informazioni e i dati relativi alla violazione sono mantenuti riservati, fermi restando gli obblighi di notifica e comunicazione previsti dagli articoli 33 e 34 RGPD.

## **Luogo di trattamento e trasferimento di dati personali**

I dati personali trattati dal **Responsabile del trattamento** per l'erogazione dei servizi, di cui all'Affidamento, sono ubicati in architetture e storage dedicati o logicamente separati.

Il **Responsabile del trattamento** assicura che la porzione dedicata ai dati del Titolare del trattamento è ubicata nel territorio dell'Unione Europea o nel territorio di Paesi non appartenenti allo Spazio Economico Europeo ritenuti adeguati tramite decisione della Commissione europea ai sensi degli art. 45 e 46 del Regolamento UE 2016/679 presso data center in cui, compatibilmente alla tipologia, vengono eseguite le procedure automatizzate per l'eventuale conservazione, duplicazione, backup e ripristino dei dati.

Il **Responsabile del trattamento** assicura che il trasferimento dei dati personali trattati avvenga su canali sicuri o in forma criptata (per esempio: HTTPS, SSH v2).

Il **Responsabile del trattamento**, in assenza di una decisione della Commissione europea o di garanzie adeguate ai sensi degli artt. 45 e 46 del Regolamento UE 2016/679, non può:

- 1) trasferire i dati personali a un titolare del trattamento o a un responsabile del trattamento in un paese terzo o in un'organizzazione internazionale situati fuori dall'Unione europea;
- 2) trasferire il trattamento di dati personali a un sub - responsabile del trattamento in un paese terzo situato fuori dall'Unione europea;
- 3) far elaborare i dati personali dal responsabile del trattamento in un paese terzo situato fuori dall'Unione europea.

## **Obblighi del responsabile relativi all'infrastruttura cloud utilizzata per l'erogazione del servizio**

In caso di utilizzo di cloud per l'erogazione del servizio, il **Responsabile del trattamento** garantisce di utilizzare un'infrastruttura cloud conforme alle «best-practice» del settore e si impegna a adeguarla ovvero a mantenerla adeguata alle necessità dell'incarico stesso, garantendo il pieno rispetto degli obblighi e adempimenti previsti dalla normativa europea e italiana in materia.

Il **Responsabile del trattamento** garantisce in particolare di utilizzare un'infrastruttura cloud conforme ai requisiti minimi previsti dalle circolari AgID n. 2 e n. 3 del 2018.

## **ATTIVITÀ DI VIGILANZA E VERIFICA DEL TRATTAMENTO**

Per sorvegliare l'osservanza del presente Atto, il **Titolare del trattamento** può effettuare periodiche azioni di verifica. Tali verifiche possono comportare la richiesta di presentare informazioni, dati, documenti e compilazione di questionari di self-assessment (verifiche documentali) nonché l'effettuazione di test, per esempio di vulnerabilità, e l'accesso a locali o macchine e programmi del **Responsabile del trattamento**.

Per la risposta alle richieste di verifiche documentali, al **Responsabile del trattamento** deve essere concesso un termine di almeno 15 (quindici) giorni, salvo che la richiesta sia dovuta alla necessità di rispondere all'Autorità di controllo o all'Autorità giudiziaria.

In tali ultime ipotesi il **Responsabile del trattamento** deve garantire una risposta compatibile con gli obblighi del  **Titolare** nei confronti di tali Autorità.

Nell'ambito di tali verifiche il **Responsabile del trattamento** fornisce l'assistenza e il supporto necessario, rispondendo alle richieste del  **Titolare del trattamento** in relazione ai dati ed ai trattamenti di cui al presente Atto e non ha diritto a compensi aggiuntivi.

Nel caso in cui, all'esito delle verifiche, ispezioni e audit, le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inadeguate ad assicurare l'applicazione del RGPD o risulti che il **Responsabile del trattamento** agisca in modo difforme o contrario alle istruzioni fornite dal  **Titolare**, quest'ultimo applicherà al **Responsabile del trattamento** le penali e le ulteriori conseguenze sul contratto previste nella Convenzione e diffonderà lo stesso ad adottare tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato.

Il **Responsabile del trattamento** è tenuto ad informare su richiesta, e comunque almeno una volta all'anno, il Titolare, mediante relazione scritta, di tutte le attività svolte in conformità a quanto previsto dal Contratto e, comunque, ogni qualvolta sia ritenuto necessario dal Titolare.

## **INDIVIDUAZIONE DI MAGGIORI LIVELLI DI SICUREZZA E ADEGUAMENTI ALLA NORMATIVA PRIVACY SOPRAVVENUTA O A ESIGENZE CONTRATTUALI SOPRAVVENUTE**

Il  **Titolare del trattamento** può proporre al **Responsabile del trattamento** ogni variazione del presente Atto che sia necessaria per adempiere agli obblighi derivanti dalla Normativa Privacy o per tenere conto delle clausole tipo e dei codici di condotta eventualmente adottati ai sensi, rispettivamente, dell'articolo 28, par. 7 e 8, e dell'articolo 40 del RGPD o ai fini delle certificazioni di cui all'articolo 42.

Il **Responsabile del trattamento** e il  **Titolare del trattamento** concordano che provvederanno, se necessario, a integrare o modificare i contenuti del presente Atto in conformità alla Normativa privacy sopravvenuta. Eventuali ulteriori modifiche e integrazioni potranno altresì essere messe a punto in conseguenza degli esiti di nuove valutazioni sui rischi correlati al trattamento e in ragione di evoluzioni tecnologiche rilevanti o comunque per il miglior assolvimento delle prestazioni contrattuali. Il Responsabile del trattamento si impegna a collaborare nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse.

## **COMUNICAZIONI**

Le comunicazioni previste dal presente Atto nei confronti del  **Titolare del trattamento** devono essere trasmesse all'indirizzo di posta elettronica certificata del Consiglio regionale ([protocollo.generale@pec.consiglio.regione.lombardia.it](mailto:protocollo.generale@pec.consiglio.regione.lombardia.it)), all'attenzione del dirigente dell'Ufficio Comunicazione interna e formazione.

Il **Responsabile del trattamento** ha l'obbligo di comunicare al  **Titolare del trattamento** un indirizzo di posta elettronica certificata e gli altri recapiti ai quali inviare le comunicazioni previste dal presente Atto.

## DISPOSIZIONI FINALI

In conformità all'art. 82 e ss., il **Responsabile del trattamento** risponde di ogni perdita, costo, spesa, multa e/o sanzione, danno derivante da o in connessione con una qualsiasi violazione delle disposizioni della Convenzione, del decreto di incarico o altro atto, della normativa privacy e dei compiti e istruzioni di cui al presente Atto da parte sua, dei suoi dipendenti o collaboratori o degli eventuali altri responsabili del trattamento di sua designazione.

Il presente Atto e lo svolgimento degli obblighi e attività in esso previsti non comporta alcun diritto del **Responsabile del trattamento** a uno specifico compenso e/o indennità e/o rimborso.

Per le controversie relative al presente atto, si applicano le disposizioni previste nell'Affidamento.

Per tutto quanto non previsto espressamente nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

## DATI DI CONTATTO DEI RESPONSABILI DELLA PROTEZIONE DEI DATI PERSONALI (RPD)

Il RPD del Consiglio regionale della Lombardia è contattabile ai seguenti recapiti:  
[rpd@consiglio.regione.lombardia.it](mailto:rpd@consiglio.regione.lombardia.it) e  
[protocollo.generale@pec.consiglio.regione.lombardia.it](mailto:protocollo.generale@pec.consiglio.regione.lombardia.it).

Il **Responsabile del trattamento** ha l'obbligo di comunicare il nominativo e i dati di contatto del proprio Responsabile per la protezione dei dati personali (art. 37 e ss. del RGPD). Qualora il Fornitore non sia obbligato a nominare il Responsabile della protezione dei dati, sarà tenuto a mettere a disposizione uno specifico indirizzo di posta elettronica per le comunicazioni in materia di protezione dei dati personali.

Il **Responsabile del trattamento** e il **Titolare del trattamento** si danno reciproca informazione di eventuali modifiche relative ai propri Responsabili della protezione dei dati personali o referenti privacy.

## ALLEGATI

A.1 *“Elenco dei trattamenti dei dati personali di titolarità del Consiglio regionale della Lombardia affidati al Responsabile del trattamento”*

A.2 *“Elenco delle misure di sicurezza applicate dal Fornitore”*

per il **Consiglio regionale della Lombardia**

Il Dirigente pro tempore dell'Ufficio  
Contratti e ICT  
(firmato digitalmente)

per la società

il Legale Rappresentante

.....

(firmato digitalmente per accettazione)

**ALLEGATO A.1 - ELENCO DEI TRATTAMENTI DI DATI PERSONALI DI TITOLARITÀ DEL CONSIGLIO REGIONALE AFFIDATI AL FORNITORE IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO**

Ai sensi dell'art. 28 RGPD, il Responsabile del trattamento, nella persona del rappresentante legale *pro tempore*, è designato, per quanto sia necessario alla corretta esecuzione delle prestazioni contrattuali, quale responsabile del trattamento dei dati personali, per conto del Consiglio regionale della Lombardia, per i trattamenti e i dati personali indicati nella seguente tabella. Eventuali altri trattamenti di dati personali potranno essere eseguiti dal medesimo Responsabile del trattamento solo a seguito di comunicazione/richiesta scritta da parte del Titolare del trattamento.

| <b>Servizio affidato</b> | <b>Finalità e ambito dei trattamenti affidati al Responsabile</b> | <b>Modalità di trattamento e principali trattamenti svolti</b> | <b>Tipologia di dati trattati e categorie di interessati</b> | <b>Responsabile CRL di gestione del servizio e referente operativo CRL</b> |
|--------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------------------------------------|
|--------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------------------------------------|

|                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                        |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Corsi di formazione a catalogo erogati in modalità e-learning | <p><b>Finalità</b><br/>Fornire corsi di formazione e aggiornamento in modalità online per i dipendenti del Consiglio regionale in base alle norme di legge statale, regionale, alle disposizioni del CCNL applicabili alla fattispecie e al piano di formazione del Consiglio - Manutenzione - Garanzia della funzionalità e sicurezza e della conformità alle norme di legge - Garanzia della inalterabilità dei dati - Sicurezza e stabilità del portale di accesso alla piattaforma online - Conformità alle previsioni in materia di cookies</p> <p><b>Ambito del trattamento</b><br/>Erogazione del servizio mediante piattaforma web - Supporto e assistenza tecnica - Gestione amministrativa</p> | <p>Il trattamento è effettuato con l'ausilio di strumenti elettronici.<br/>Le operazioni di trattamento autorizzate sono:<br/> X  raccolta  _  registrazione  X  organizzazione  X  strutturazione  _  conservazione  _  adattamento  _  modifica  X  visualizzazione  _  estrazione  X  uso  _  comunicazione agli interessati e al Consiglio regionale  _  diffusione  _  raffronto  _  interconnessione  _  limitazione  X  cancellazione secondo le istruzioni del Titolare del trattamento  _  distruzione secondo le istruzioni del Titolare del trattamento  _  copia, duplicazione, riproduzione e registrazione solo su autorizzazione del Titolare del trattamento.<br/>La trasmissione dei dati personali è consentita solo su espressa autorizzazione del Titolare con modalità sicure (es. file criptati con password comunicata con altro canale).<br/>Le prestazioni comportano:<br/>- la predisposizione di misure di sicurezza applicativa per garantire integrità, stabilità e riservatezza dei dati personali;<br/>- attività tecniche e funzioni di amministratore di sistema;<br/>- connessione sicura HTTPS;<br/>- accesso ai servizi mediante dispositivi fissi;<br/>- download di materiale;</p> | <p>Dati personali comuni (nome, cognome, indirizzo di posta elettronica consiliare, esito del corso di formazione partecipazione, durata della formazione, orario di accesso, esito del corso di formazione)<br/>Credenziali di autenticazione<br/>Gestione di eventuali cookies generati dall'applicativo<br/>Dati di navigazione e log relativi all'utilizzo della piattaforma<br/>Interessati: dipendenti indicati dal Consiglio quali utenti finali del servizio.</p> | <p>Direttore dell'esecuzione: dirigente Ufficio Comunicazione interna e formazione</p> |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|

|  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |  |
|--|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|  |  | <ul style="list-style-type: none"> <li>- comunicazioni ed istruzioni tecniche ed operative per risoluzione di problemi o lo svolgimento dei corsi di formazione;</li> <li>- tracciamento accesso degli utenti con indicazione data ed orario di accesso (logged in) e di uscita (logged out), ip di accesso, cookie statistici, tentativi di accesso errati;</li> <li>- estrazione di documenti di monitoraggio sull'utilizzo della piattaforma da parte degli utenti;</li> <li>-autenticazione tramite accesso con proprie credenziali;</li> <li>- applicazione alle credenziali di autenticazione di metodi sicuri di cifratura che non ne consentano la visione in chiaro da parte di terzi.</li> <li>- la consultazione, elaborazione di attestati di partecipazione, conservazione per il periodo di 6 mesi dalla conclusione dell'affidamento;</li> <li>-rilascio attestati di partecipazione oppure di partecipazione e di profitto.</li> </ul> <p>Il Fornitore può assegnare a soggetti interni al Consiglio profilo SuperUser per entrare nella piattaforma di erogazione del servizio al fine di monitorare l'andamento della fruizione dei corsi di tutti gli utenti</p> <p>Estrazione in formato .csv dei nominativi di chi ha iniziato, ha terminato ed ha ottenuto l'attestato di profitto/frequenza o la trasmissione massiva degli attestati di partecipazione con modalità sicura (cifrata/protezione con password).</p> |  |  |
|--|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|

|  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  |  |
|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|  |  | <p>Sono escluse attività di profilazione degli utenti.</p> <p>Le prestazioni possono essere effettuate presso la sede del Consiglio ovvero da remoto utilizzando un collegamento crittografato VPN mediante utenza di autenticazione fornita dal Consiglio regionale.</p> <p>I dati non possono essere utilizzati per altri scopi (salvo se anonimizzati).</p> <p>Il sistema di gestione del processo di controllo utenti/accessi deve avvenire nel rispetto dei principi di sicurezza informatica, per confermare che gli utenti siano chi dicono di essere e che abbiano il diritto di accedere in base a criteri di accesso e identità concordati con il Titolare.</p> <p>Il sistema finale di auditing e monitoraggio del servizio può comportare il trattamento esclusivamente di dati non riconducibili agli interessati.</p> <p>Conservazione</p> <p>Per i log, cookies e dati di navigazione: massimo sei mesi.</p> <p>Per gli altri dati: il Responsabile provvede alla cancellazione dei dati personali decorso un mese dalla conclusione dell'affidamento, salvo con riferimento agli attestati (6 mesi) o diversa istruzione del Titolare e salvo che il diritto dell'Unione o degli Stati membri, cui è soggetto il Responsabile, prescriva la conservazione dei dati personali. Il</p> |  |  |
|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|

|  |  |                                                                                                                                                                                                                                                                                                                                                  |  |  |
|--|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|  |  | Responsabile garantisce l'integrale trasferimento dei dati contenuti nei sistemi e supporti utilizzati per il trattamento al Titolare o a terzi da questi indicati con modalità e organizzazione tali da consentirne il trattamento secondo le modalità previste per l'erogazione del servizio oggetto dell'incarico e protetti da crittografia. |  |  |
|--|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|

## ALLEGATO A.2 - ELENCO DELLE MISURE DI SICUREZZA

Fermo quanto stabilito con riguardo a specifiche misure di sicurezza nell'Atto di designazione o definito in altro atto contrattuale con il Titolare, il **Responsabile del trattamento** nell'ambito delle attività previste contrattualmente garantisce di applicare le seguenti misure di sicurezza:

| Sicurezza applicativa      |                                                                                                                                                                                                                                                 |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Barrare le misure adottate | Misure di sicurezza                                                                                                                                                                                                                             |
| X                          | gestione di più profili con privilegi diversi                                                                                                                                                                                                   |
| X                          | utilizzo credenziali uninominali                                                                                                                                                                                                                |
| X                          | autenticazione delle utenze username/password                                                                                                                                                                                                   |
| X                          | utilizzo di password sicure (almeno quattordici caratteri alfanumerici)                                                                                                                                                                         |
| X                          | cambio periodico delle password (almeno ogni sei mesi)                                                                                                                                                                                          |
| _                          | autenticazione utenze multifattore                                                                                                                                                                                                              |
| _                          | utilizzo di protocolli di autenticazione (ad esempio RADIUS, IEEE 802.1X, ecc.)                                                                                                                                                                 |
| X                          | supporto di protocolli sicuri e cifrati (HTTPS, SSH v2, ecc.)                                                                                                                                                                                   |
| X                          | ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL)                                                                                               |
| X                          | Messaggi di posta elettronica inviati devono essere crittografati tramite protocolli crittografici (TLS / SSL)                                                                                                                                  |
| _                          | utilizzo di meccanismi di autenticazione basati su crittografia asimmetrica, a chiave pubblica, fornita dal Fornitore, con lunghezza basata sulla criticità della comunicazione (es. 256 bit per le meno critiche, 512 bit per le più critiche) |
| X                          | profili di autorizzazione differenziati tra gli utenti                                                                                                                                                                                          |
| X                          | funzionalità di "richiesta creazione o cambio della password al primo accesso"                                                                                                                                                                  |
| X                          | blocco dell'utenza dopo un numero definito (fisso o variabile) di tentativi falliti di accesso                                                                                                                                                  |
| X                          | accessi utenti registrati su un archivio (log) non cancellabile con il reset                                                                                                                                                                    |
| X                          | gestione dei log di sistema (accessi, allarmi, ecc.)                                                                                                                                                                                            |
| _                          | mascheratura della base dati                                                                                                                                                                                                                    |
| X                          | Encryption/cifratura                                                                                                                                                                                                                            |

| <b>Barrare le misure adottate</b> | <b>Misure di sicurezza</b>                                                                                                                      |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| _                                 | cifratura delle comunicazioni tra la componente di gestione remota centralizzata e la componente locale installata presso la sede dell'ente     |
| X                                 | tracciatura delle accessi                                                                                                                       |
| X                                 | tracciatura delle modifiche                                                                                                                     |
| X                                 | protezione dei dati estratti                                                                                                                    |
| X                                 | validazione dei dati in input                                                                                                                   |
| X                                 | protezione delle comunicazioni client/server                                                                                                    |
| _                                 | archivi separati tra dati generici e dati particolari (sensibili e/o giudiziari)                                                                |
| X                                 | aggiornamento periodico software utilizzati                                                                                                     |
| X                                 | utilizzo di programmi contro il rischio di intrusione e accesso abusivo                                                                         |
| X                                 | utilizzo di programmi antivirus                                                                                                                 |
| _                                 | cancellazione dati di navigazione                                                                                                               |
| _                                 | anonimizzazione dati di navigazione                                                                                                             |
| _                                 | filtraggio di indirizzi IP                                                                                                                      |
| X                                 | vulnerability assessment                                                                                                                        |
| _                                 | utilizzo per l'accesso a internet di un proxy centralizzato e dotato di configurazione coerente con la politica di sicurezza definita dall'ente |
| _                                 | rispetto della politica di sicurezza dell'ente                                                                                                  |
| _                                 | definizione delle specifiche di sicurezza applicate                                                                                             |
| _                                 | implementazione delle specifiche di sicurezza nel codice e nella struttura della basedati                                                       |
| X                                 | condivisione della documentazione per gestire il servizio                                                                                       |
| _                                 | Altro                                                                                                                                           |

#### Sicurezza infrastrutturale

| <b>Barrare le misure adottate</b> | <b>Misura di sicurezza</b>                                                                                                        |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| X                                 | gestione di più profili con privilegi diversi                                                                                     |
| X                                 | utilizzo credenziali uninominali per quanto attiene le componenti infrastrutturali di competenza del responsabile del trattamento |

| <b>Barrare le misure adottate</b> | <b>Misura di sicurezza</b>                                                                                                                                                                                                                      |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b> X </b>                        | gli utenti non devono essere in grado di disattivare o bypassare le impostazioni di sicurezza                                                                                                                                                   |
| <b> X </b>                        | autenticazione delle utenze username/password                                                                                                                                                                                                   |
| <b> X </b>                        | utilizzo di password sicure (almeno quattordici caratteri alfanumerici)                                                                                                                                                                         |
| <b> _ </b>                        | autenticazione utenze multifattore                                                                                                                                                                                                              |
| <b> X </b>                        | utilizzo di protocolli di autenticazione (ad esempio RADIUS, IEEE 802.1X, ecc.)                                                                                                                                                                 |
| <b> X </b>                        | uso di protocolli sicuri e cifrati (HTTPS, SSH v2, ecc.)                                                                                                                                                                                        |
| <b> _ </b>                        | utilizzo di meccanismi di autenticazione basati su crittografia asimmetrica, a chiave pubblica, fornita dal Fornitore, con lunghezza basata sulla criticità della comunicazione (es. 256 bit per le meno critiche, 512 bit per le più critiche) |
| <b> X </b>                        | profili di autorizzazione differenziati tra gli utenti                                                                                                                                                                                          |
| <b> X </b>                        | funzionalità di “richiesta creazione o cambio della password al primo accesso”                                                                                                                                                                  |
| <b> X </b>                        | blocco dell'utenza dopo un numero definito (fisso o variabile) di tentativi falliti di accesso                                                                                                                                                  |
| <b> X </b>                        | accessi utenti registrati su un archivio (log) non cancellabile con il reset                                                                                                                                                                    |
| <b> X </b>                        | gestione dei log di sistema (accessi, allarmi, ecc.)                                                                                                                                                                                            |
| <b> X </b>                        | programma di backup dei dati                                                                                                                                                                                                                    |
| <b> X </b>                        | programma di backup delle configurazioni                                                                                                                                                                                                        |
| <b> X </b>                        | protezione/cifratura dei backup                                                                                                                                                                                                                 |
| <b> _ </b>                        | archiviazione separata dati comuni e dati particolari (sensibili e/o giudiziari)                                                                                                                                                                |
| <b> X </b>                        | programma di test dei restore                                                                                                                                                                                                                   |
| <b> X </b>                        | protezione da malware                                                                                                                                                                                                                           |
| <b> X </b>                        | le applicazioni antivirus e le firme di rilevamento devono essere aggiornate almeno su base settimanale                                                                                                                                         |
| <b> X </b>                        | protezione/cifratura delle linee di comunicazione                                                                                                                                                                                               |
| <b> _ </b>                        | cifratura delle comunicazioni tra la componente di gestione remota centralizzata e la componente locale installata presso la sede dell'ente                                                                                                     |
| <b> _ </b>                        | isolamento della rete da altri sistemi                                                                                                                                                                                                          |
| <b> X </b>                        | protezione del traffico tramite Intrusion Detection System                                                                                                                                                                                      |
| <b> X </b>                        | protezione del traffico tramite Instrusion Prevention System                                                                                                                                                                                    |

| <b>Barrare le misure adottate</b> | <b>Misura di sicurezza</b>                                                                                                                    |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b> X </b>                        | protezione del traffico tramite Web Application Firewall                                                                                      |
| <b> X </b>                        | protezione/cifratura del file system                                                                                                          |
| <b> X </b>                        | attivazione delle restrizioni di accesso sul file system                                                                                      |
| <b> X </b>                        | tracciatura degli accessi amministrativi                                                                                                      |
| <b> _ </b>                        | tracciatura delle attività amministrative                                                                                                     |
| <b> X </b>                        | tracciatura degli accessi al database                                                                                                         |
| <b> _ </b>                        | tracciatura degli accessi a file system                                                                                                       |
| <b> X </b>                        | raccolta centralizzata log                                                                                                                    |
| <b> _ </b>                        | utilizzo per l'accesso a internet di un proxy centralizzato e dotato di configurazione coerente con la politica di sicurezza definita dal CRL |
| <b> X </b>                        | programma di protezione dischi rimovibili                                                                                                     |
| <b> _ </b>                        | programma di controllo piattaforma software                                                                                                   |
| <b> X </b>                        | soluzione di disaster recovery                                                                                                                |
| <b> _ </b>                        | soluzione dlp applicata al contesto                                                                                                           |
| <b> X </b>                        | dismissione supporti di archiviazione già utilizzati                                                                                          |
| <b> X </b>                        | gestione supporti di archiviazione dismessi                                                                                                   |
| <b> X </b>                        | verifica annuale dell'operato degli amministratori                                                                                            |
| <b> X </b>                        | aggiornamento delle soluzioni e dei servizi di sicurezza e adeguamento alle normative UE o nazionali senza costi aggiuntivi                   |
| <b> _ </b>                        | presenza di un SOC del fornitore                                                                                                              |
| <b> X </b>                        | dispositivi di sicurezza perimetrale su reti del Fornitore (es. Firewall, sistemi di Network Detection ed Event & Log Monitoring, SIEM, ecc.) |
| <b> X </b>                        | gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente              |
| <b> _ </b>                        | Altro                                                                                                                                         |

**Sicurezza fisica per i trattamenti su supporti non elettronici se occasionalmente svolti**

| <b>Barrare le misure adottate</b> | <b>Misura di sicurezza</b>                               |
|-----------------------------------|----------------------------------------------------------|
| <b> X </b>                        | limitazione di accesso ai locali deputati al trattamento |

| <b>Barrare le misure adottate</b> | <b>Misura di sicurezza</b>                                                                            |
|-----------------------------------|-------------------------------------------------------------------------------------------------------|
| _                                 | profilazione degli accessi in base a ruolo                                                            |
| _                                 | utilizzo tessere di accesso uninominali limitazione di accesso agli archivi cartacei                  |
| X                                 | limitazione di accesso agli archivi cartacei                                                          |
| X                                 | archiviazione cartacea distinta per livello di severità                                               |
| _                                 | tracciatura degli accessi ai repository di dati cartacei                                              |
| _                                 | tracciatura degli accessi ai locali                                                                   |
| X                                 | presenza di sistemi antieffrazione                                                                    |
| X                                 | videosorveglianza locali                                                                              |
| X                                 | movimentazione materiali in modalità sicura                                                           |
| X                                 | sigillatura contenitori movimentati                                                                   |
| X                                 | Triturazione della documentazione cartacea contenente dati personali                                  |
| X                                 | Definizione di regole per la cancellazione sicura dei dati (es. Modello basato sulla norma DIN 66398) |
| _                                 | Altro                                                                                                 |

### Sicurezza Organizzativa

| <b>Barrare le misure adottate</b> | <b>Misure di sicurezza</b>                                                                                                                                               |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| X                                 | formazione privacy del personale                                                                                                                                         |
| X                                 | definizione di procedure per assicurare la segretezza                                                                                                                    |
| X                                 | definizione di un elenco dei dipendenti che saranno impiegati sul singolo progetto e sottoscrizione per ogni dipendente di dichiarazioni di riservatezza/confidenzialità |
| X                                 | nomina referente privacy                                                                                                                                                 |
| X                                 | nomina incaricati del trattamento                                                                                                                                        |
| _                                 | presenza dpo                                                                                                                                                             |
| X                                 | definizione di una procedura di data breach                                                                                                                              |
| X                                 | struttura per la prevenzione e gestione degli incidenti informatici                                                                                                      |
| X                                 | procedura di ripristino dei dati in caso di incidente fisico o tecnico                                                                                                   |

| Barrare le misure adottate          | Misure di sicurezza                                                                                                                                                                                                    |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> | consegna, entro il giorno successivo, di un report sugli incidenti di sicurezza avvenuti contenente: tipologia di attacco subito, vulnerabilità sfruttate, sequenza temporale degli eventi e contromisure adottate     |
| <input type="checkbox"/>            | adozione delle procedure e politiche di sicurezza definite dall'ente                                                                                                                                                   |
| <input type="checkbox"/>            | possesso della certificazione ISO/IEC 27001 o, in assenza, di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di un piano di qualità secondo lo standard ISO 10005                                    |
| <input type="checkbox"/>            | piano di auditing annuale sul sistema di sicurezza da parte di società specializzata, approvata dall'ente                                                                                                              |
| <input checked="" type="checkbox"/> | possibilità di auditing a richiesta dell'ente                                                                                                                                                                          |
| <input type="checkbox"/>            | possibilità di verifiche di conformità dei servizi da parte dell'ente                                                                                                                                                  |
| <input type="checkbox"/>            | possesso di certificazioni di sicurezza da parte del personale                                                                                                                                                         |
| <input type="checkbox"/>            | consegna, entro il giorno successivo alla richiesta, dei log di sistema generati dai dispositivi di sicurezza utilizzati, almeno in formato CSV o TXT                                                                  |
| <input checked="" type="checkbox"/> | condivisione della documentazione tecnica (schede tecniche, manuali, guide operative) per la corretta configurazione e gestione degli aspetti di sicurezza                                                             |
| <input checked="" type="checkbox"/> | dichiarazione di conformità alla normativa vigente in materia di sicurezza cibernetica e al GDPR                                                                                                                       |
| <input checked="" type="checkbox"/> | spese per il ripristino della situazione preattacco informatico a carico del Fornitore                                                                                                                                 |
| <input checked="" type="checkbox"/> | utilizzo, previa autorizzazione, di repliche dei dati dell'ente solo nel territorio dell'UE                                                                                                                            |
| <input type="checkbox"/>            | dichiarazione di disponibilità a far parte di un Comitato di Direzione Tecnica                                                                                                                                         |
| <input checked="" type="checkbox"/> | disponibilità alla sottoscrizione di clausola di non divulgazione                                                                                                                                                      |
| <input checked="" type="checkbox"/> | gestione di vulnerabilità scoperte sui prodotti oggetto della fornitura senza costi aggiuntivi                                                                                                                         |
| <input checked="" type="checkbox"/> | monitoraggio e valutazione continua sulla pubblicazione di upgrade/patch/hotfix necessari a risolvere eventuali vulnerabilità presenti nei dispositivi utilizzati per erogare i servizi e nelle infrastrutture gestite |
| <input type="checkbox"/>            | descrizione dettagliata della soluzione tecniche applicate (dispositivi hardware e software impiegato, modalità operative, politiche di sicurezza)                                                                     |
| <input type="checkbox"/>            | Altro                                                                                                                                                                                                                  |

Nei casi in cui si evidenziasse una non piena corrispondenza tra la tipologia di trattamento prevista per l'esecuzione del servizio e le misure di sicurezza richieste, il **Responsabile del trattamento** s'impegna a comunicarlo per scritto al Titolare, fornendo al medesimo l'effettuata analisi del rischio e indicando le misure di sicurezza ritenute adeguate.