

SCHEMI TIPO MODULISTICA

SCHEMA A⁽²⁾
(art. 474, c. 3)

ADDENDUM AL CONTRATTO DI LAVORO

CONFERIMENTO DI COMPITI E FUNZIONI IN QUALITÀ DI SOGGETTO DESIGNATO AI SENSI DELL'ARTICOLO 2 QUATERDECIES DEL D.LGS. 196/2003 (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.) E SUCCESSIVE MODIFICAZIONI. ISTRUZIONI PER L'ESERCIZIO DELLE FUNZIONI CONFERITE.

PREMESSO CHE

L'articolo 474, comma 3, del regolamento regionale 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale) e successive modificazioni:

- a) stabilisce che la Giunta regionale, in qualità di titolare o di Responsabile del trattamento può prevedere, ai sensi dell'articolo 2 quaterdecies del d.lgs. 196/2003 e successive modificazioni, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano conferiti a persone fisiche che operano sotto la propria autorità, espressamente designate secondo lo schema "A" dell'allegato "NN" al r.r. 1/2002, da allegare quale addendum al contratto di lavoro;
- b) individua come soggetti designati di diritto il Capo di Gabinetto, il Direttore Generale, i Direttori regionali, i Direttori delle Agenzie regionali, l'Avvocato coordinatore e il dirigente cui è attribuita la competenza relativamente alle funzioni previste dal decreto legislativo 6 settembre 1989, n. 322 (Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'art. 24 della legge 23 agosto 1988, n. 400) e alle convenzioni con l'ISTAT per l'attuazione del Programma Statistico Nazionale;

L'articolo 474, comma 7 bis, del r.r. 1/2002 e successive modificazioni stabilisce che la Giunta regionale, per mezzo dei soggetti designati, agisce in qualità di Responsabile del trattamento ai sensi dell'articolo 4, n. 8) del RGPD.

¹ Allegato inserito dall'art. 6, comma 1, del r.r.2 novembre 2020, n.27, pubblicato sul BUR Lazio 3 novembre 2020, n.132

² Schema sostituito dall'articolo 35, comma 1, del r.r. 11 aprile 2024, n. 4, pubblicato sul Supplemento n. 1 del BUR Lazio 11 aprile 2024, n. 30

VISTO l'articolo 2-quaterdecies del d. lgs. 196/2003 e successive modificazioni, il quale dispone che *“il Titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità”*;

VISTO il decreto legislativo 30 marzo 2001, n. 165 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche) e successive modificazioni;

VISTO 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), che garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento al diritto di protezione dei dati personali;

ATTESO che le soluzioni tecniche e organizzative relative al trattamento dei dati personali richiedono alla Regione un costante monitoraggio e che tali misure, periodicamente riesaminate ed aggiornate, qualora necessario, devono tener conto dello stato dell'arte e dei costi di attuazione, oltre che della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso;

ATTESO che il titolare del trattamento è tenuto a mettere in atto misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati, quali la pseudonimizzazione, la minimizzazione e anche ad integrare, nel trattamento, le necessarie garanzie al fine di soddisfare i requisiti del suddetto regolamento e tutelare i diritti degli interessati alla riservatezza ed all'adeguato trattamento dei dati personali e che è tenuto, altresì, a mettere in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;

CONSIDERATO che i suddetti obblighi valgono per la quantità dei dati personali raccolti, per la portata del trattamento, per il periodo di conservazione e l'accessibilità e che le misure da adottare devono garantire che, per impostazione predefinita, non siano resi accessibili dati personali ad un numero indefinito di persone fisiche senza l'intervento della persona fisica;

CONSIDERATO che ai fini del RGPD per “trattamento” si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (articolo 4, n. 2) del RGPD);

TENUTO CONTO che, ai sensi dell'articolo 24 del RGPD, il Titolare del trattamento è tenuto a mettere in atto le misure, tecniche ed organizzative, adeguate per garantire ed essere in grado di dimostrare che il trattamento sia effettuato conformemente al RGPD;

TENUTO CONTO che l'articolo 29 del RGPD stabilisce la regola generale per cui *“chiunque agisca sotto l'autorità del responsabile del trattamento o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri”*;

DATO ATTO che il <indicare nome e cognome> in qualità di Capo di Gabinetto/Avvocato coordinatore/Direttore <indicare nome della Direzione>/dirigente responsabile <indicare nome dell'Area competente in materia di statistica> è, secondo quanto disposto dall'articolo 474, comma 3, del r.r. 1/2002 e successive modificazioni, soggetto designato al trattamento dei dati ai sensi e per gli effetti di cui all'articolo 2-quaterdecies del d.lgs. 196/2003 e successive modificazioni;

RITENUTO che il <indicare nome e cognome> in qualità di Capo di Gabinetto/Avvocato coordinatore/Direttore<indicare nome della Direzione>/dirigente responsabile <indicare nome dell'Area competente in materia di statistica>, per l'ambito di attribuzioni, funzioni e competenze conferite, abbia le garanzie sufficienti per mettere in atto tutte le misure tecniche ed organizzative adeguate a soddisfare i requisiti del RGPD e garantire la tutela dei diritti degli interessati;

Tutto ciò premesso

SI CONVIENE QUANTO SEGUE

Art. 1

(Obblighi del soggetto designato)

1. Il <indicare nome e cognome>, quale soggetto designato al trattamento dei dati ai sensi dell'articolo 2 *quaterdecies* del d.lgs. 196/2003 e successive modificazioni e dell'articolo 474, comma 3, del r.r. 1/2002 e successive modificazioni, svolge i compiti e assume le responsabilità previste dalle disposizioni vigenti in materia di trattamento di dati personali e osserva scrupolosamente quanto in esse previsto, nonché le istruzioni che seguono.

Art. 2

(Istruzioni per il trattamento dei dati personali)

1. Il <indicare nome e cognome>, Soggetto designato, nell'ambito delle sue funzioni, presiede ai trattamenti di dati personali di competenza della <indicare i riferimenti della struttura di afferenza>, la cui elencazione e descrizione è riportata nel "Registro delle attività di Trattamento" di cui all'articolo 30 del RGPD, attenendosi al rispetto delle seguenti **istruzioni**:
 - a) i trattamenti devono essere svolti nel pieno rispetto delle previsioni normative vigenti in materia di protezione dei dati personali, nonché tenendo conto dei provvedimenti e dei comunicati ufficiali emessi dall'Autorità Garante per la Protezione dei Dati Personali, di seguito denominata Garante;
 - b) ciascun trattamento deve avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento; deve pertanto essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi;
 - c) il soggetto designato dovrà evitare che i dati personali siano soggetti a rischi di perdita o distruzione anche accidentale, che ai dati possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini istituzionali per i quali i dati sono stati raccolti e per i quali vengono trattati;
 - d) in ogni fase del trattamento non si possono eseguire operazioni per fini non previsti tra i compiti assegnati e si potrà accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere tali compiti;
 - e) la raccolta dei dati personali e la loro successiva registrazione devono avvenire per il solo perseguimento delle finalità istituzionali della Regione e, comunque, per scopi:
 - 1) *determinati*, pertanto non è consentita la raccolta come attività fine a sé stessa;
 - 2) *espliciti*, quindi il soggetto interessato deve essere informato sulle finalità del trattamento;
 - 3) *legittimi*, pertanto, oltre al trattamento, anche il fine della raccolta dei dati deve essere lecito;
 - f) i dati personali trattati sono: dati genericamente di natura personale (articolo 4, n. 1), del RGPD); dati sensibili (articolo 9 del RGPD "Categorie particolari di dati personali"); dati giudiziari (articolo 10 del RGPD);
 - g) le categorie di interessati sono quelle identificate nelle parti di competenza della <indicare i riferimenti della struttura di afferenza> del "Registro delle attività di Trattamento" di cui all'articolo 30 del RGPD;
 - h) le operazioni di trattamento nell'ambito della struttura di competenza, dovranno essere

organizzate in conformità con la normativa in materia di protezione dei dati personali applicabile ed in osservanza delle eventuali indicazioni scritte impartite dalla Regione, assicurando l'applicazione del principio della protezione dei dati fin dalla progettazione e protezione predefinita di cui all'articolo 25 del RGPD, determinando i mezzi del trattamento e mettendo in atto le misure tecniche e organizzative adeguate, di cui all'articolo 32 del RGPD, prima dell'inizio delle attività. Inoltre, dovrà essere adottata ogni misura adeguata, fisica e logica, atta a garantire che i dati personali siano trattati in ossequio al principio di necessità e che siano trattati solamente per le finalità previste e per il tempo strettamente necessario al raggiungimento delle stesse (privacy by default);

- i) in veste di soggetto designato al trattamento dei dati personali, dovrà collaborare con il Titolare del trattamento affinché siano garantiti tutti i diritti dell'interessato di cui al Capo III del RGPD. In particolare, dovrà attenersi ad ogni istruzione scritta impartita al riguardo dal Titolare;
- j) dovranno essere rese disponibili al Titolare del trattamento, tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti previsti dalla normativa in materia di protezione dei dati personali relativamente alla struttura di competenza, consentendo di effettuare periodicamente attività di verifica, comprese ispezioni realizzate dal Titolare stesso, dal Responsabile della Protezione dei Dati o da un altro soggetto incaricato;
- k) informare il Titolare del trattamento ed il Responsabile della Protezione dei Dati personali, qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti;
- l) i dati devono, inoltre, essere:
 - 1) *esatti*, cioè precisi e rispondenti al vero e, se necessario, aggiornati;
 - 2) *pertinenti*, ovvero il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
 - 3) *completi*: idonei a contemplare specificamente il concreto interesse e diritto del soggetto interessato (da non intendersi nel senso di raccogliere il maggior numero di informazioni possibili);
 - 4) *non eccedenti* in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;
 - 5) *conservati per un periodo non superiore a quello necessario* per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita;
- m) se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dalla normativa vigente in materia di protezione dei dati personali, è necessario provvedere, previa comunicazione al Responsabile della Protezione dei Dati (DPO) della Regione, al blocco dei dati stessi, ossia alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento, fornendo, ad esempio, l'informativa omessa, ovvero provvedendo alla cancellazione dei dati se non è possibile procedere alla regolarizzazione.

2. In conformità alla normativa vigente in materia di protezione dei dati personali ed in osservanza delle eventuali indicazioni scritte impartite al riguardo dal Titolare del trattamento, dovrà:
- a) individuare e, se presenti, designare le persone autorizzate al trattamento, detti incaricati, che prestano la propria attività all'interno della struttura di propria competenza;
 - b) controllare l'operato degli incaricati al trattamento, nonché sensibilizzare gli stessi sugli aspetti normativi ed organizzativi in materia di tutela dei dati personali;
 - c) garantire che i profili di accesso ai sistemi informativi da parte degli incaricati al trattamento siano configurati anteriormente all'inizio del trattamento, nonché verificare, almeno una volta l'anno, che tali profili siano conformi con le mansioni svolte. In caso di sospensione dall'attività lavorativa o revoca/esclusione dall'incarico dovrà essere comunicato alle strutture competenti la necessità di procedere alla disattivazione dell'utenza;
 - d) assicurare, all'interno della propria struttura, il pieno rispetto degli adempimenti formali nei modi e nei tempi previsti dalla normativa vigente, tra i quali la predisposizione e il rilascio di informative e la gestione dei diritti degli interessati;
 - e) collaborare con il Garante in caso di ispezioni, al fine di fornire informazioni, documenti e ogni facilitazione di accesso alle banche dati inerenti all'Ufficio di competenza;
 - f) collaborare nelle verifiche predisposte dal DPO, al fine di fornire informazioni, documenti e ogni facilitazione di accesso alle banche dati;
 - g) informare prontamente il DPO di ogni questione rilevante in base alla normativa sulla protezione dei dati personali, come la presentazione di eventuali istanze inerenti all'esercizio dei diritti degli interessati ai sensi degli articoli da 15 a 22 del RGPD;
 - h) informare tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il DPO di ogni violazione di dati personali (cosiddetto data breach) entro 24 ore dall'avvenuta conoscenza dell'evento. In ogni caso, l'informativa deve essere accompagnata da ogni documentazione utile, per permettere al Titolare, ove ritenuto necessario, di notificare tale violazione al Garante e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando ne è venuto a conoscenza, ai sensi degli articoli 33 e 34 del RGPD;
 - i) nel caso in cui il Titolare debba fornire informazioni aggiuntive al Garante, supportare il Titolare stesso nella misura in cui le informazioni richieste e/o necessarie per il Garante siano esclusivamente in possesso del soggetto designato;
 - l) collaborare, per la struttura di propria competenza, alla redazione ed aggiornamento del Registro delle attività di trattamento di cui all'articolo 30 del RGPD, cooperando con il Titolare e con il Garante, laddove ne venga fatta richiesta ai sensi dell'articolo 30, paragrafo 4, del RGPD;
 - m) collaborare per i trattamenti della struttura di competenza e, unitamente al DPO, allo svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente a quanto prescritto dall'articolo 35 del RGPD e nella eventuale consultazione del Garante, prevista ai sensi dell'articolo 36 del RGPD;
 - n) garantire che la protezione dei dati personali all'interno della struttura di propria competenza sia realizzata in base alle misure di sicurezza previste dall'articolo 32 del RGPD idonee a ridurre al minimo i rischi di divulgazione, distruzione, perdita o modifica anche accidentale o illegale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
 - o) collaborare, in caso di modifica della normativa in materia di protezione dei dati personali e nei limiti delle proprie competenze tecniche/organizzative e delle proprie risorse, con il Titolare e con il DPO, affinché siano sviluppate, adottate ed implementate misure correttive di adeguamento ai nuovi requisiti introdotti;
 - p) proporre al Titolare la designazione di eventuali ulteriori responsabili del trattamento individuati in conformità alle relative disposizioni del RGPD;

q) designare gli amministratori di sistema della struttura di appartenenza, nel rispetto di quanto previsto dal Provvedimento del Garante della Protezione dei dati Personali 27 novembre 2008 (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema) nonché degli ulteriori criteri e modalità definiti dall'allegato "LL" al r.r. 1/2002 e successive modificazioni e darne comunicazione alla direzione regionale competente in materia di sistemi informativi.

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

Luogo e data:

IL TITOLARE DEL TRATTAMENTO

Per accettazione Luogo e data

IL SOGGETTO DESIGNATO

NOMINA SOGGETTI INCARICATI

(INTESTAZIONE DELLA STRUTTURA)

Oggetto: Nomina del soggetto incaricato al trattamento di dati personali ai sensi dell'articolo 474, comma 5, del r. r. 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale) e successive modificazioni e degli articoli 28, paragrafo 3, lett. b), 29 e 32, paragrafo 4, del Regolamento UE 2016/679 (RGPD), e ai sensi dell'articolo 2 *quaterdecies*, comma 2, del d.lgs. 196/2003 (Codice in materia di protezione dei dati personali) e successive modifiche.

Visto l'articolo 474, comma 3, del r.r. 1/2002 e successive modificazioni, il quale individua come soggetti designati di diritto allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali, il Capo dell'Ufficio di Gabinetto, il Direttore Generale, i direttori regionali, i direttori delle Agenzie regionali, l'Avvocato coordinatore, il dirigente cui è attribuita la competenza relativamente alle funzioni previste dal decreto legislativo 6 settembre 1989, n. 322 (Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'art. 24 della legge 23 agosto 1988, n. 400) e alle convenzioni con l'ISTAT per l'attuazione del Programma Statistico Nazionale e il responsabile della struttura organizzativa autonoma di livello direzionale;

Visto l'articolo 474, comma 5, del r.r. 1/2002 e successive modificazioni, il quale prevede che la Giunta Regionale, in qualità di titolare del trattamento e i soggetti designati autorizzano, ai sensi degli articoli 28, paragrafo 3, lettera b), 29 e 32, paragrafo 4, del RGPD, nonché dell'articolo 2-*quaterdecies*, comma 2, del d.lgs. 196/2003 e successive modifiche, alle operazioni di trattamento dei dati personali, con specifico atto di nomina redatto secondo lo schema "B" dell'allegato "NN" del r.r. 1/2002, tutti i dipendenti o collaboratori a qualsiasi titolo, detti soggetti incaricati, che effettuano operazioni di trattamento dati sotto l'autorità diretta del titolare o del soggetto designato;

Visto il Regolamento UE 2016/679 del Parlamento e del Consiglio Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali,

³ Schema sostituito dall'articolo 36, comma 1, del r.r. 11 aprile 2024, n. 4, pubblicato sul Supplemento n. 1 del BUR Lazio 11 aprile 2024, n. 30

nonché alla libera circolazione di tali dati, di seguito RGPD, che garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, con particolare riferimento alla riservatezza e al diritto di protezione dei dati personali;

Visto il decreto legislativo 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) e successive modificazioni;

Considerato che ai fini del RGPD si intende per:

- “*trattamento*”, qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione (articolo 4, n. 2), RGPD);
- “*dato personale*” qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (articolo 4, n. 1) del RGPD);
- “*categorie particolari di dati personali*” si intendono i dati personali che rivelino l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale nonché i dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona (articolo 9, paragrafo 1, RGPD).

Tenuto conto che la figura del soggetto incaricato risulta coerente con il principio di “responsabilizzazione” dei Titolari del trattamento, la cui attuazione richiede l’adozione di misure atte a garantire proattivamente l’osservanza del RGPD nella sua interezza, come evidenziato dal Garante per la Protezione dei dati personali nella “Guida all’applicazione del Regolamento Europeo in materia di protezione dei dati personali”;

Tenuto conto che alla luce degli articoli 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, del RGPD in tema di misure tecniche e organizzative di sicurezza, il Garante ritiene opportuno che i Titolari del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione dei soggetti incaricati del trattamento stesso, così come delineatesi negli anni, anche attraverso gli interventi del Garante stesso;

Tenuto conto che alla luce dell’art. 2 *quaterdecies*, comma 2, del d. lgs. 196/2003 e successive modifiche, il titolare o il responsabile del trattamento è tenuto a

individuare le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta;

Considerato che la Giunta regionale, in qualità di titolare del trattamento, ai sensi dell'articolo 30 del RGPD, ha proceduto alla predisposizione del "Registro delle attività di trattamento", riportante, per ciascuna direzione, le informazioni in ordine ai trattamenti effettuati dalla Giunta stessa;

Considerato che la Giunta regionale, in qualità di titolare del trattamento, ai sensi degli articoli 33 e 34 del RGPD, ha proceduto alla redazione della "Procedura di *Personal Data Breach*", allo scopo di illustrare le azioni da mettere in atto, a fronte dell'accadimento di un incidente, accertato e classificato come violazione di dati personali (*Personal Data Breach*);

Tenuto conto delle mansioni già attribuite nel contratto di lavoro in essere con il Titolare e derivanti dall'assegnazione alla struttura amministrativa di afferenza;

DISPONE

1) di nominare il **<indicare nome e cognome>**, **soggetto incaricato al trattamento** dei dati personali relativamente alle attività normalmente svolte nell'ambito della Direzione Regionale **<inserire riferimenti Direzione e Area>**, in conformità e nei limiti delle proprie competenze espresse negli ordini di servizio e nelle norme del contratto di riferimento;

2) di impartire, ai fini dell'esercizio delle attività di cui al punto 1), le seguenti istruzioni:

- nel trattare i dati personali, si deve operare garantendo la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati personali confidenziali e, di norma, soggetti ad un dovere di riservatezza. Pertanto, non si dovranno divulgare a terzi le informazioni di cui si è venuti a conoscenza;
- si devono adottare tutte le misure necessarie a verificare l'esattezza dei dati raccolti e registrati, e, se necessario, correggerli ed aggiornarli di conseguenza;
- si è tenuti ad informare, tempestivamente e senza ingiustificato ritardo, di ogni evento attinente alla sicurezza o violazione di dati personali (cosiddetto *personal data breach*), il soggetto designato, per permettere al Titolare, ove ritenuto necessario, di notificare la violazione al Garante per la protezione dei dati personali e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando il Titolare ne è venuto a conoscenza;
- la condotta tenuta in ogni fase di lavoro dovrà evitare che i dati personali siano soggetti a rischi di perdita o distruzione anche accidentale; che ai dati possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini istituzionali per i quali i dati sono stati raccolti e per i quali vengono trattati;
- in ogni fase del trattamento non si possono eseguire operazioni per fini non previsti tra i compiti assegnati e si potrà accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere tali compiti;
- per i trattamenti dei dati personali che comportino l'uso di sistemi informatici e telematici (PC fisso, PC portatile o altro), l'accesso a tali dati può avvenire solo dopo almeno un processo di autenticazione attraverso password o codici di accesso

secondo quanto disposto dalle regole della Giunta Regionale. Ogni incaricato deve mantenere segreta la password di accesso al proprio PC, evitando di divulgarla a terzi o di trascriverla su fogli. Nessun dato personale, su supporto magnetico, digitale o cartaceo, potrà essere lasciato incustodito;

- tutto il materiale cartaceo contenente dati personali in argomento deve essere custodito con diligenza e conservato in maniera tale da non risultare facilmente visibile a persone terze o comunque ai non autorizzati al trattamento. Tali misure devono essere applicate anche a tutte le forme di riproduzione dei dati personali (ad esempio pen drive, CD/DVD, fotocopie);
- l'incaricato coadiuva il Titolare e/o il soggetto designato nell'aggiornamento del "Registro delle attività del Trattamento", indicato in premessa;
- l'incaricato è tenuto a comunicare tempestivamente, qualora necessario, al soggetto designato o al Responsabile per la Protezione dei dati indicato in premessa, ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi, nonché ogni evento legato a operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle definite dalla Giunta regionale;
- in qualunque circostanza non si abbia la certezza in merito alla correttezza di un'operazione di trattamento, ci si deve rivolgere senza indugio al soggetto designato;
- l'incaricato si impegna a rispettare l'obbligo legale di riservatezza sui trattamenti effettuati e su qualsiasi informazione o circostanza di cui fosse venuto a conoscenza, così come richiesto dal RGPD;

- 3) di stabilire che ulteriori istruzioni rispetto a quelle elencate potranno, di volta in volta, essere fornite dal Titolare e/o dal Soggetto Designato al trattamento, in base alla normativa vigente;
- 4) di stabilire che la presente nomina, disposta ai sensi della normativa vigente in materia di protezione dei dati personali, avrà la medesima durata del rapporto di lavoro presso la Giunta regionale e comunque dell'assegnazione alla struttura amministrativa di afferenza, al termine della quale cesserà l'efficacia dell'autorizzazione ad effettuare alcun tipo di trattamento sui dati.

Il Soggetto Designato(Direttore Regionale)
<inserire nome e cognome>

NOMINA AMMINISTRATORE DI SISTEMA

(INTESTAZIONE DELLA STRUTTURA)

Oggetto: Nomina Amministratore di Sistema/Base dati/Rete ai sensi dell'articolo 474, comma 7, del r.r. 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale) e successive modificazioni e del Provvedimento Generale del Garante per la protezione dei dati personali del 27/11/2008 (Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema) e successive modificazioni, pubblicato sulla Gazzetta Ufficiale n. 300 del 24/12/2008.

Visto l'articolo 474, comma 3, del r.r. 1/2002 e successive modificazioni, il quale individua come Soggetti designati di diritto allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali, il Capo di Gabinetto, i Direttori regionali, i Direttori delle Agenzie regionali, l'Avvocato coordinatore e il dirigente cui è attribuita la competenza relativamente alle funzioni previste dal decreto legislativo 6 settembre 1989, n. 322 (Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'art. 24 della legge 23 agosto 1988, n. 400) e alle convenzioni con l'ISTAT per l'attuazione del Programma Statistico Nazionale;

Visto l'articolo 474, comma 7, del r.r. 1/2002 e successive modificazioni, il quale prevede che i soggetti designati, qualora il trattamento dei dati personali venga effettuato con strumenti elettronici direttamente acquisiti dalla struttura di appartenenza, nominano gli amministratori di sistema con specifico atto di organizzazione, redatto sulla base dello schema "C" dell'allegato "NN" al r.r. 1/2002, nel rispetto di quanto previsto dal Provvedimento del Garante della Protezione dei dati Personali 27 novembre 2008 e successive modificazioni, nonché degli ulteriori criteri e modalità definiti dall'allegato "LL" al r.r. 1/2002;

Visto il Regolamento UE 2016/679 del Parlamento e del Consiglio Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, di seguito RGPD, che garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, con particolare riferimento alla riservatezza ed al diritto di protezione dei dati personali.

Visto il Provvedimento del Garante per la Protezione dei Dati Personali del 27/11/2008 e successive modificazioni;

Considerato che il suddetto Provvedimento richiede che si proceda alla designazione individuale degli Amministratori di Sistema (System Administrator), degli Amministratori di Base Dati (Database Administrator) e degli Amministratori di Rete (Network Administrator) che, nell'esercizio delle proprie funzioni, hanno accesso, anche fortuito, a dati personali;

Considerato che ai fini del RGPD per:

- "trattamento" si intende, qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la

raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (articolo 4, n.2), del RGPD);

- "dato personale" qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (articolo 4, n. 1) del RGPD);
- "categorie particolari di dati personali" si intendono i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (articolo 9, paragrafo 1, del RGPD).

Considerato che la Regione, ai sensi dell'articolo 30 del RGPD, ha proceduto alla predisposizione del "Registro delle attività di trattamento", riportante per ciascuna direzione le informazioni in ordine ai trattamenti effettuati dalla Regione stessa;

Considerato che la Regione, ai sensi degli articoli 33 e 34 del RGPD, ha proceduto alla redazione della "Procedura di Personal Data Breach", allo scopo di illustrare le azioni da mettere in atto, a fronte dell'accadimento di un incidente, accertato e classificato come violazione di dati personali (Personal Data Breach);

Tenuto conto delle mansioni già attribuite nel contratto di lavoro in essere con il Titolare e derivanti dall'assegnazione alla struttura amministrativa di afferenza;

Ritenuto che il/la dott./dott.ssa <inserire nome e cognome> ha l'esperienza, le capacità e l'affidabilità necessarie a fornire idonee garanzie del pieno rispetto delle disposizioni in materia di trattamento di dati personali, ivi compreso il profilo relativo alla sicurezza;

DISPONE

1) di nominare il/la **dott./dott.ssa <inserire nome e cognome>** quale **Amministratore di Sistema** relativamente alle attività di competenza;

2) di stabilire il seguente elenco degli ambiti di operatività dell'Amministratore di sistema in base al profilo di autorizzazione assegnato: **<inserire profilo di autorizzazione>**:

-

-

3) di stabilire che l'elenco sopra riportato potrà essere modificato al manifestarsi di specifiche necessità della direzione, in quanto le attività di profilazione e creazione delle utenze potranno rendere necessaria la modifica/integrazione degli ambiti di operatività sopra identificati;

4) di impartire, ai fini dell'esercizio delle attività di Amministratore di sistema di cui al punto 2), le seguenti istruzioni:

- nell'adempimento dell'esercizio delle proprie funzioni, l'Amministratore di sistema opera quale soggetto incaricato al trattamento di dati personali, ai sensi dell'articolo 474, comma 5, del r.r.1/2002

e successive modificazioni e degli articoli 28, paragrafo 3, lett. b), 29 e 32, paragrafo 4, del RGPD ed è tenuto ad osservare le istruzioni, attuali e future, impartite dalle competenti strutture della Regione;

- tutti i dati di cui l'Amministratore di sistema viene a conoscenza devono essere trattati esclusivamente per fini aziendali e con modalità tali da garantire la massima riservatezza, considerando i suddetti dati confidenziali e, di norma, non soggetti ad alcuna divulgazione a terzi;
- in qualunque circostanza non si abbia la certezza in merito alla correttezza di un'operazione di trattamento, ci si deve rivolgere senza indugio al Soggetto designato al trattamento;
- l'Amministratore di sistema si impegna all'obbligo legale di riservatezza sui trattamenti effettuati e su qualsiasi informazione o circostanza di cui fosse venuto a conoscenza, così come richiesto dal RGPD;

5) di stabilire, in conformità a quanto prescritto dal Provvedimento del Garante per la Protezione dei Dati Personali 27/11/2008 e successive modificazioni, indicato in premessa, che questa struttura provvederà a:

- svolgere con cadenza almeno annuale, nei limiti consentiti dalle norme legali e contrattuali, un'attività di verifica dell'operato dell'Amministratore di sistema, previa registrazione degli accessi logici (autenticazione informatica) ai sistemi e conservazione degli stessi per un congruo periodo non inferiore a 6 mesi. I dati registrati a tale scopo dai sistemi non vengono utilizzati in alcun modo per il controllo a distanza dei lavoratori e le tecnologie utilizzate a tal fine sono compatibili con quanto disposto dalla normativa vigente in materia;
- riportare gli estremi identificativi dell'Amministratore di sistema in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante;
- rendere conoscibile, all'interno della propria organizzazione, l'identità dell'Amministratore di sistema, la cui attività riguardi anche indirettamente sistemi che trattano o permettono il trattamento di informazioni di carattere personale dei lavoratori;

6) di stabilire che ulteriori istruzioni rispetto a quelle elencate potranno, di volta in volta, essere fornite dal Titolare e/o dal Soggetto designato al trattamento, in base alla normativa vigente;

7) di stabilire che la presente nomina, disposta ai sensi della normativa vigente in materia di protezione dei dati personali, avrà la medesima durata del rapporto di lavoro con la Regione e comunque dell'assegnazione alla struttura amministrativa di afferenza, al termine della quale cesserà l'efficacia dell'autorizzazione ad effettuare alcun tipo di trattamento sui dati.

Il Soggetto Designato (Direttore Regionale)
<inserire nome e cognome>

INFORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI

**INFORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ARTICOLO
13 DEL REGOLAMENTO EUROPEO 2016/679 - RGD**

1. Premessa

Ai sensi dell'articolo 13 del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la Direttiva 95/46/CE (di seguito Regolamento UE n. 2016/679), la Regione Lazio, in qualità di Titolare del trattamento, è tenuta a fornirle informazioni in merito all'utilizzo dei suoi dati personali.

2. Identità e i dati di contatto del Titolare del trattamento

Il Titolare del trattamento dei dati personali di cui alla presente informativa è Regione Lazio, Via R. Raimondi Garibaldi 7– 00147 Roma. Al fine di semplificare le modalità di inoltro e ridurre i tempi per il riscontro si invita a presentare alla Regione Lazio le richieste di esercizio diritti di cui al successivo punto 10, scrivendo ai seguenti indirizzi e-mail: dpo@regionelazio.it e PEC: DPO@regione.lazio.legalmail.it.

3. Il Responsabile della protezione dei dati personali

Il Responsabile della protezione dei dati designato è contattabile all'indirizzo e-mail dpo@regione.lazio.it, all'indirizzo DPO@regione.lazio.legalmail.it, oppure a seguente indirizzo: protocollo@regione.lazio.legalmail.it.

4. Responsabili del trattamento

La Regione Lazio può avvalersi di soggetti terzi per l'espletamento di attività che comportano trattamenti di dati di cui la Regione stessa è Titolare. Conformemente a quanto stabilito dalla normativa, tali soggetti assicurano livelli di esperienza, capacità e affidabilità tali da garantire il rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza dei dati.

Le istruzioni, i compiti e gli oneri in capo a tali soggetti terzi sono formalizzati con la designazione degli stessi a "Responsabili del trattamento" ai sensi dell'articolo 28 del Regolamento UE 2016/679. I Responsabili designati sono sottoposti a verifiche periodiche al fine di constatare il mantenimento dei livelli di garanzia registrati in occasione dell'affidamento dell'incarico iniziale.

5. Soggetti autorizzati al trattamento

I Suoi dati personali sono trattati da personale interno previamente autorizzato e designato quale incaricato del trattamento, a cui sono impartite idonee istruzioni in ordine a misure, accorgimenti, modus operandi, tutti volti alla concreta tutela dei Suoi dati personali.

6. Finalità e base giuridica del trattamento

⁴ Schema abrogato dall'articolo 37, comma 1, del r.r. 11 aprile 2024, n. 4, pubblicato sul Supplemento n. 1 del BUR Lazio 11 aprile 2024, n. 30

Il trattamento dei Suoi dati personali è necessario per lo svolgimento delle funzioni istituzionali di cui è investita la Regione e, pertanto, è effettuato ai sensi dell'articolo 6 "Liceità del trattamento", paragrafo 1 lett. e) del Regolamento UE 2016/679 ("il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento"). I dati personali sono trattati per le seguenti finalità strettamente connesse e necessarie alla fruizione del Portale e dei Servizi richiesti, nonché allo svolgimento di tutte le attività conseguenti, in particolare per:

- l'inserimento nell'Albo fornitori e adempimenti connessi;
- la partecipazione alle gare per l'acquisizione di beni e servizi funzionali allo svolgimento di indagini di mercato come previsto dalla normativa vigente in materia di appalti pubblici;
- l'invio di comunicazioni e di aggiornamenti nell'ambito dei programmi della Regione Lazio.

Inoltre, per garantire l'efficienza del servizio, i dati personali degli utenti potranno essere utilizzati per effettuare prove tecniche e di verifica, o indagini dirette a verificare il grado di soddisfazione degli utenti sul servizio offerto e richiesto.

I dati personali forniti dagli utenti che inoltrano richieste sono utilizzati al solo fine di eseguire il servizio o la prestazione richiesta e sono comunicati a terzi nel solo caso in cui ciò sia necessario per l'adempimento delle richieste (esempio servizio di spedizione della documentazione eventualmente richiesta) o quando la comunicazione sia imposta da obblighi normativi. La Regione Lazio si riserva la facoltà di effettuare attività di comunicazione e aggiornamento nell'ambito delle funzionalità del Portale.

7. Destinatarî dei dati personali

I Suoi dati personali non sono oggetto di comunicazione o diffusione.

8. Trasferimento dei dati personali a Paesi extra UE

I Suoi dati personali non sono trasferiti al di fuori dell'Unione europea.

9. Periodo di conservazione

I Suoi dati sono conservati per:

- un periodo di 10 anni a partire dall'aggiudicazione della gara;
- per un periodo di 10 anni dalla data della revoca, nel caso in cui il fornitore richieda la cancellazione dall'Albo.

A tal fine, anche mediante controlli periodici, viene verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al trattamento.

10. I suoi diritti

Ai sensi degli articoli 13, paragrafo 2, lettere b) e d) e 14, paragrafo 2, lettere d) ed e) nonché degli articoli 15, 16, 17, 18, e 21 del RGPD, ha tra l'altro, il diritto, in qualunque momento, di chiedere al Titolare del trattamento:

- l'accesso ai Suoi dati personali;
- la rettifica e l'integrazione degli stessi;
- la cancellazione dei dati (laddove non sussista un obbligo legale di conservazione);
- la limitazione del trattamento dei dati e di opporsi al trattamento degli stessi dati qualora ricorrano i presupposti previsti dalle disposizioni normative vigenti.

Inoltre, ha il diritto di proporre un reclamo all'Autorità Garante per la protezione dei dati personali, seguendo le procedure e le indicazioni pubblicate sul sito web ufficiale dell'Autorità stessa.

11. Conferimento dei dati

Il conferimento dei Suoi dati è facoltativo, ma necessario per le finalità sopra indicate. Il mancato conferimento comporterà l'impossibilità di ottenere quanto richiesto.

12. Tipi di dati trattati

Dati di navigazione

I sistemi informatici e le procedure software preposte al funzionamento di questo sito web acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet. Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti. In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente. Questi dati vengono utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso del sito e per controllarne il corretto funzionamento e vengono cancellati immediatamente dopo l'elaborazione. I dati potrebbero essere utilizzati per l'accertamento di responsabilità in caso di ipotetici reati informatici ai danni del sito.

Dati forniti volontariamente dall'utente

L'invio facoltativo, esplicito e volontario di messaggi di posta elettronica agli indirizzi indicati su questo sito comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti nella missiva. La registrazione facoltativa, esplicita e volontaria, tramite appositi moduli web (form) presenti sul nostro sito, comporta la successiva acquisizione di tutti i dati riportati nei campi compilati dall'utente ed il trattamento, conformemente a quanto riportato nelle specifiche informative riportate per ogni singolo form, è effettuato esclusivamente in adempimento di attività istituzionali proprie dell'Ente.

Cookies

Un "cookie" è un piccolo file di testo creato da alcuni siti web per immagazzinare informazioni sul computer dell'utente al momento in cui questo accede al sito. I cookie sono inviati da un server web al browser dell'utente e memorizzati sul computer di quest'ultimo; vengono, quindi, re-inviati al sito web al momento delle visite successive. Il sito della Regione Lazio fa uso dei cosiddetti "cookies di sessione", che risiedono esclusivamente nella memoria del computer dell'utente e non vengono memorizzati in modo persistente. Ciò implica la loro cancellazione una volta che il browser viene chiuso. L'uso è strettamente limitato alla trasmissione di identificativi di sessione, costituiti da numeri casuali generati dal server, necessari per consentire l'esplorazione sicura ed efficiente del sito. L'utilizzo di cookies permanenti è strettamente limitato all'acquisizione di dati statistici relativi all'accesso al sito e/o per mantenere le preferenze dell'utente (lingua, layout, ecc.). Il portale si avvale di un software per la rilevazione degli accessi al proprio sito che ricorre all'utilizzo di cookies permanenti, allo scopo di raccogliere informazioni statistiche sui "visitatori unici" (persone diverse) del sito. Questi cookies, definiti come "Unique Visitor Cookies", contengono un codice alfanumerico che identifica i computer di navigazione, senza tuttavia alcuna ulteriore raccolta di dati personali.

Link a siti esterni

Questo sito internet contiene collegamenti ipertestuali detti “link” (ossia strumenti che consentono il collegamento ad una pagina web di un altro sito: i siti esterni raggiungibili tramite link attraverso il Portale della Regione Lazio sono sviluppati e gestiti da soggetti sui quali l’Ente non ha alcuna titolarità né controllo e non è in alcun modo responsabile circa contenuti, qualità, accuratezza e servizi offerti. La visita e l’utilizzo dei siti consultati dall’utente dal presente sito tramite link, quindi, è rimessa esclusivamente alla totale discrezionalità e responsabilità dell’utente utilizzatore. La presente informativa, pertanto, è resa solo per il sito della Regione Lazio e non anche per altri siti web eventualmente consultati dall’utente tramite link.

INFORMATIVA

SUI DATI PERSONALI AI VISITATORI

INFORMATIVA AI VISITATORI

(ai sensi dell'articolo 13 del Regolamento UE 2016/679 - RGPD - in materia di protezione dei dati personali)

La Giunta regionale in qualità di Titolare del trattamento, con sede in Via R. Raimondi Garibaldi 7–00147 Roma, ai sensi dell'articolo 13 del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito “RGPD”), che abroga la Direttiva 95/46/CE, Le fornisce di seguito l’informativa circa le modalità di trattamento dei dati personali da Lei conferiti, al fine di accedere alle sedi della Giunta regionale.

Il RGPD garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell’interessato, con particolare riferimento alla riservatezza, all’identità personale e al diritto alla protezione dei dati personali.

Conformemente a quanto previsto dall’articolo 13 del RGPD, La informiamo pertanto che:

- la base giuridica del trattamento è quella di cui all’articolo 6, paragrafo 1, lett. e) del RGPD secondo il quale “*il trattamento è necessario per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri*”;
- i dati personali forniti verranno utilizzati nei limiti e per il perseguimento delle finalità relative alla registrazione e archiviazione della Sua presenza, nella qualità di visitatore negli uffici della Giunta regionale, anche per motivi di sicurezza e controllo interno;
- i documenti di identità consegnati al personale di vigilanza verranno custoditi strettamente per il periodo di permanenza del visitatore nei locali della Giunta regionale;
- il conferimento dei dati è facoltativo; resta inteso che l’eventuale rifiuto a fornire tali dati comporterà l’impossibilità di accesso negli uffici della Giunta regionale;
- i dati personali forniti saranno trattati “in modo lecito e secondo correttezza”;
- il trattamento sarà effettuato anche con l’ausilio di strumenti elettronici e/o automatizzati, ai quali possono accedere esclusivamente i soggetti autorizzati nel pieno rispetto di quanto previsto dal RGPD;
- non è previsto alcun processo decisionale automatizzato di cui all’art. 22 RGPD;

⁵ Schema sostituito dall’articolo 38, comma 1, del r.r. 11 aprile 2024, n. 4, pubblicato sul Supplemento n. 1 del BUR Lazio 11 aprile 2024, n. 30

- i dati potranno essere trattati con la collaborazione di soggetti terzi espressamente nominati Responsabili esterni del trattamento dal Titolare;
- i dati potranno essere comunicati:
 - a tutte le strutture preposte a verifiche e controlli in merito al corretto adempimento delle finalità su indicate;
 - al personale e ai collaboratori in qualità di responsabili e persone autorizzate al trattamento dei dati per le pratiche che La riguardano/interessano; tutti i soggetti sono debitamente informati ed istruiti circa gli adempimenti e le misure da adottare in materia di protezione dei dati personali;
- i dati personali non sono soggetti a diffusione;
- i dati personali saranno conservati per il tempo strettamente necessario al perseguimento delle finalità per cui i dati sono trattati, nei limiti stabiliti dalla normativa vigente e, comunque, non oltre il termine di tre mesi dall'ultimo accesso alle sedi della Giunta regionale.
- i dati raccolti non saranno oggetto di trasferimento verso paesi al di fuori dello Spazio Economico Europeo (SEE).

La informiamo altresì che:

- Titolare del trattamento è la Giunta regionale, con sede in Via R. Raimondi Garibaldi 7– 00147 Roma;
- come previsto dall'articolo 37 del RGPD, la Giunta regionale ha proceduto a designare, con DGR n. del, il Responsabile della Protezione dei Dati personali (DPO), contattabile presso il seguente indirizzo e-mail: dpo@regione.lazio.it oppure all'indirizzo PEC: dpo@regione.lazio.legalmail.it.

Ai sensi degli articolo 13, paragrafo 2, lettere b) e d) e 14, paragrafo 2, lettere d) e e) nonché degli articoli 15, 16, 17, 18 e 21 e 22 del RGPD, i soggetti cui si riferiscono i dati personali hanno il diritto, in qualunque momento, di chiedere al Titolare del trattamento l'accesso ai dati personali, la rettifica, l'integrazione, la cancellazione degli stessi laddove applicabile, la limitazione del trattamento dei dati che la riguardano o di opporsi al trattamento degli stessi qualora ricorrano i presupposti previsti dal RGPD e, laddove possibile, di non essere sottoposti ad una decisione basata unicamente sul trattamento automatizzato.

I diritti di cui sopra possono essere esercitati dall'interessato inviando una richiesta al seguente indirizzo di posta elettronica: urp@regione.lazio.it e PEC: urp@regione.lazio.legalmail.it.

L'interessato ha il diritto di proporre un reclamo al Garante per la protezione dei dati personali, seguendo le procedure e le indicazioni pubblicate sul sito web ufficiale dell'Autorità: www.garanteprivacy.it.

ATTO CHE DISCIPLINA I TRATTAMENTI SVOLTI DAL RESPONSABILE DEL TRATTAMENTO PER CONTO DELLA GIUNTA REGIONALE DEL LAZIO (IL TITOLARE DEL TRATTAMENTO) AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 679/2016

ALLEGATO ALLA DETERMINAZIONE REGIONALE N. ___ DEL ____

TRA

La Giunta regionale del Lazio, con sede in Via R. Raimondi Garibaldi 7– 00147 Roma, nella persona del Dott.....;

E

La *<indicare ragione e denominazione sociale della Società>*, (di seguito, per brevità, anche la “Società”, il “Responsabile” o il “Responsabile del trattamento”), con sede in

.....in persona del legale rappresentante pro tempore Dott. ;

PREMESSO CHE

la Giunta Regionale del Lazio (di seguito anche il “Titolare” o “Regione Lazio”), in qualità di Titolare del trattamento:

- svolge attività che comportano il trattamento di dati personali nell’ambito dei propri compiti (istituzionalmente affidati);
- è consapevole di essere tenuta a mettere in atto misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati e adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

VISTO l’articolo 474, comma 2, del regolamento regionale 6 settembre 2002, n. 1 (*Regolamento di organizzazione degli uffici e dei servizi della Giunta Regionale*) e successive modificazioni, il quale prevede che il Titolare del trattamento, con specifico atto negoziale di incarico ai singoli responsabili del trattamento, disciplini i trattamenti affidati al responsabile, i compiti e le istruzioni secondo quanto previsto dall’articolo 28, paragrafo 3, del Regolamento (UE) 2016/679 e in coerenza con le indicazioni del Responsabile della Protezione dei Dati del Titolare (di seguito anche “DPO”); nell’atto di incarico è, altresì, definita la possibilità di nomina di uno o più sub-responsabili, secondo quanto previsto dall’articolo 28, paragrafi 2 e 4, del Regolamento (UE) 2016/679;

VISTO 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 anche “RGPD” o “Regolamento (UE) 2016/679”), il quale

⁶ Schema sostituito dall’articolo 39, comma 1, del r.r. 11 aprile 2024, n. 4, pubblicato sul Supplemento n. 1 del BUR Lazio 11 aprile 2024, n. 30

garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento al diritto alla protezione dei dati personali;

VISTO il decreto legislativo 196/2003 “*Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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*” e successive modificazioni;

CONSIDERATO che le attività, erogate in esecuzione del Contratto <*indicare riferimenti del contratto*>, tra la Regione Lazio e <*indicare ragione e denominazione sociale della Società*>, implicano da parte di quest'ultima, il trattamento dei dati personali di cui è Titolare la Giunta regionale del Lazio, ai sensi di quanto previsto dal Regolamento (UE) 2016/679;

PRESO ATTO che l'articolo 4, n. 2) del RGPD definisce “*trattamento*”: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

PRESO ATTO che l'articolo 4, n. 7) del RGPD definisce “*Titolare del trattamento*”: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

PRESO ATTO che l'art. 4, n. 8) del RGPD definisce “*Responsabile del trattamento*”: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

VISTO il Provvedimento del Garante per la Protezione dei Dati Personali 27/11/2008 (Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema) e successive modificazioni, pubblicato sulla Gazzetta Ufficiale n. 300 del 24/12/2008;

CONSIDERATO che il suddetto Provvedimento richiede che si proceda alla designazione individuale degli Amministratori di Sistema (System Administrator), degli Amministratori di Base Dati (Database Administrator), degli Amministratori di Rete (Network Administrator) e degli Amministratori di Software Complessi, che, nell'esercizio delle proprie funzioni, hanno accesso, anche fortuito, a dati personali (di seguito anche "AdS");

VISTO il provvedimento dell'Agenzia per l'Italia Digitale (di seguito anche "AgID"), (Misure minime di sicurezza ICT per le Pubbliche Amministrazioni"), adottato in attuazione della Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015 (di seguito per brevità "Misure minime AgID), che ha dettato le regole da osservare per garantire un uso appropriato dei privilegi di AdS;

RITENUTO che, ai sensi dell'articolo 28, paragrafo 1 del RGPD, la Società presenta garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento dei dati personali di cui la Giunta Regionale Lazio è Titolare soddisfi i requisiti e il pieno rispetto delle disposizioni previste dal RGPD;

CONSIDERATO che il RGPD prevede all'articolo 28, punto 6 che "Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43";

VISTA la "DECISIONE DI ESECUZIONE (UE) 2021_915" relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio (Testo rilevante ai fini del SEE), che prevede, in particolare, che "Il titolare del trattamento e il responsabile del trattamento [sono] liberi di includere le clausole contrattuali tipo stabilite nella presente decisione in un contratto più ampio e di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo o pregiudichino i diritti o le libertà fondamentali degli interessati. L'utilizzo delle clausole contrattuali tipo lascia impregiudicato qualunque obbligo contrattuale del titolare del trattamento e/o del responsabile del trattamento di garantire il rispetto dei privilegi e delle immunità applicabili.";

Quanto sopra premesso, le parti stipulano e convengono quanto segue:

SEZIONE I

1. Clausola 1

Scopo e ambito di applicazione

- a) scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del 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);
- b) il Titolare del trattamento ed il responsabile del trattamento di cui all'allegato I accettano le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del Regolamento (UE) 2016/679;
- c) le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.
- d) gli allegati da I a VI costituiscono parte integrante delle clausole;
- e) le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il Titolare del trattamento a norma del Regolamento (UE) 2016/679;
- f) le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del Regolamento (UE) 2016/679.

2. Clausola 2

Invariabilità delle clausole

- a) le parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati;
- b) quanto previsto alla lettera a) non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

3. Clausola 3

Interpretazione

- a) quando le presenti clausole utilizzano i termini definiti nel Regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui al Regolamento stesso;
- b) le presenti clausole vanno lette e interpretate alla luce delle disposizioni del Regolamento (UE) 2016/679;
- c) le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal Regolamento (UE) 2016/679, o che pregiudichi i diritti o le libertà fondamentali degli interessati.

4. Clausola 4

Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

5. Clausola 5 (facoltativa)

Clausola di adesione successiva

- a) qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le parti, aderire alle presenti clausole in qualunque momento, in qualità di titolare del trattamento o di responsabile del trattamento, compilando gli allegati e firmando l'allegato I;
- b) una volta compilati e firmati gli allegati di cui alla lettera a), l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un titolare del trattamento o di un responsabile del trattamento, conformemente alla sua designazione nell'allegato I;
- c) l'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II OBBLIGHI DELLE PARTI

6. Clausola 6

Descrizione del trattamento

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del Titolare del trattamento, sono specificati nell'allegato II.

7. Clausola 7

Obblighi delle parti

7.1. Istruzioni

- a) il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate;
- b) il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il Regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. Limitazione delle finalità

Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del titolare del trattamento.

7.3. Durata del trattamento dei dati personali

Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato II.

7.4. Sicurezza del trattamento

- a) Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati;
- b) Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento al proprio personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. Dati “sensibili” o “particolari”

Se il trattamento riguarda dati personali che rivelano l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l’appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili» o «particolari», ai sensi dell’articolo 9 del RGPD), il responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari. Tali garanzie supplementari vanno esplicitate nell’allegato III.

7.6. Documentazione e rispetto

- a) le parti devono essere in grado di dimostrare il rispetto delle presenti clausole;
- b) il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole;
- c) il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal Regolamento (UE) 2016/679. Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un’attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento;
- d) il titolare del trattamento può scegliere di condurre l’attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole, non inferiore a 10 giorni;
- e) su richiesta, le parti mettono a disposizione delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. Ricorso a sub-responsabili del trattamento (ulteriori responsabili)

- a) il responsabile del trattamento ha l’autorizzazione generale del titolare del trattamento per ricorrere a ulteriori responsabili del trattamento (nel documento anche “sub- responsabili”), sulla base di un elenco concordato. Il responsabile del trattamento informa per iscritto il titolare del trattamento in merito all’aggiunta o alla sostituzione di sub-responsabili del trattamento nel suddetto elenco, con un anticipo di almeno 15 giorni, dando così al titolare del trattamento tempo sufficiente per potersi opporre. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione;
- b) qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l’esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento, si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento

- è soggetto a norma delle presenti clausole e del Regolamento (UE) 2016/679;
- c) su richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti d'ufficio o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia;
 - d) il responsabile del trattamento resta pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali;
 - e) il responsabile del trattamento concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il titolare del trattamento ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

7.8. Trasferimenti internazionali

- a) qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere ad un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del Regolamento (UE) 2016/679;
- b) il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività comportino il trasferimento di dati personali ai sensi del capo V del Regolamento (UE) 2016/679, il responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto del capo V del Regolamento (UE) 2016/679, utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del Regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

8. Clausola 8

Assistenza al titolare del trattamento

- a) il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento;
- b) il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempire agli obblighi di cui alle lettere a) e alla presente lettera, il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento;
- c) oltre all'obbligo di assistere il titolare del trattamento in conformità della lettera b), il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il

rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:

- 1) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
 - 2) l'obbligo, prima di procedere al trattamento, di consultare le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;
 - 3) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;
 - 4) gli obblighi di cui all'articolo 32 Regolamento (UE) 2016/679;
- d) le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

9. Clausola 9

Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del Regolamento (UE) 2016/679, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento stesso.

9.1. Violazione riguardante dati trattati dal Titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento, assiste il titolare del trattamento:

- a) nel notificare la violazione dei dati personali alle autorità di controllo competenti, senza ingiustificato ritardo, dopo che il titolare del trattamento ne è venuto a conoscenza (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
- b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del Regolamento (UE) 2016/679 devono essere indicate nella notifica del titolare del trattamento e includere almeno:
 - 1) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati, nonché le categorie e il numero approssimativo di registrazioni dei dati personali;
 - 2) le probabili conseguenze della violazione dei dati personali;
 - 3) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, anche, qualora necessario, per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo;

- c) nell'adempire, in conformità dell'articolo 34 del Regolamento (UE) 2016/679, all'obbligo di comunicare, senza ingiustificato ritardo, la violazione dei dati personali all'interessato, qualora la violazione degli stessi dati sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2. Violazione riguardante dati trattati dal responsabile del trattamento

In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

- a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
- b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
- c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Le parti stabiliscono nell'allegato III tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare stesso ai sensi degli articoli 33 e 34 del Regolamento (UE) 2016/679.

SEZIONE III DISPOSIZIONI FINALI

10. Clausola 10

Inosservanza delle clausole e risoluzione

- a) fatte salve le disposizioni del Regolamento (UE) 2016/679, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole;
- b) il titolare del trattamento ha diritto di risolvere il contratto relativamente al trattamento dei dati personali conformemente alle presenti clausole qualora:
 - 1) il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento ai sensi della lettera a) e il rispetto delle presenti clausole non sia stato adempiuto entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
 - 2) il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del Regolamento (UE) 2016/679;
 - 3) il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o delle autorità di controllo competenti per quanto riguarda i propri obblighi in conformità alle presenti clausole o al Regolamento (UE) 2016/679;
- c) il responsabile del trattamento ha diritto di risolvere il contratto relativamente al trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato, ai sensi della clausola 7.1, lettera b), il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili, il titolare del trattamento insista sul rispetto delle istruzioni stesse;
- d) dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

SEZIONE IV

ULTERIORI DISPOSIZIONI

11. Clausola 11

Il responsabile del trattamento dei dati personali nell'effettuare le operazioni di trattamento connesse all'esecuzione del suddetto contratto dovrà attenersi alle seguenti disposizioni operative:

- a) i trattamenti dovranno essere svolti nel pieno rispetto delle normative vigenti in materia di protezione dei dati personali, nonché tenendo conto dei provvedimenti e dei comunicati ufficiali emessi dal Garante per la protezione dei dati personali. In particolare:
 - i trattamenti sono svolti per le **finalità indicate nell'allegato II**;
 - i dati personali trattati in ragione delle attività di cui ai suddetti contratti hanno ad oggetto: dati personali "comuni" (articolo 4, n. 1) del RGPD, eventualmente dati particolari (articolo 9 del RGPD "Categorie particolari di dati personali") ed in casi particolari/eccezionali, previsti dalla normativa vigente, dati giudiziari di cui all'articolo 10 del RGPD (sostanzialmente ex dati giudiziari); **<eliminare le eventuali tipologie di dati non oggetto di trattamento>**
 - le categorie di interessati sono **<indicare le tipologie di interessato cui i dati afferiscono>**;
- b) il responsabile è autorizzato a procedere all'organizzazione di ogni operazione di trattamento dei dati nei limiti stabiliti dai contratti in essere tra le parti e dalle vigenti disposizioni contenute nel RGPD;
- c) il responsabile si impegna, già in fase contrattuale, al fine di garantire il rispetto del principio della "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" di cui all'articolo 25 del RGPD, a determinare i mezzi "non essenziali" del trattamento e a mettere in atto le misure tecniche e organizzative adeguate, ai sensi dell'articolo 32 del RGPD, prima dell'inizio delle attività, nei limiti della propria autonomia consentita dalle normative vigenti e dal presente atto;
- d) il responsabile dovrà eseguire i trattamenti funzionali alle attività ad esso attribuite e comunque non incompatibili con le finalità per cui i dati sono stati raccolti. Qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, il responsabile dovrà informare il titolare del trattamento ed il responsabile della protezione dei dati (DPO) della Giunta regionale del Lazio;
- e) il responsabile – per quanto di propria competenza – è tenuto, in forza di normativa cogente e del contratto, a garantire – per sé, per i propri dipendenti e per chiunque collabori a qualunque titolo – il rispetto della riservatezza, integrità, disponibilità dei dati, nonché l'utilizzo dei predetti dati per le sole finalità specificate nel presente documento e nell'ambito delle attività di sicurezza di specifico interesse del titolare;
- f) il responsabile ha il compito di curare, in relazione alla fornitura del servizio di cui al contratto in oggetto, l'attuazione delle misure prescritte dal Garante per la protezione dei dati personali (di seguito anche il "Garante") in merito all'attribuzione delle funzioni di "Amministratore di sistema" di cui al provvedimento del 27 novembre 2008, e successive modificazioni ed integrazioni ed, in particolare, di:
 - 1) designare come amministratore di sistema, con le modalità previste dal provvedimento del 27 novembre 2008, le persone fisiche autorizzate ad accedere in modo privilegiato, ai sensi dello stesso provvedimento, ai dati personali del cui trattamento la Giunta regionale del Lazio è titolare;
 - 2) conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte all'interno della società quali amministratori di sistema, in relazione ai dati personali del cui trattamento la Giunta regionale del Lazio è titolare;
 - 3) attuare le attività di verifica periodica, con cadenza almeno annuale, sul loro operato secondo

- quanto prescritto dallo stesso provvedimento; gli esiti di tali verifiche dovranno essere comunicati al titolare del trattamento su richiesta dello stesso;
- g) il responsabile si impegna a garantire, senza ulteriori oneri per il titolare, l'esecuzione di tutti i trattamenti individuati al momento della stipula del contratto e dei quali dovesse insorgere in seguito la necessità ai fini dell'esecuzione del contratto stesso;
 - h) il responsabile dovrà attivare le necessarie procedure aziendali per identificare ed istruire le persone autorizzate al trattamento dei dati personali ed organizzarne i compiti in maniera che le singole operazioni di trattamento risultino coerenti con le disposizioni di cui alla presente nomina, facendo in modo, altresì, che, sulla base delle istruzioni operative loro impartite, i trattamenti non si discostino dalle finalità istituzionali per cui i dati sono stati raccolti e trattati. Il responsabile garantirà, inoltre, che le persone autorizzate al trattamento siano vincolate da un obbligo, legalmente assunto, di riservatezza;
 - i) il responsabile si attiverà per garantire l'adozione delle misure di sicurezza di cui all'articolo 32 del RGPD. In particolare, tenuto conto delle misure di sicurezza in atto, adottate a protezione dei trattamenti dei dati per conto della Giunta regionale del Lazio, come previste dal contratto vigente, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento e, sulla base delle risultanze dell'analisi dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, che derivano in particolare dalla distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati, porrà in essere le opportune azioni organizzative per l'ottimizzazione di tali misure, al fine di garantire un livello di sicurezza adeguato al rischio. Tali misure comprendono, tra le altre:
 - 1) la pseudonimizzazione e la cifratura dei dati personali;
 - 2) misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
 - 3) misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
 - 4) procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, il responsabile terrà conto, in special modo, dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Il responsabile assicura, inoltre, che le operazioni di trattamento dei dati sono effettuate nel rispetto delle misure di sicurezza tecniche, organizzative e procedurali a tutela dei dati trattati, in conformità alle previsioni di cui ai provvedimenti di volta in volta emanati dalle Autorità nazionali ed europee (a ciò autorizzate), qualora le stesse siano applicabili rispetto all'attività effettivamente svolta come responsabile del trattamento.

Nel caso in cui, considerata la propria competenza e ove applicabile rispetto alle attività svolte, il responsabile dovesse ritenere che le misure adottate non siano più adeguate e/o idonee a prevenire/mitigare i rischi sopramenzionati, è tenuto a darne tempestiva comunicazione scritta al titolare e a porre comunque in essere tutti gli interventi temporanei, ritenuti essenziali e improcrastinabili, in attesa delle soluzioni definitive da concordare con il titolare.

L'adozione e l'adeguamento delle misure di sicurezza tecniche devono aver luogo prima di iniziare e/o continuare qualsiasi operazione di trattamento di dati.

Il responsabile è tenuto a segnalare prontamente al titolare l'insorgenza di problemi tecnici attinenti alle operazioni di raccolta e trattamento dei dati ed alle relative misure di sicurezza, che possano comportare rischi di distruzione o perdita, anche accidentale, dei dati stessi, ovvero di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta/dei trattamenti.

Il responsabile, ove applicabile, dovrà, altresì, adottare le misure minime di sicurezza ICT per le pubbliche amministrazioni, di cui alla circolare AgID del 18 aprile 2017, n. 2/2017, nonché le eventuali ulteriori misure specifiche stabilite dal titolare, nel rispetto dei contratti vigenti;

- l) il responsabile dovrà predisporre e tenere a disposizione del titolare la documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito riportate; inoltre renderà disponibili al titolare tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti normativi previsti dal RGPD, consentendo di effettuare periodicamente attività di verifica, comprese ispezioni realizzate dal titolare stesso o da un altro soggetto da questi incaricato;
- m) il responsabile adotterà le politiche interne e attuerà, ai sensi dell'articolo 25 del RGPD, le misure che soddisfano i principi della protezione dei dati personali fin dalla progettazione di tali misure; adotterà ogni misura adeguata a garantire che i dati personali siano trattati in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il tempo strettamente necessario al raggiungimento delle stesse;
- n) il responsabile, ai sensi dell'articolo 30 del RGPD e nei limiti di quanto dallo stesso stabilito, è tenuto a tenere un registro delle attività di trattamento effettuate sotto la propria responsabilità per conto del titolare e a cooperare con il titolare stesso e con il Garante per la protezione dei dati personali, laddove ne venga fatta richiesta ai sensi dell'articolo 30, paragrafo 4, del RGPD;
- o) il responsabile è tenuto ad informare di ogni violazione di dati personali (cosiddetta *personal data breach*) il titolare ed il responsabile della protezione dei dati (DPO) della Giunta regionale del Lazio, tempestivamente e senza ingiustificato ritardo, entro 24 ore dall'avvenuta conoscenza dell'evento. Tale notifica, da effettuarsi tramite PEC da inviare all'indirizzo protocollo@regione.lazio.legalmail.it e dpo@regione.lazio.legalmail.it, deve essere accompagnata da ogni documentazione utile, ai sensi degli articoli 33 e 34 del RGPD, per permettere al titolare, ove ritenuto necessario, di notificare questa violazione al Garante per la protezione dei dati personali e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando il titolare stesso ne è venuto a conoscenza. Nel caso in cui il titolare debba fornire informazioni aggiuntive alla suddetta autorità, il responsabile supporterà il titolare nella misura in cui le informazioni richieste e/o necessarie per il Garante siano esclusivamente in possesso del responsabile e/o di suoi sub-responsabili;
- p) il responsabile garantisce gli adempimenti e le incombenze anche formali verso il Garante per la protezione dei dati quando richiesto e nei limiti dovuti, adoperandosi per collaborare tempestivamente, per quanto di competenza, sia con il titolare sia con il Garante per la protezione dei dati personali. In particolare:
 - fornisce informazioni sulle operazioni di trattamento svolte;
 - consente l'accesso alle banche dati oggetto delle operazioni di trattamento;
 - consente l'esecuzione di controlli;
 - compie quanto necessario per una tempestiva esecuzione dei provvedimenti inibitori, di natura temporanea;
- q) il responsabile si impegna ad adottare, su richiesta del Titolare e nel rispetto degli obblighi contrattuali assunti, nel corso dell'esecuzione dei contratti, ulteriori garanzie quali l'applicazione di un codice di condotta applicato o di un meccanismo di certificazione approvato ai sensi degli articoli 40 e 42 del RGPD, laddove adottati. Il titolare potrà in ogni momento verificare l'adozione di tali ulteriori garanzie;
- r) il responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del titolare;
- s) il responsabile è tenuto a comunicare al titolare ed al DPO della Regione Lazio il nome ed i dati del proprio DPO, laddove il responsabile stesso lo abbia designato, conformemente a quanto prescritto dall'articolo 37 del RGPD. Il DPO collaborerà e si terrà in costante contatto con il DPO della Regione

Lazio;

- t) Per “persone autorizzate al trattamento” ai sensi dell’articolo 4, punto 10, secondo quanto stabilito dal Regolamento, si intendono le persone fisiche che, sotto la diretta autorità del responsabile, sono autorizzate ad effettuare le operazioni di trattamento dati personali riconducibili alla titolarità della Regione Lazio;
- u) il responsabile è tenuto ad autorizzare tali soggetti, ad individuare e verificare almeno annualmente l’ambito dei trattamenti agli stessi consentiti e ad impartire ai medesimi istruzioni dettagliate circa le modalità del trattamento;
- v) le “persone autorizzate al trattamento” sono tenute al segreto professionale e alla riservatezza, anche per il periodo successivo all’estinzione del rapporto di lavoro intrattenuto con il responsabile, in relazione alle operazioni di trattamento da essi eseguite;
- z) il responsabile è tenuto, altresì, a vigilare sulla puntuale osservanza delle istruzioni allo stesso impartite.

Il Titolare del trattamento

Il Responsabile del trattamento

ALLEGATO I

Elenco delle parti

Titolare del trattamento:
Giunta Regionale del Lazio

Sede: Via R. Raimondi Garibaldi 7– 00147 Roma,
<Nome, qualifica e dati di contatto del referente>

Dati di contatto del Responsabile della Protezione dei Dati personali (DPO):

.....

Data _____

Firma

.....

Responsabile del trattamento Ragione sociale

Sede legale:

via, n.

CAP, località, Provincia Tel. (+39) ##

PEC: laziocrea@legalmail.it

Dati di contatto del Responsabile della Protezione dei Dati personali (DPO):

.....

Nome, qualifica e dati di contatto del referente:

Inserire nome referente interno

CONTESTO DI RIFERIMENTO

La Regione Lazio con determinazione regionale n..... del..... ha definito i rapporti fra le parti.

ALLEGATO II

Descrizione del trattamento

Categorie di interessati i cui dati personali sono trattati

Categorie di dati personali trattati

Dati particolari trattati (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari.

Natura del trattamento

.....

Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento

Durata del trattamento

Per il trattamento da parte di (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento.

ALLEGATO III

Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei trattamenti e dei dati

NOTA ESPLICATIVA:

Le misure tecniche e organizzative devono essere descritte in modo concreto e non genericamente.

Descrizione delle misure di sicurezza tecniche e organizzative messe in atto dal o dai responsabili del trattamento (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.

Le misure applicate al trattamento sono:

- *designazione degli incaricati:*
- *tenuta del registro delle attività di trattamento:*
- *misure di pseudonimizzazione e cifratura dei dati personali:*
- *misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento. Il responsabile del trattamento è tenuto a disciplinare (se del caso) e applicare in relazione ai trattamenti svolti per conto della Regione Lazio:*
- *misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico:*
- *procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento:*
- *misure di identificazione e autorizzazione dell'utente:*
- *misure di protezione dei dati durante la trasmissione:*
- *misure di protezione dei dati durante la conservazione:*
- *misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati:*
- *misure per garantire la registrazione degli eventi:*
- *misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita:*
- *misure di informatica interna e di gestione e governance della sicurezza informatica:*
- *misure di certificazione/garanzia di processi e prodotti:*

- *misure per garantire la minimizzazione dei dati:*
- *misure per garantire la qualità dei dati:*
- *misure per garantire la conservazione limitata dei dati:*
- *misure per garantire la responsabilità:*
- *misure per consentire la portabilità dei dati e garantire la cancellazione:*

Per i trasferimenti a (sub-) responsabili del trattamento, descrivere anche le misure tecniche e organizzative specifiche che il (sub-) responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento.

Descrizione delle misure tecniche e organizzative specifiche che il responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento.

Elenco dettaglio delle misure tecniche in essere	
1	Limitazione dell'accesso fisico agli spazi dove sono presenti parti rilevanti del sistema informativo al personale del responsabile, il quale, all'occorrenza, presidia e verifica eventuali attività svolte da terzi preventivamente autorizzate
2	Separazione dei database e degli ambienti di sviluppo, test da quelli di produzione
3	Adozione di sistemi antimalware inclusi nell'antivirus MS e Defender for Endpoint e presenza di MS SCCM per distribuzione software, comunicazione agli utenti su sicurezza, virus, phishing, malware ecc.
4	Svolgimento dei backup dei dati, in funzione del contesto e della tipologia, con modalità e durate di conservazione diverse. I relativi ripristini dei dati possono essere di vario tipo: ad esempio ripristini applicativi; per danni causati da rilasci non andati a buon fine; per errori umani con utenze nominative; per corruzione dati; ripristini per aggiornamento ambienti di test e produzione, ripristini per test di funzionamento backup, ecc.
5	Registrazione dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni mediante log management
6	Sottoposizione a log e riconducibilità alla singola persona delle attività degli amministratori, dei database e dei server
7	Utilizzo di un unico server NTP interno come riferimento per tutte le sincronizzazioni
8	Svolgimento delle attività di installazione e in generale di manutenzione solo da personale preventivamente formato, competenteed autorizzato

9	<p>Segregazione degli accessi alle diverse componenti del datacenter; in generale il personale autorizzato ad accedere ai server, non ha accesso agli apparati di rete. La profilazione degli utenti avviene tramite differenti gruppi su active directory.</p> <p>Inoltre, sulle reti pubbliche e sulle reti wireless, sono utilizzati protocolli che proteggono il dato (https nel caso delle reti pubbliche e WPA2 nel caso delle reti wireless). La verifica della disponibilità delle reti viene effettuata tramite software di monitoraggio.</p> <p>Il monitoraggio degli accessi amministrativi sugli apparati di rete avviene tramite syslog e su piattaforma SIEM. Inoltre, apposito software salva le configurazioni ad ogni modifica, consentendo di visualizzare le modifiche e fare eventuale rollback.</p> <p>Tutti gli apparati ed i sistemi sono autenticati. L'autenticazione dei sistemi avviene tramite LDAP.</p> <p>Infine, ci sono specifiche reti (vpn sistemistica e rete della control room) che sono le uniche a poter aver accesso alla rete di gestione degli apparati. Tali apparati hanno una rete di management dedicata e fisicamente separata.</p>
---	--

10	Le reti interne al datacenter sono protette da firewall perimetrale. Inoltre è previsto un firewall interno al datacenter per la segregazione delle reti interne.
11	Nella realizzazione dei servizi si provvede a valutare il livello di sicurezza necessario e ad applicare le limitazioni ritenute opportune per garantire la separazione tra domini. Si applicano, in base alle specificità, segregazione di reti, fisiche e/o logiche, gestione degli accessi tramite gateway con specifici firewall e router.
12	Tutte le comunicazioni tramite posta elettronica si basano sulla sicurezza data dal server di posta, le comunicazioni in rete (nei casi ritenuti necessari) avvengono in https. Quando necessario scambiare file si usano canali sicuri in STFP
13	Le informazioni coinvolte nelle trasmissioni dei servizi applicativi sono protette mediante l'utilizzo di canali sicuri (firewall, VPN), e mediante certificato o cifratura
14	Gli ambienti di test applicativi, gestiti direttamente dai gruppi di progetti che ne sono responsabili, non contengono mai dati reali, ma solo dati fittizi
15	Le installazioni e configurazioni dei vari asset, quanto possibile, vengono fatte mediante template preventivamente predisposti e verificati. I predetti template sono disponibili esclusivamente al personale autorizzato alle installazioni in sola lettura
16	Le operazioni di amministrazione remota sui server sono eseguite con protocolli sicuri ad esempio SSH ed RDP
17	Eventuali eventi di cambiamento della configurazione e dei permessi di sicurezza del sistema sono inviati al SIEM
18	Le credenziali di amministratore di dominio sono conservate in un wallet protetto da password
19	Per i messaggi di posta è attivo il servizio antispam di Microsoft in Cloud (EOP)
20	<p>Impostazione della scadenza delle password su base trimestrale su tutti gli account con inibizione globale della possibilità di non farscadere le password.</p> <p>Definizione interna dei processi di gestione delle password impostate su account impersonali o di servizio, al fine di favorirne un' opportuna rotazione periodica.</p> <p>Favorire, ove possibile, l'utilizzo di gMSA (group Managed Service Accounts, un ibrido tra account di servizio ed account utente), per la gestione degli account di servizio. Nel caso di applicazioni che non supportano i gMSA, creazione di policy per rendere le password complesse ed aggiornarle con frequenza.</p>

21	Previsione di elevati requisiti di complessità delle password su tutti gli account, quali: requisito di lunghezza minima di 8 caratteri; Invito a non utilizzare password comuni; educazione degli utenti a non utilizzare le password già utilizzate in ambito aziendale per scopi non legati al lavoro.
22	Razionalizzazione degli account di dominio, evitando l'annidamento di gruppi di utenti all'interno di altri gruppi amministrativi. Riduzione degli account amministrativi ad un numero essenziale, secondo i seguenti approcci: - Applicazione di restrizioni agli account locali per l'accesso remoto. - Limitazione dell'accesso di rete a tutti gli account di amministratore locale.
23	Segmentazione delle reti evitando subnet eccessivamente ampie e limitando, di fatto, la possibilità per un potenziale attaccante di eseguire movimenti laterali, favorendo il principio del privilegio minimo
24	Ove necessario, aggiornamento di firmware o SO di tutti i sistemi e i dispositivi di protezione perimetrale (Firewall, IDS/IPS, Proxy /Reverse Proxy) alle ultime release rilasciate dai rispettivi produttori

25	Individuazione di un'unica tipologia di accesso e gestione remota dei sistemi (ad esempio RDP), evitando l'utilizzo esteso di strumenti di terze parti sfruttabili anche da utenti malintenzionati (ad esempio Dameware, AnyDesk, LogMeIn)
26	Aggiornamento, all'occorrenza, dei sistemi operativi risultanti in stato end of life o end of support.
27	In caso di intrusione o minaccia, reinstallazione completa di tutti i sistemi server e contestuale posizionamento in segmenti di rete suddivisi per layer di sicurezza (Tier), ad accesso limitato e amministrabili solo da un numero limitato di workstation, a loro volta isolate dalle altre reti
28	Standardizzazione della configurazione dei Domain Controller, evitando di adibire gli stessi a ruoli secondari come ad esempio Print Server. Limitazione dell'accesso ai sistemi critici solo ad un numero ristretto di utenti, e solo da specifiche postazioni
29	Utilizzo di apparati "Next generation Firewall" periferici, segregazione dei siti, attivazione dei moduli IDS/IPS
30	Utilizzo di politiche restrittive sulla navigazione in internet degli utenti, favorendo il principio del privilegio minimo
31	Dissuasione rispetto all'utilizzo di account di servizio per accedere in modo interattivo. Monitoraggio costante dell'utilizzo degli account di servizio ed indagini circa eventuali accessi interattivi, ad esempio utilizzando il servizio offerto da Active Directory e le Group Policy ai fini della registrazione dettagliata degli eventi
32	Utilizzo di tecnologia SIEM e/o di un servizio di Cyber Detection & Protection, essenziale per la sicurezza dell'infrastruttura e per la raccolta e razionalizzazione centralizzata di log ed eventi di sicurezza provenienti da diverse sorgenti
33	Utilizzo di un servizio di Security Awareness & Training finalizzato all'educazione degli utenti in ambito Cyber Security
34	Esecuzione di assessment periodici sui livelli di maturità dei controlli di sicurezza previsti dai principali standard nazionali ed internazionali. Definizione di diversi domini di intervento analizzando gli obiettivi dell'ente e le informazioni relative ad incidenti pregressi correlati. Valutazione di possibili ulteriori azioni a fronte dei risultati dell'assessment. Consolidamento della propensione al rischio minimo e definizione di soglie di tolleranza del rischio in ciascun dominio individuate.

35	Al fine di prevenire attacchi esterni, esecuzione assessment periodici su sistemi Linux/Unix. Valutazione di possibili ulteriori azioni a fronte dei risultati ottenuti (es. individuazione di account non censiti, creati dall'eventuale attaccante allo scopo di futuri utilizzi; individuazione di possibili tracce di accesso non autorizzato ai sistemi, come autenticazioni fuori dall'orario di servizio o mediante account non noti).
36	Utilizzo di servizi continuativi di Vulnerability Assessment, Penetration Testing & Patch Management. Identificazione continua delle vulnerabilità dei sistemi, al fine di recepire il reale livello di sicurezza dell'infrastruttura e definire un piano di rientro assegnando le giuste priorità sulla base della criticità dei processi di Patching rispetto all'impatto sulla produzione

ALLEGATO IV

Elenco dei sub-responsabili del trattamento e/o terzi autorizzati al trattamento

(ove applicabile indicare eventuali subappaltatori del fornitore)

Saranno qui inseriti i sub-responsabili individuati a seguito di specifica esigenza del titolare.

Ragione sociale del sub-responsabile

SUB-TRATTAMENTO DELEGATO: Gestione xxxxxxxxxxxxxx.

ALLEGATO V

Disciplina dei servizi di Amministratore di Sistema

(laddove le prestazioni contrattuali implicino l'erogazione di servizi di amministrazione di sistema)

In conformità a quanto prescritto dal Provvedimento del Garante del 27/11/2008 e successive modificazioni ed alle misure minime AgID relativamente alle utenze amministrative, laddove le prestazioni contrattuali implicino l'erogazione di servizi di amministrazione di sistema, la società, in qualità di responsabile del trattamento, si impegna a:

- 1) individuare i soggetti ai quali affidare il ruolo di amministratori di sistema (System Administrator), amministratori di base dati (Database Administrator), amministratori di rete (Network Administrator) e/o amministratori di software complessi e, sulla base del successivo atto di designazione individuale, impartire le istruzioni a detti soggetti, vigilando sul relativo operato;
- 2) assegnare ai suddetti soggetti una user id che contenga riferimenti agevolmente riconducibili all'identità degli amministratori e che consenta di garantire il rispetto delle seguenti regole:
 - a) divieto di assegnazione di user id generiche e già attribuite anche in tempi diversi;
 - b) utilizzo di utenze amministrative anonime, quali "root" di Unix o "Administrator" di Windows, solo per situazioni di emergenza; le relative credenziali devono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso;
 - c) disattivazione delle user id attribuite agli amministratori che non necessitano più di accedere ai dati;
- 3) associare alle user id assegnate agli Amministratori una password e garantire il rispetto delle seguenti regole:
 - a) utilizzare password con lunghezza minima di almeno 14 caratteri, qualora l'autenticazione a più fattori non sia supportata;
 - b) cambiare la password alla prima connessione e successivamente almeno ogni 30 giorni (password aging);
 - c) le password devono differire dalle ultime 5 utilizzate (password history);
 - d) conservare le password in modo da garantirne disponibilità e riservatezza;
 - e) registrare tutte le immissioni errate di password. Ove tecnicamente possibile, gli account degli amministratori devono essere bloccati dopo un numero massimo di tentativi falliti di login;
 - f) assicurare che l'archiviazione di password o codici PIN su qualsiasi supporto fisico avvenga solo in forma protetta da sistemi di cifratura;
- 4) assicurare la completa distinzione tra utenze privilegiate e non privilegiate di amministratore, alle quali devono corrispondere credenziali diverse;
- 5) assicurare che i profili di accesso, in particolare per le utenze con privilegi amministrativi, rispettino il principio del need-to-know, ovvero che non siano

attribuiti diritti superiori a quelli realmente necessari per eseguire le normali attività di lavoro. Le utenze con privilegi amministrativi devono essere utilizzate per il solo svolgimento delle funzioni assegnate;

- 6) mantenere aggiornato un inventario delle utenze privilegiate (Anagrafica AdS), anche attraverso uno strumento automatico in grado di generare un alert quando è aggiunta una utenza amministrativa e quando sono aumentati i diritti di un'utenza amministrativa;
- 7) adottare sistemi di registrazione degli accessi logici (log) degli amministratori ai sistemi e conservare gli stessi per un congruo periodo non inferiore a 6 mesi. Qualora la società utilizzi sistemi messi a disposizione dalla Regione, comunicare agli amministratori che la Regione stessa procederà alla registrazione e conservazione dei log;
- 8) impedire l'accesso diretto ai singoli sistemi con le utenze amministrative. In particolare, deve essere imposto l'obbligo per l'amministratore di accedere con una utenza normale e solo successivamente dargli la possibilità di eseguire, come utente privilegiato, i singoli comandi;
- 9) utilizzare, per le operazioni che richiedono utenze privilegiate di amministratore, macchine dedicate, collocate in una rete logicamente dedicata, isolata rispetto ad internet. Tali macchine non devono essere utilizzate per altre attività;
- 10) comunicare al momento della sottoscrizione del presente atto, e comunque con cadenza almeno annuale ed ogni qualvolta se ne verifichi la necessità, alla Regione gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema, di base dati, di rete e/o di software complessi, specificando per ciascuno di tali soggetti:
 - a) il nome e cognome;
 - b) la user id assegnata agli amministratori;
 - c) il ruolo degli amministratori (ovvero di Sistema, base dati, di rete e/o di software complessi);
 - d) i sistemi che gli stessi gestiscono, specificando per ciascuno il profilo di autorizzazione assegnato;
- 11) eseguire, con cadenza almeno annuale, le attività di verifica dell'operato degli amministratori e consentire comunque alla Regione, ove ne faccia richiesta, di eseguire in proprio dette verifiche;
- 12) nei limiti dell'incarico affidato, mettere a disposizione del titolare e del DPO della Regione quando formalmente richieste, le seguenti informazioni relative agli amministratori: log in riusciti, log in falliti, log out. Tali dati dovranno essere resi disponibili per un congruo periodo non inferiore a 6 mesi;
- 13) durante l'esecuzione dei contratti, nell'eventualità di qualsivoglia modifica della normativa in materia di protezione dei dati personali, che generi nuovi requisiti (ivi incluse nuove misure di sicurezza di natura fisica, logica e/o organizzativa), la società si impegna a collaborare, nei limiti delle proprie competenze tecniche/organizzative e delle proprie risorse, con il titolare affinché siano sviluppate, adottate ed implementate misure correttive di adeguamento ai nuovi requisiti.

ALLEGATO VI

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

Benché non siano direttamente destinatari delle disposizioni di cui all'articolo 25 del RGPD, i responsabili del trattamento rappresentano figure essenziali ai fini della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita e dovrebbero essere consapevoli del fatto che il titolare è tenuto a trattare i dati personali solo utilizzando sistemi e tecnologie che integrano i principi di protezione dei dati.

Nel trattare i dati per conto del titolare, o nel fornire al titolare soluzioni di trattamento, il responsabile deve adottare e implementare soluzioni di progettazione che integrano la protezione dei dati nel trattamento. Ciò significa a sua volta che la progettazione di prodotti e servizi dovrebbe semplificare le esigenze dei titolari.

Nell'applicare l'articolo 25 del RGPD si deve tener presente che un principale obiettivo di progettazione è costituito dall'integrare nelle misure adeguate per lo specifico trattamento l'*efficace attuazione* dei principi e la *tutela* dei diritti degli interessati. Al fine di agevolare e potenziare l'adozione della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, di seguito sono elencate alcune istruzioni:

- 1) la protezione dei dati deve essere presa in considerazione sin dalle fasi iniziali della pianificazione di un trattamento e ancor prima di definirne i mezzi;
- 2) se il responsabile del trattamento è coadiuvato da un responsabile della protezione dei dati (RPD), questo deve essere coinvolto per integrare la protezione dei dati fin dalla progettazione e protezione per impostazione predefinita nelle procedure di acquisizione e sviluppo, nonché lungo l'intero ciclo di vita del trattamento;
- 3) il responsabile del trattamento deve essere in grado di dimostrare che la protezione dei dati fin dalla progettazione e protezione per impostazione predefinita è parte integrante del ciclo di vita dello sviluppo delle soluzioni adottate per il trattamento;
- 4) il responsabile del trattamento deve tenere conto degli obblighi di fornire una tutela specifica ai minori e ad altri interessati vulnerabili, nel rispetto della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita;
- 5) il responsabile del trattamento deve agevolare l'attuazione della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita al fine di supportare il titolare nell'adempimento degli obblighi previsti dall'articolo 25 del RGPD. Si ricorda che il titolare non può scegliere un responsabile del trattamento che non offre sistemi in grado di consentire o facilitare l'adempimento degli obblighi di cui all'articolo 25 in capo al titolare stesso, poiché sarà quest'ultimo a rispondere dell'eventuale mancata attuazione;
- 6) il responsabile del trattamento deve svolgere un ruolo attivo nel garantire che siano soddisfatti i criteri relativi allo «stato dell'arte» e notificare ai titolari del trattamento qualunque modifica a tale «stato dell'arte» che possa compromettere l'efficacia delle misure adottate;

- 7) il responsabile del trattamento deve essere in grado di dimostrare in che modo i propri mezzi (hardware, software, servizi o sistemi) permettano al titolare di soddisfare i requisiti in materia di responsabilizzazione in conformità della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, per esempio utilizzando indicatori chiave di prestazione (KPI) per dimostrare l'efficacia delle misure e delle garanzie nell'attuazione dei principi e dei diritti;
- 8) il responsabile del trattamento deve consentire al titolare del trattamento di essere corretto e trasparente nei confronti degli interessati per quanto concerne la valutazione e dimostrazione dell'effettiva attuazione della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, analogamente a quanto si verifica nella dimostrazione della loro conformità con il RGPD in base al principio di responsabilizzazione;
- 9) le tecnologie di rafforzamento della protezione dei dati (PET, *privacy-enhancing technologies*) che hanno raggiunto lo stato dell'arte possono essere utilizzate fra le misure da adottare in conformità dei requisiti della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, se del caso, secondo un approccio basato sul rischio. Si ricorda che di per sé, le PET non coprono necessariamente gli obblighi di cui all'articolo 25 del RGPD;
- 10) il responsabile del trattamento deve tenere conto che i sistemi preesistenti sono soggetti agli stessi obblighi in materia di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita ai quali soggiacciono i sistemi nuovi, cosicché, ove non siano già conformi ai principi della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita e non sia possibile effettuare modifiche per adempiere ai relativi obblighi, i sistemi preesistenti non sono conformi agli obblighi del RGPD e non possono essere utilizzati per trattare dati personali;
- 11) il responsabile del trattamento deve trattare solo i dati personali che sono adeguati, pertinenti e limitati a quanto necessario per la finalità. La minimizzazione dei dati realizza e rende operativo il principio di necessità. Nel proseguire il trattamento, il responsabile deve valutare periodicamente se i dati personali trattati siano ancora adeguati, pertinenti e necessari o se occorra cancellarli o renderli anonimi.
- 12) la minimizzazione può anche riferirsi al grado di identificazione. Se la finalità del trattamento non richiede che i set di dati definitivi si riferiscano a una persona fisica identificata o identificabile (come nelle statistiche), ma lo richiede il trattamento iniziale (ad es. prima dell'aggregazione dei dati), il responsabile cancella o rende anonimi i dati personali non appena non sia più necessaria l'identificazione. Se l'identificazione continua a essere necessaria per le altre attività di trattamento, i dati personali dovrebbero essere pseudonimizzati al fine di ridurre i rischi per i diritti degli interessati.

**CLAUSOLE DEI CONTRATTI IN CUI IL FORNITORE DEVE ESSERE
NOMINATO RESPONSABILE DEL TRATTAMENTO**

“Protezione dei dati personali”

La Regione Lazio, in qualità di Titolare del Trattamento, con atto formale riportato in allegato (**inserire riferimenti dell'Allegato**) al presente Contratto e parte integrante dello stesso, nomina la Società, Responsabile del trattamento dei dati ai sensi degli articoli 4, n. 8) e 28 del 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.

Con la sottoscrizione del presente contratto, la Società si obbliga ad accettare la nomina a Responsabile del Trattamento, nonché a sottoscrivere l'atto di nomina di cui all'Allegato (**inserire riferimenti dell'Allegato**) contestualmente al contratto e comunque entro e non oltre il termine di quindici giorni dalla data di stipula del contratto stesso.

Sottoscritto l'atto, la Società garantisce l'osservanza delle prescrizioni in esso contenute da parte del proprio personale dipendente, nonché di quello incaricato per l'esecuzione del Contratto.

STIPULA CONTRATTO <testo valido anche per Convenzione/Protocollo d'Intesa>

Art. ... - Trattamento dei dati personali

Le parti dichiarano di avere rilasciato, prima della sottoscrizione del presente contratto, tutte le informazioni di cui all'articolo 13 del Regolamento UE 2016/679 (di seguito RGPD) circa il trattamento dei dati personali conferiti per l'esecuzione del contratto stesso e di essere a conoscenza dei diritti che spettano alle persone fisiche in qualità di interessati in virtù dell'articolo 13, paragrafo 2, lettere b) e d) e 14, paragrafo 2, lettere d) e e), nonché degli articoli 15, 16, 17, 18, e 21 del RGPD, che potranno essere esercitati, in qualunque momento, presso i recapiti indicati nelle policy privacy pubblicate sui siti web di ciascuna Parte.

Le parti si impegnano a improntare il trattamento dei dati raccolti per la gestione del contratto e l'esecuzione economica ed amministrativa dello stesso, nonché per l'adempimento degli obblighi legali ad esso connessi e per fini di studio e statistici, ai principi di correttezza, liceità e trasparenza, nel pieno rispetto di quanto previsto dal RGPD e dal decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni.

Inparticolare le parti s'impegnano a trattare i dati, il cui conferimento è obbligatorio per l'esecuzione del contratto, esclusivamente con la collaborazione di personale autorizzato al trattamento, nonché di soggetti terzi espressamente nominati Responsabili del trattamento ai sensi dell'articolo 28 del RGPD. Il trattamento sarà effettuato tramite l'utilizzo di procedure informatizzate ovvero mediante trattamenti manuali. I dati non saranno oggetto di comunicazione e/o trasferimento verso paesi terzi e saranno conservati per il tempo strettamente necessario al perseguimento delle finalità per cui i dati sono trattati, nei limiti stabiliti da leggi o regolamenti e, comunque, non oltre il termine di 10 anni dall'ultimo atto o comunicazione inerente il procedimento stesso.

CLAUSOLA DA INSERIRE NEI CONTRATTI LADDOVE il Soggetto Terzo debba essere nominato Responsabile al trattamento dei dati personali ai sensi dell'articolo 28 del RGPD

Articolo ... - Responsabile del Trattamento dei Dati Personali

Le attività oggetto del presente contratto implicano, da parte della Società, il trattamento dei dati personali di cui è Titolare la Regione Lazio, ai sensi del Regolamento UE 2016/679 (di seguito RGPD).

Regione Lazio, ai sensi dell'articolo 28 del RGPD, riconosce che la Società dispone delle garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento dei dati personali di cui la Regione Lazio è Titolare soddisfi i requisiti e il pieno rispetto delle disposizioni previste dal RGPD.

La Regione Lazio, in qualità di Titolare del Trattamento, con atto formale riportato in allegato (Allegato n. ...) al contratto e parte integrante dello stesso, nomina la Società quale Responsabile del trattamento dei dati ai sensi degli articoli 4, n. 8) e 28 del RGPD. Con la sottoscrizione del presente contratto, la Società si impegna ad accettare la nomina a Responsabile del Trattamento. La Società si impegna, inoltre, a sottoscrivere l'atto di nomina di cui all'Allegato n. ..., entro il termine di quindici giorni, dalla data di stipula del presente contratto.

Allegato n. ...

Oggetto “Nomina a Responsabile del trattamento dei dati personali ai sensi degli articoli 4, n. 8) e 28 del RGPD – Regolamento (UE) 679/2016 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”.

Va compilato secondo il modello di cui allo schema “G”

“Protezione dei dati personali”

La Regione Lazio, in qualità di Titolare del Trattamento, garantisce che i dati personali saranno trattati ai sensi del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito RGPD), che abroga la Direttiva 95/46/CE, e ai sensi del decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni.

I dati personali saranno utilizzati esclusivamente per il perseguimento delle finalità istituzionali proprie della Regione Lazio, nei limiti stabiliti da espresse disposizioni normative e saranno trattati per finalità connesse e strumentali al presente disciplinare di gara e all'eventuale stipula ed esecuzione del contratto.

La Regione Lazio può venire a conoscenza, oltre che di dati di natura personale, anche di quelli relativi a condanne penali e reati (articolo 10 del RGPD). Tali dati saranno trattati per le sole finalità previste dalla normativa vigente, mediante l'ausilio di strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità stesse e, comunque, in modo da garantire la sicurezza, la riservatezza, l'integrità e la disponibilità degli stessi.

I dati saranno trattati, direttamente dal Titolare o dal personale espressamente autorizzato al trattamento nonché da soggetti terzi espressamente nominati Responsabili del trattamento dal Titolare ai sensi dell'articolo 28 del RGPD.

STIPULA CONTRATTO <testo valido anche per Convenzione/Protocollo d'Intesa>

Art. - Trattamento dei dati personali

Le parti dichiarano di avere rilasciato, prima della sottoscrizione del presente contratto tutte le informazioni di cui all'articolo 13 del Regolamento UE 2016/679 (di seguito RGPD) circa il trattamento dei dati personali conferiti per l'esecuzione del contratto stesso e di essere a conoscenza dei diritti che spettano alle persone fisiche in qualità di interessati in virtù dell'articolo 13, paragrafo 2, lettere b) e d) e 14, paragrafo 2, lettere d) e e), nonché degli articoli 15, 16, 17, 18 e 21 del citato RGPD, che potranno essere esercitati, in qualunque momento, presso i recapiti indicati nelle policy privacy pubblicate sui siti web di ciascuna parte.

Le parti si impegnano a improntare il trattamento dei dati raccolti per la gestione del contratto e l'esecuzione economica ed amministrativa dello stesso, nonché per l'adempimento degli obblighi legali ad esso connessi, e per fini di studio e statistici, ai principi di correttezza, liceità e trasparenza nel pieno rispetto di quanto definito dal RGPD e ai sensi del decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni.

In particolare le parti si impegnano a trattare i dati, il cui conferimento è obbligatorio per l'esecuzione dell'atto, esclusivamente con la collaborazione di personale autorizzato al trattamento, nonché da soggetti terzi espressamente nominati Responsabili del trattamento ai sensi dell'articolo 28 del RGPD. Il trattamento sarà effettuato tramite l'utilizzo di procedure informatizzate ovvero mediante trattamenti manuali. I dati non

saranno oggetto di comunicazione e/o trasferimento verso paesi terzi e saranno conservati per il tempo strettamente necessario al perseguimento delle finalità per cui i dati sono trattati, nei limiti stabiliti da leggi o regolamenti e, comunque, non oltre il termine di 10 anni dall'ultimo atto o comunicazione inerente il procedimento stesso.

CLAUSOLA DA INSERIRE NEI CONTRATTI LADDOVE il Soggetto Terzo debba essere nominato Responsabile al trattamento dei dati personali ai sensi dell'articolo 28 del RGPD.

Articolo - Responsabile del Trattamento dei Dati Personali

Le attività oggetto del presente contratto implicano, da parte della Società, il trattamento dei dati personali di cui è Titolare Regione Lazio, ai sensi del Regolamento UE 2016/679 (di seguito definito per brevità anche il "RGPD").

Regione Lazio, ai sensi dell'articolo 28 del RGPD, riconosce che la Società dispone delle garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento dei dati personali di cui la Regione Lazio è Titolare soddisfi i requisiti e il pieno rispetto delle disposizioni previste dal RGPD.

Regione Lazio, in qualità di Titolare del Trattamento, con atto formale riportato in allegato (Allegato n. ...) al contratto e parte integrante dello stesso, nomina la Società quale Responsabile del trattamento dei dati ai sensi degli articoli 4, n. 8) e 28 del RGPD. Con la sottoscrizione del presente contratto, la Società si impegna ad accettare la nomina a Responsabile del Trattamento. La Società si impegna, inoltre, a sottoscrivere l'atto di nomina di cui all'Allegato n. ..., entro il termine di quindici giorni, dalla data di stipula del presente contratto.

Allegato n. ...

Oggetto "Nomina a Responsabile del trattamento dei dati personali ai sensi degli articoli 4, n. 8) e 28 del RGPD – Regolamento (UE) 679/2016 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".

Va compilato secondo il modello di cui allo schema "G".

Schema tipo - Accordo di contitolarità ai sensi dell'articolo 26 del Reg. (UE) 2016/679.

TRA

La Giunta della Regione Lazio (Soggetto designato: _____) (C.F.: _____ - P. IVA: _____) con sede in _____, PEC: _____, all'uopo rappresentato da _____

E

_____ (C.F.: _____ - P. IVA: _____) con sede in _____, PEC: _____, all'uopo rappresentato da _____

_____ (d'ora innanzi, entrambe le parti saranno identificate, congiuntamente, quali "Contitolari" o "Parti")

PREMESSO CHE

- 1) è in essere tra le Parti un progetto comune consistente in _____, il quale comporta la necessità di determinare congiuntamente le finalità e le modalità del trattamento dei dati personali coinvolti nella realizzazione del medesimo progetto comune;
- 2) che in data 25 maggio 2018 è divenuto pienamente operativo il Regolamento (CE) del 27 aprile 2016, n. 2016/679/UE (Regolamento del Parlamento europeo e del Consiglio, 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";
- 3) l'articolo 4, paragrafo 1, n. 7) del RGPD definisce quale titolare del trattamento "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali";
- 4) l'articolo 474, comma 1, del r.r. 1/2002 definisce quale titolare del trattamento dei dati personali, ai sensi dell'articolo 4, n. 7) e dell'articolo 24 del RGPD, la Giunta regionale, cui spettano tutte le attività demandate al titolare dal RGPD e, in particolare, l'adozione di misure tecniche e organizzative idonee a garantire e a consentire di dimostrare, che il trattamento dei dati personali è effettuato conformemente al RGPD;
- 5) la Giunta regionale, in qualità di titolare del trattamento, può prevedere, ai sensi dell'articolo _____

2-

⁷ Schema inserito dall'art. 22, comma 1, del r.r., 27 aprile 2023, n. 3, pubblicato sul Bur Lazio del 2 maggio 2023, n.35.

- quaterdecies* del d.lgs. 196/2003 e successive modificazioni, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano conferiti a persone fisiche, che operano sotto la propria autorità, espressamente designate;
- 6) a norma dell'articolo 26, paragrafo 1 del RGPD *“Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati”*;
 - 7) a norma dell'articolo 26, paragrafo 2 del RGPD *“L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato”*;
 - 8) è intenzione delle Parti contraenti regolamentare in modo trasparente i diritti e gli obblighi reciproci quali conseguono alla puntuale osservanza delle norme e dei principi contenuti nel RGPD, con particolare riguardo all'esercizio dei diritti dell'interessato, nonché i rispettivi ruoli nella comunicazione delle informazioni agli interessati, addivenendo alla sottoscrizione del presente accordo;

SI CONVIENE E SI STIPULA QUANTO SEGUE

Articolo 1 – Pattuizioni preliminari

1. Nell'ambito delle rispettive responsabilità come determinate dal presente Accordo, i Contitolari dovranno in ogni momento adempiere ai propri obblighi conformemente ad esso e in modo tale da trattare i dati senza violare le disposizioni normative vigenti e nel pieno rispetto delle linee guida e dei Codici di condotta applicabili, di volta in volta approvati dall'Autorità di controllo.
2. Resta inteso tra le Parti che, ai sensi dell'articolo 26, paragrafo 3, del Regolamento (EU) 2016/679, indipendentemente dalle disposizioni del presente Accordo, l'interessato potrà esercitare i propri diritti nei confronti di e contro ciascun Contitolare del trattamento.
3. In coerenza con la propria missione e i propri valori, i Contitolari si impegnano reciprocamente a proteggere i dati personali di ogni persona fisica che si trovasse ad avere contatto o ad operare con i medesimi (“Interessato”), nel rispetto dell'identità, della dignità di ogni essere umano e delle libertà fondamentali costituzionalmente garantite nel rispetto del RGPD relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione degli stessi.
4. Il presente accordo non determina l'insorgere di alcun diritto alla revisione di prezzi od altre forme di impegno, anche economico, già definiti tra le Parti, trattandosi di obblighi ed adempimenti derivanti da norme di legge già conosciute.
5. Il presente accordo annulla e/o sostituisce qualsivoglia regolazione pattizia esistente tra le Parti in relazione al medesimo oggetto, di talché, a far data dalla sua stipulazione, i loro rapporti saranno regolati esclusivamente dal presente accordo.
6. Qualsiasi modifica od integrazione del presente accordo potrà farsi soltanto per iscritto a

pena di nullità.

7. Il contenuto essenziale di questo accordo di Contitolarità è messo a disposizione dell'Interessato nella sezione Trasparenza del Portale di ciascuno dei Contitolari.

Articolo 2 - Oggetto del trattamento

1. I Contitolari dichiarano, in merito al trattamento dei Dati Personali, di condividere le decisioni relative alle finalità e modalità del trattamento di dati e, in particolare:
- le seguenti banche dati: dipendenti e collaboratori, _____;
 - le finalità del trattamento di dati personali, ciascuna con le proprie specificità legate alle attività concretamente svolte;
 - i mezzi del trattamento e le modalità del trattamento di dati personali;
 - la politica di conservazione dei dati;
 - lo stile e le modalità di comunicazione delle informative ai sensi dell'articolo 13 del RGPD;
 - la procedura di gestione dei consensi (ove necessari);
 - la designazione e la formazione dei soggetti autorizzati;
 - istruzioni sull'uso degli strumenti informatici per il personale;
 - la gestione delle comunicazioni e nomine dei responsabili ai sensi dell'articolo 28 del RGPD;
 - la tenuta dei registri del trattamento ai sensi dell'articolo 30 del RGPD;
 - le procedure nel caso di trasferimento dei dati fuori dall'UE;
 - gli strumenti ed i mezzi utilizzati per l'attuazione delle decisioni e in parte anche per l'operatività dei Contitolari, soprattutto in relazione alle misure di sicurezza fisiche, organizzative e tecniche;
 - l'approccio basato sul rischio;
 - i profili e la politica di sicurezza dei dati personali, la procedura del *Data Breach* e la procedura di valutazione di impatto sulla protezione dei dati personali (DPIA);
 - la gestione della procedura di esercizio dei diritti dell'Interessato;
 - una raccolta congiunta delle procedure sulla protezione dei dati personali attraverso la tenuta comune e gestione di un modello organizzativo.
2. La contitolarità è riferita al trattamento dei dati personali ed ha ad oggetto il trattamento di tutti i dati già presenti, in tutti gli archivi sia cartacei che informatizzati, e di tutti quelli che si acquisiranno in futuro. Il flusso dei dati personali sarà così strutturato: ____.
3. Con il presente accordo i Contitolari convengono che i dati personali presenti negli archivi sia cartacei che informatizzati, nonché quelli futuri, verranno trattati per le seguenti _____ finalità: _____.
4. Le attività alla base del presente accordo comportano il trattamento delle seguenti categorie di dati personali: __.
5. Le categorie di interessati sono: _____

Articolo 3 – Durata ed effetti conseguenti allo scioglimento del Contratto

1. Il presente accordo diviene efficace tra le parti all'atto della sua sottoscrizione e ha durata sino a _____, salvo proroga e fermi restando i casi di cessazione anticipata ai sensi della normativa vigente.
2. Il Trattamento dei dati personali in regime di contitolarità, pertanto, deve avere una durata non superiore a quella necessaria agli scopi per i quali i dati personali sono stati raccolti e tali dati devono essere conservati nei sistemi e nelle banche dati dei Contitolari

in una forma che consenta l'identificazione degli Interessati per un periodo di tempo non superiore a quello suddetto, fatto salvo che il trattamento e la conservazione dei dati medesimi ad opera di ciascuno dei Contitolari sia imposta dalla normativa vigente.

3. A seguito della cessazione del trattamento, nonché a seguito della cessazione del rapporto convenzionale sottostante, qualunque ne sia la causa, i Contitolari saranno tenuti a provvedere alla integrale distruzione dei dati personali trattati, salvi i casi in cui la conservazione dei dati sia richiesta dalla normativa vigente o il caso in cui si verificano circostanze autonome e ulteriori che giustifichino la continuazione del trattamento dei dati da parte dei singoli Contitolari, con modalità limitate e per il periodo di tempo a ciò strettamente necessario.
4. Ciascun Contitolare provvede a rilasciare apposita dichiarazione scritta contenente l'attestazione che, presso di sé, non esiste alcuna copia dei dati personali e delle informazioni trattate nell'ambito del progetto comune. Sul contenuto di tale dichiarazione l'altro Contitolare si riserva il diritto di effettuare controlli e verifiche volte ad accertarne la veridicità.

Articolo 4 – Obblighi tra le parti

1. La tutela dei dati personali è fondata sull'osservanza dei principi illustrati nel presente documento che i Contitolari si impegnano a diffondere, rispettare e far rispettare ai propri amministratori, ai propri dipendenti e collaboratori ed ai soggetti terzi con cui collaborano nello svolgimento della propria attività istituzionale. In particolare, i Contitolari sono impegnati affinché la politica della protezione dati personali, equamente consegua, sia compresa, attuata e sostenuta da tutti i soggetti, interni ed esterni, coinvolti nelle attività dei Contitolari, tenuto conto della loro realtà concreta, delle loro possibilità anche economiche e dei loro valori.
2. I Contitolari si impegnano a mantenere e garantire la riservatezza e la protezione dei dati personali raccolti, trattati e utilizzati in virtù del rapporto di contitolarità. In particolare, essi, anche disgiuntamente tra loro, si impegnano a:
 - a) comunicare e diffondere la propria politica in merito alla protezione dei dati personali;
 - b) prestare ascolto e attenzione a tutte le parti interessate proprie – a mero titolo esemplificativo: amministratori, personale dipendente e collaboratori, cittadini, utenti e beneficiari di prestazioni anche di natura assistenziale, fornitori, consulenti – e tenendo in debito conto le loro istanze in materia di trattamento di dati personali e dando pronto riscontro;
 - c) trattare i dati personali in modo lecito, corretto e trasparente in linea con i principi costituzionali e con la normativa vigente in materia, in particolare il RGPD, e solo per il tempo strettamente necessario alle finalità previste, comprese quelle per ottemperare agli obblighi di legge;
 - d) raccogliere i dati personali limitandosi a quelli indispensabili per effettuare le attività costituenti il progetto comune (dati personali pertinenti e limitati);
 - e) trattare i dati personali secondo i principi di trasparenza per le sole finalità specifiche ed espresse nelle proprie informative;
 - f) adottare processi di aggiornamento e di rettifica dei dati personali trattati per assicurarsi che i dati personali siano, per quanto possibile, corretti e aggiornati;
 - g) conservare e tutelare i dati personali di cui è in possesso con le migliori tecniche di preservazione disponibili;
 - h) garantire il continuo aggiornamento delle misure di protezione dei dati personali. Tale impegno sarà costantemente seguito nell'ambito del principio di responsabilizzazione mettendo in atto, con costanza, misure tecniche e organizzative adeguate e politiche idonee, per garantire ed essere in grado di dimostrare che il trattamento è effettuato

conformemente al RGPD, tenuto conto dello stato dell'arte, della natura dei dati personali custoditi e dei rischi ai quali sono esposti. Ciascun Contitolare eseguirà un monitoraggio periodico sul livello di sicurezza raggiunto, al fine di renderlo sempre adeguato al rischio;

- i) garantire il tempestivo recupero della disponibilità dei dati personali in caso di incidente fisico o tecnico
 - l) rendere chiare, trasparenti e pertinenti le modalità di trattamento dei dati personali e la loro conservazione in maniera da garantirne un'adeguata sicurezza;
 - m) favorire lo sviluppo del senso di responsabilizzazione e la consapevolezza dell'intera organizzazione verso i dati personali, visti come dati di proprietà dei singoli interessati;
 - n) assicurare il rispetto delle disposizioni legislative e regolamentari applicabili alla tutela dei dati personali aggiornando eventualmente la gestione della protezione dei dati personali;
 - o) prevenire e minimizzare, compatibilmente con le risorse disponibili, l'impatto di potenziali violazioni o trattamenti illeciti e/o dannosi dei dati personali;
 - p) promuovere l'inserimento della protezione dati personali nel piano di miglioramento continuo che il Contitolare persegue con i propri sistemi di gestione.
3. I Contitolari si impegnano con particolare riguardo all'esercizio dei diritti dell'Interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, ad uniformare le modalità, lo stile, i modelli e soprattutto le procedure per la protezione dei dati personali a favore dell'Interessato.
4. La comunicazione dei dati personali necessari a garantire il perseguimento del progetto comune avverrà curandone l'esattezza, la veridicità, l'aggiornamento, la pertinenza e la non eccedenza rispetto alle finalità per le quali sono stati raccolti e saranno successivamente trattati.

Articolo 5 - Incaricati e persone autorizzate

1. Ciascuno dei Contitolari dovrà identificare e designare le persone autorizzate ad effettuare operazioni di trattamento sui dati trattati nel perseguimento del progetto comune, identificando l'ambito autorizzativo consentito ai sensi dell'articolo 29 del RGPD e provvedendo alla relativa formazione, anche in merito ai principi di liceità e correttezza a cui deve conformarsi la politica per la protezione dei dati personali e il trattamento dei dati personali nonché al rispetto delle misure di salvaguardia adottate.
2. Ciascuno dei Contitolari garantisce che i propri dipendenti e collaboratori sono affidabili ed hanno piena conoscenza della normativa primaria e secondaria in materia di protezione dei dati personali.
3. Ciascuno dei Contitolari identifica un referente interno alla propria struttura, con il compito di relazionarsi con analogo soggetto designato dall'altra parte, a presidio del corretto adempimento di quanto previsto dal presente accordo. Il nominativo ed i dati di contatto del referente interno sono tempestivamente comunicati all'altra parte.

Articolo 6 - Responsabili del trattamento

1. Ciascuno dei Contitolari che ravvisasse la necessità di avvalersi di un responsabile del trattamento per l'esecuzione di specifiche attività richieste nell'ambito del progetto comune, è tenuto a comunicarlo all'altraparte con congruo preavviso.
2. Su tale responsabile del trattamento sono imposti, mediante un contratto od un altro atto giuridico previsto ai sensi del diritto dell'Unione o degli Stati membri, specifici obblighi in materia di protezione dei dati, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti previsti dalla vigente.

3. I rapporti tra i Contitolari e gli eventuali responsabili del trattamento restano disciplinati dall'articolo 28 del RGPD.

Articolo 7 – Valutazione d'impatto e Violazioni di dati personali

1. Nei casi previsti dall'articolo 35 del RGPD, la valutazione d'impatto sulla protezione dei dati personali ed il suo eventuale riesame, così come la consultazione preventiva di cui all'articolo 36 del RGPD, sono a carico di _____, il quale informa tempestivamente l'altro Contitolare della relativa necessità e dell'attività compiuta.
2. In eventuali casi di violazione della sicurezza dei dati personali che comportino, accidentalmente od in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati e tali da mettere a rischio i diritti e le libertà degli individui i cui dati personali sono trattati nel contesto del progetto comune, l'attività di coordinamento ai fini dell'adempimento degli obblighi di cui agli articoli 33 e 34 del RGPD è affidata a _____ il quale curerà la predisposizione di un apposito documento (*data breach policy*), ove non già esistente ed adottato.
3. Al verificarsi di una violazione di dati personali, il Contitolare non assegnatario dell'attività di coordinamento provvederà:
 - a) ad informare l'altro Contitolare tempestivamente ed in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione fornendogli tutti i dettagli della violazione stessa, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sugli Interessati coinvolti e le misure adottate per mitigare i rischi;
 - b) a fornire assistenza per far fronte alla violazione ed alle sue conseguenze, soprattutto in capo agli Interessati coinvolti. Esso, inoltre, si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive ed attuando tutte le azioni correttive approvate e/o richieste dal Contitolare assegnatario dell'attività di coordinamento. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al Trattamento eseguito.
4. Ciascun Contitolare si impegna a predisporre e a tenere aggiornato un registro interno delle violazioni di dati personali nonché a raccogliere e a conservare tutti i documenti relativi ad ogni violazione, compresi quelli inerenti alle circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Articolo 8 - Decisioni in merito ai trasferimenti internazionali di dati personali

1. Il presente accordo prevede che i dati personali saranno trattati all'interno del territorio dell'Unione Europea.
2. Nell'ipotesi in cui per questioni di natura tecnica e/o operativa si rendesse necessario avvalersi di soggetti ubicati al di fuori dell'Unione Europea, il trasferimento dei dati personali, limitatamente allo svolgimento di specifiche attività di Trattamento, sarà regolato in conformità a quanto previsto dal capo V del RGPD. Saranno quindi adottate tutte le cautele necessarie al fine di garantire la più totale protezione dei dati personali basando tale trasferimento: su decisioni di adeguatezza dei paesi terzi destinatari espresse dalla Commissione Europea; su garanzie adeguate espresse dal soggetto terzo destinatario ai sensi dell'articolo 46 del RGPD; sull'adozione di norme vincolanti d'impresa.

Articolo 9 - Condivisione della procedura per l'esercizio dei diritti dell'Interessato

1. I Contitolari designano congiuntamente un referente unitario quale punto di contatto per gli interessati. Le richieste di esercizio dei diritti e gli eventuali reclami presentati dagli interessati saranno gestiti in via esclusiva dal referente unico, contattabile ai recapiti che saranno resi noti unitamente al suo nominativo, restando in ogni caso inteso che gli interessati potranno esercitare i propri diritti nei confronti di ciascun Contitolare.
2. In particolare, qualora il referente unitario riceva richieste provenienti dall'Interessato, finalizzate all'esercizio dei propri diritti, esso dovrà:
 - darne tempestiva comunicazione scritta a ciascun Contitolare a mezzo di posta elettronica certificata, allegando copia delle richieste ricevute;
 - coordinarsi, ove necessario e per quanto di propria competenza, con le funzioni interne designate da ciascun Contitolare per gestire le relazioni con l'Interessato;
 - verificare la sussistenza dei presupposti e consentirne, differirne o rifiutarne l'esercizio, dandone tempestiva comunicazione scritta a ciascun Contitolare a mezzo di posta elettronica certificata.
3. Il referente unitario fornisce altresì assistenza a ciascuno dei Contitolari nell'ambito dei procedimenti amministrativi e giudiziari instaurati dall'Interessato o dall'Autorità di controllo in conseguenza dell'attività di cui al presente articolo.

Articolo 10 - Verifiche circa il rispetto delle regole di protezione dei dati personali

1. Ciascuno dei Contitolari riconosce all'altro il diritto di effettuare controlli (audit) relativamente alle operazioni aventi ad oggetto il trattamento dei dati personali nell'ambito del progetto comune. A tal fine, ciascuno dei Contitolari ha il diritto di disporre – a proprie cure e spese – verifiche a campione o specifiche attività di audit o di rendicontazione in ambito protezione dei dati personali e sicurezza, avvalendosi di personale espressamente incaricato a tale scopo, presso le sedi dell'altro.
2. Ciascuno dei Contitolari rende disponibile tutta la documentazione necessaria per dimostrare la conformità a tutti i suoi obblighi e per consentire la conduzione di audit, comprese le ispezioni, e per contribuire a tali verifiche.
3. Ciascuno dei Contitolari deve informare e coinvolgere tempestivamente l'altra parte in tutte le questioni riguardanti il trattamento dei dati personali ed in particolare nel caso di richieste di informazioni, controlli, ispezioni ed accessi da parte dell'Autorità di controllo;

Articolo 11 - Responsabilità per violazione delle disposizioni

I Contitolari si obbligano, in solido tra loro, a predisporre, attuare e aggiornare tutti gli adempimenti previsti in materia di protezione dei dati personali.

Articolo 12 - Responsabile della Protezione dei dati personali

1. Ciascuno dei Contitolari rende noto che il Responsabile della Protezione dei Dati personali (RPD o DPO) in conformità alla previsione contenuta nell'articolo 37, paragrafo 1, lettera a) del GDPR, è stato individuato quale soggetto idoneo:

Detto nominativo è stato altresì comunicato al Garante per la Protezione dei Dati Personali con procedura telematica.

Articolo 13 – Clausole nulle o inefficaci

Qualora una o più clausole del presente accordo divengano contrarie a norme imperative

o di ordine pubblico, esse saranno considerate come non apposte e non incideranno sulla validità dello stesso, fatto salvo il diritto di ciascuna parte di chiedere una modifica dell'accordo.

Articolo 14 – Comunicazioni

Qualsiasi comunicazione relativa al presente accordo dovrà essere data per iscritto ed a mezzo di posta elettronica certificata, con ricevuta di accettazione e conferma di consegna, purché inviati o consegnati all'indirizzo indicato in testa all'accordo. Tale indirizzo potrà essere modificato da ciascuna delle Parti, dandone comunicazione all'altra ai sensi del presente articolo.

Articolo 15 – Disposizioni finali

Per quanto non espressamente indicato nella presente Appendice, si rinvia a quanto previsto dal RGPD, dalle disposizioni normative vigenti, nonché ai provvedimenti dell'Autorità di controllo.

Per il Titolare del
trattamento

Il Soggetto designato
<inserire nome e

cognome>

Per il Contitolare del
trattamento

Il rappresentante

<inserire nome e

legale

cognome>