ALLEGATO NN (art. 476 ter)([1])

SCHEMI TIPO MODULISTICA

SCHEMA A([2])
(art. 474, c. 3)

ADDENDUM AL CONTRATTO DI LAVORO

CONFERIMENTO DI COMPITI E FUNZIONI IN QUALITA' 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, adeguare 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 2quaterdecies 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

SCHEMA B([3])
(art. 474, c. 5)

NOMINA SOGGETTI AUTORIZZATI([4])

(INTESTAZIONE DELLA STRUTTURA)

Oggetto: Nomina del soggetto autorizzato 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 autorizzati, 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

[4] Le parole "incaricato" e "incaricati" sono sostituite (ovunque ricorrano) rispettivamente dalle parole "autorizzato" e "autorizzati" dall'articolo 7, comma 1, lettere a) e b), del r.r. 4 aprile 2025, n. 8, pubblicato sul BUR Lazio 8 aprile 2025, n. 28.

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 autorizzato 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 autorizzati 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 autorizzato 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 autorizzato 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' autorizzato coadiuva il Titolare e/o il soggetto designato nell'aggiornamento del "Registro delle attività del Trattamento", indicato in premessa;
- l' autorizzato 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' autorizzato 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>

SCHEMA C

(art. 474, c. 7)

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>

SCHEMA D([5])

SCHEMA E([6])

SCHEMA F([7])

[5] 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

[6] Schema abrogato dall'articolo 8, comma 1, del r.r. 4 aprile 2025, n. 8, pubblicato sul BUR Lazio 8 aprile 2025, n. 28.

[7] Schema abrogato dall'articolo 9, comma 1, del r.r. 4 aprile 2025, n. 8, pubblicato sul BUR Lazio 8 aprile 2025, n. 28, precedentemente 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

SCHEMA G([1])

(art. 474, c. 2)

ATTO DI DISCIPLINA DEI TRATTAMENTI SVOLTI DAL RESPONSABILE DEL TRATTAMENTO PER CONTO DEL TITOLARE DEL TRATTAMENTO

AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 679/2016

NOTA ESPLICATIVA: scegliere l'opzione coerente:

- Allegato __ alla determinazione dirigenziale n.___del ___

oppure

- Allegato __ alla deliberazione di Giunta Regionale n._____del ___

TRA

La Giunta Regionale del Lazio, con sede in Via R. Raimondi Garibaldi 7– 00147 Roma, codice fiscale 80143490581, nella persona del/lla Dott./Dott.ssa _____in qualità di Direttore della *"Direzione _____"*, autorizzato alla sottoscrizione del presente contratto, in virtù dei poteri conferiti con la Deliberazione di Giunta Regionale n._____ del gg/mese/aaaa, (di seguito anche il "Titolare" o "Regione Lazio");

E

La _____<*indicare ragione e denominazione sociale della Società*>, con sede in _____, n. _____ – cap._____, città _____ nella persona del Dott./Dott.ssa _____, nella sua qualità di _____ in virtù dei poteri conferiti con _____ (di seguito anche la "Società", il "Responsabile" o il "Responsabile del trattamento");

VISTI

- 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 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;
- 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;

[1] Schema sostituito dall'articolo 10, comma 1, del r.r. 4 aprile 2025, n. 8, pubblicato sul BUR Lazio 8 aprile 2024, n. 28

- le Clausole Contrattuali Tipo (anche dette "SCC") tra Titolari del trattamento e Responsabili del trattamento, adottate a norma dell'articolo 28 del Regolamento (UE) 2016/679 (in seguito anche "GDPR") con la Decisione di esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021 che definisce le modalità con le quali il Responsabile del trattamento si impegna ad effettuare per conto del Titolare le operazioni di trattamento dei dati personali;
- 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;

NOTA ESPLICATIVA: aggiungere se ricorre la fattispecie

- 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, il quale prevede la 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");
- 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;

PREMESSO CHE

- la Giunta Regionale del Lazio, in qualità di Titolare del trattamento che svolge attività che comportano il trattamento di dati personali nell'ambito dei propri compiti istituzionalmente affidati, è tenuta a mettere in atto misure tecniche e organizzative, volte ad attuare in modo efficace i principi di protezione dei dati e adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
- le attività, erogate in esecuzione del Contratto <indicare riferimenti del contratto>, tra la Giunta Regionale del 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;
- 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;
- 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;

- 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;
- l'articolo 28, punto 6 del RGPD prevede 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";
- il presente contratto si basa sulle Clausole Contrattuali Tipo tra Titolari del trattamento e Responsabili del trattamento, adottate con la Decisione di esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021 sopra richiamata;
- 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;

Tutto ciò premesso, le parti stipulano e convengono quanto segue:

SEZIONE I

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.

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.

Clausola 3

Interpretazione

c) quando le presenti clausole utilizzano i termini definiti nel Regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui al Regolamento stesso;
d) le presenti clausole vanno lette e interpretate alla luce delle disposizioni del Regolamento (UE) 2016/679;
e) 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.

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.

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

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.

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 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.

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'adempiere 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.

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'adempiere, 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

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

Clausola 11

Ulteriori Disposizioni

Il Responsabile del trattamento dei dati personali nell'effettuare le operazioni di trattamento connesse all'esecuzione del suddetto contratto dovrà attenersi alle seguenti ulteriori 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 e per le finalità indicate nell'allegato II;
b) il Responsabile è autorizzato a procedere all'organizzazione di ogni operazione di trattamento dei dati nei limiti stabiliti dal contratto 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 in merito all'attribuzione delle funzioni di "Amministratore di sistema" di cui al provvedimento del 27 novembre 2008, e successive modificazioni ed integrazioni e, 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 si impegna ad 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 impegna ad attivare 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.

   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 deve adottare le politiche interne e, ai sensi dell'articolo 25 del RGPD, le misure che soddisfano i principi della protezione dei dati personali fin dalla progettazione di tali misure; adotta inoltre 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;

m) 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;

n) 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, va effettuata tramite PEC da inviare agli indirizzi protocollo@pec.regione.lazio.it, dpo@pec.regione.lazio.it, databreach@pec.regione.lazio.it; la stessa 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;

o) 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;

p) il Responsabile si impegna a 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;

q) 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 e ai patti e alle condizioni previste nel RGPD e nel presente contratto;

r) 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;

s) il Responsabile è tenuto ad individuare e verificare almeno annualmente l'ambito dei trattamenti consentiti alle persone autorizzate e ad impartire ai medesimi istruzioni dettagliate circa le modalità del trattamento;

t) 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;

u) 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):

_____

RESPONSABILE DEL TRATTAMENTO

Ragione sociale:

Sede legale:

Tel.:

Mail:

PEC:

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

_____

<Nome, qualifica e dati di contatto del referente>

CONTESTO DI RIFERIMENTO

I Rapporti tra le parti sono stati definiti con:

NOTA ESPLICATIVA: scegliere una o più delle seguenti opzioni:

- *deliberazione di Giunta Regionale n._____ del_____ avente ad oggetto "_____";*
- *determinazione dirigenziale n._____ del_____ avente ad oggetto "_____";*
- *contratto sottoscritto in data____, registrato in data al n._____;*
- *Altro_____.*

ALLEGATO II

Descrizione del trattamento

Categorie di interessati i cui dati personali sono trattati:

NOTA ESPLICATIVA: valorizzare la/le opzione/i coerente/i:

[ ] a) Dipendenti/Consulenti
[ ] b) Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
[ ] c) Associati, soci, aderenti, simpatizzanti, sostenitori
[ ] d) Soggetti che ricoprono cariche sociali
[ ] e) Beneficiari o assistiti
[ ] f) Pazienti
[ ] g) Minori
[ ] h) Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
[ ] i) Altro_____
(*Esempio:*
- cittadini,
- disabili,
- referenti aziende clienti;
- rappresentanti legali aziende potenziali;
- personale dipendente delle aziende clienti;
- etc etc da individuare).

***Categorie di dati personali trattati**:*

NOTA ESPLICATIVA: valorizzare la/le opzione/i coerente/i:

[ ] a) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
[ ] b) Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
[ ] c) Dati di accesso e di identificazione (username, password, customer ID, altro…)
[ ] d) Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
[ ] e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione Internet, altro…)
[ ] f) Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
[ ] g) Dati di profilazione
[ ] h) Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
[ ] i) Dati relativi all'ubicazione
[ ] l) Dati che rivelano l'origine razziale o etnica
[ ] m) Dati che rivelano le opinioni politiche
[ ] n) Dati che rivelano le convinzioni religiose o filosofiche
[ ] o) Dati che rivelano l'appartenenza sindacale

[ ] p) Dati relativi alla vita sessuale o all'orientamento sessuale
[ ] q) Dati relativi alla salute
[ ] r) Dati genetici
[ ] s) Dati biometrici
[ ] t) Altro_____

[Esempio:
eliminare e/o aggiungere in base ai dati personali effettivamente trattati:
Dati comuni:
- caratteristiche individuali (ad es. peso, altezza ecc.),
- codice fiscale e altri codici identificativi (matricola lavoratore);
- indirizzo di residenza e/o domicilio,
- n. carta d'identità,
- indirizzo IP,
- codice IBAN,
- n. di targa,
- dati personali contenuti nel cedolino dello stipendio;
- dati reddituali e compensi percepiti;
- informazioni presenti nei curriculum vitae;
- Informazioni aventi natura "soggettiva" quali opinioni o valutazioni, anche espresse con codici o in termini numerici (valutazioni della prestazione/capacità lavorativa/l'affidabilità; notizie contenute nelle relazioni/consulenze/perizie; esito di test psicologici/disegni; informazioni contenute sotto forma di testo libero come un messaggio di posta elettronica; etc)]

[ ] u) Dati sensibili/particolari trattati (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, (esempio 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):

NOTA ESPLICATIVA: indicare la tipologia di dati particolari trattata:

_____

(Esempio:
Dati sensibili/particolari:
- origine razziale o etnica
- opinioni politiche
- convinzioni religiose o filosofiche
- appartenenza sindacale
- dati genetici
- dati biometrici (immagini registrate da un sistema di videosorveglianza);
- dati relativi alla salute: idoneità al lavoro (compreso informazioni di cui è vietata in ogni caso la pubblicazione a "erogazione ai sensi della legge 104/1992"; "soggetto portatore di handicap"; "anziano non autosufficiente"; "indici di autosufficienza nelle attività della vita quotidiana"; "contributo per ricovero in struttura sanitaria" o per "assistenza sanitaria")
- dati relativi alla vita sessuale o all'orientamento sessuale;

Con riferimento alle categorie particolari di dati (cd. sensibili), il Responsabile del trattamento si impegna ad adottare le prescrizioni contenute nel Provvedimento del Garante Privacy n. 146 del 5 giugno 2019 (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 176 del 29 luglio 2019) per il trattamento di:

NOTA ESPLICATIVA: valorizzare la/le opzione/i coerente/i:

☐ categorie particolari di dati nei rapporti di lavoro, le Prescrizioni di cui all'aut. gen. n. 1/2016;
☐ categorie particolari di dati da parte degli organismi di tipo associativo, delle fondazioni, delle chiese e associazioni o comunità religiose, le Prescrizioni di cui all'aut. gen. n. 3/2016;
☐ categorie particolari di dati da parte degli investigatori privati, le Prescrizioni di cui all'aut. gen. n. 6/2016;
☐ dati genetici e i campioni biologici, le Prescrizioni di cui all'aut. gen. n. 8/2016;
☐ dati personali per scopi di ricerca scientifica, le Prescrizioni di cui all'aut. gen. n. 9/2016;
☐ nessuna delle Prescrizioni di cui sopra.
Il Responsabile deve essere in grado di dimostrare, laddove necessario, il rispetto delle succitate specifiche prescrizioni.

[ ] v) Dati giudiziari:
- informazioni relative a condanne penali e a reati, o a connesse misure di sicurezza.

Natura del trattamento:

Il trattamento è svolto in maniera:

NOTA ESPLICATIVA: valorizzare la/le opzione/i coerente/i:

[ ] manuale;

[ ] informatizzata

[ ] Altro

Finalità per le quali i dati personali sono trattati per conto del Titolare del trattamento e relative basi giuridiche

I dati devono essere raccolti per le seguenti finalità determinate, esplicite e legittime, e quindi trattati secondo modalità compatibili con tale finalità (art. 5 par. 1 lett. b):

NOTA ESPLICATIVA: inserire le finalità del trattamento

Se il Responsabile del trattamento viola il Regolamento (UE) 2016/679, ovvero agisce in modo difforme o contrario rispetto alle legittime istruzioni impartite dal Titolare, determinando le finalità e i mezzi del trattamento ai sensi dell'art. 28, paragrafo 10, del GDPR è da considerarsi Titolare del trattamento in questione.

Durata del trattamento:

Il trattamento potrà essere svolto fino al termine del rapporto contrattuale definito negli atti sopra richiamati fatti salvi eventuali proroghe e rinnovi.

Al termine o alla cessazione di efficacia del contratto il Responsabile del trattamento deve restituire al Titolare tutti i dati personali trattati per suo conto e cancellare le eventuali copie esistenti in suo possesso (su qualsiasi supporto) secondo le istruzioni ricevute dal Titolare, certificando altresì a quest'ultimo di averlo fatto, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali trattati.

Il Titolare si riserva la facoltà di disporre tale verifica tramite un revisore, anche di terza parte, a condizione che non abbia una relazione competitiva con il Responsabile stesso.

È esplicitamente esclusa la pratica del "blocco da fornitore" (c.d. *Vendor lock-in*).

Finché i dati non sono restituiti e cancellati, il Responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

NOTA ESPLICATIVA: In caso di trattamenti da parte di (sub-)Responsabile/i del trattamento, specificare di seguito gli elementi contenuti nel presente allegato II (categorie di interessati, categorie di dati, natura del trattamento, ecc.) riferiti ad ogni singolo sub-Responsabile.

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 e devono prevedere anche le specifiche misure da adottare al fine di fornire assistenza al Titolare del trattamento. Le misure si devono riferire alla specifica fattispecie. Eliminare le misure non pertinenti e non applicabili e eventualmente aggiungere misure non previste.

Si descrivono di seguito le misure di sicurezza tecniche e organizzative che il Responsabile del trattamento deve mettere in atto, (comprese le eventuali certificazioni in possesso del Responsabile del trattamento pertinenti, ove presenti), 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.

1) PRIVACY BY DESIGN E BY DEFAULT

Il Responsabile del trattamento deve rispettare i principi di protezione dei dati fin dalla progettazione (privacy by design) e protezione dei dati per impostazione predefinita (privacy by default) di cui all'art. 25 GDPR comunicando al Titolare le soluzioni individuate e adottate per rispettare tali principi (cfr. Considerando 78 GDPR).

In attuazione di tali principi, il Responsabile del trattamento, anche quando utilizza sistemi tecnologici realizzati da terzi, dovrà eseguire un'analisi dei rischi e accertarsi

che le funzionalità corrispondano alle finalità del trattamento individuate che abbiano una specifica base giuridica.

2) ELENCO AGGIORNATO SUB-RESPONSABILI

Quando il primo Responsabile del trattamento è autorizzato a ricorrere a un altro Responsabile del trattamento per l'esecuzione di specifiche attività, a prescindere dal carattere specifico o generale dell'autorizzazione preliminare scritta del Titolare del trattamento, il primo Responsabile deve tenere un elenco aggiornato degli altri (sub-)responsabili. Su richiesta del Titolare e/o e in caso di accertamenti anche da parte del Garante, il primo Responsabile del trattamento gli fornisce prontamente e non oltre 24 ore copia dell'elenco aggiornato.

3) ATTIVITA' DI REVISIONE, COMPRESE LE ISPEZIONI

Su richiesta del Titolare del trattamento, a intervalli annuali o se vi sono indicazioni di inosservanza, il Responsabile del trattamento consentirà e contribuirà alle attività di revisione delle attività di trattamento di cui alle presenti clausole. Nel decidere in merito a un riesame o a un'attività di revisione, il Titolare del trattamento potrà tenere conto delle pertinenti certificazioni in possesso del Responsabile del trattamento.

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 di almeno 72 ore.

4) TRASFERIMENTO DATI EXTRA UE

È generalmente vietato il trasferimento di dati da parte del Responsabile del trattamento verso un paese terzo o un'organizzazione internazionale, ovvero a sub-responsabili del trattamento che non rientrano nell'ambito di applicazione territoriale del GDPR, compresi trasferimenti successivi. Il Responsabile del trattamento si assicura che anche il sub-Responsabile del trattamento non effettui trasferimenti di dati verso un paese terzo o un'organizzazione internazionale. Il Primo Responsabile, nella scelta di ulteriori fornitori, deve privilegiare, a parità di garanzie in materia di protezione dei dati personali, fornitori che sono situati sul territorio nazionale e dell'Unione europea, istruendoli sulla necessità di conservare i dati all'interno dell'Unione stessa.

In via del tutto residuale, il Primo Responsabile può ricorrere a responsabili situati in Paesi terzi, nel rispetto delle misure previste dal capo V del GDPR.

In presenza di una decisione di adeguatezza, il Primo Responsabile del trattamento è tenuto in ogni caso a chiedere specifica autorizzazione al Titolare, in considerazione degli obblighi connessi ai trasferimenti internazionali di cui al capo V del GDPR.

Ad ogni modo, il trasferimento di dati extra UE può essere effettuato soltanto su istruzione documentata del Titolare del trattamento o per adempiere a 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 GDPR.

5) AMMINISTRATORE DI SISTEMA

Nel caso in cui il Responsabile effettua trattamenti, anche in parte, mediante strumenti elettronici, si impegna ad individuare e a designare gli Amministratori di Sistema ("AdS"), conformandosi altresì, nell'affidamento di tale incarico, a tutto quanto previsto dal provvedimento del Garante Privacy del 27 novembre 2008 [doc. web n. 1577499] (G.U. n. 300 del 24 dicembre 2008), come modificato in base al provvedimento del 25 giugno 2009.

Le persone fisiche designate AdS considerate come tali sono le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti nonché altre figure equiparabili quali gli amministratori di base dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
Delle misure e degli accorgimenti prescritti con la designazione di Amministratore di Sistema il Responsabile del trattamento è tenuto a darne la prova; deve altresì conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema, tenendo costantemente aggiornato tale documento interno (come da Allegato V) e in caso di accertamenti anche da parte del Garante fornire prontamente e comunque entro 24 ore il medesimo documento al Titolare.

6) MISURE MINIME E MISURE AGID:
Il Responsabile deve dotarsi delle misure minime di sicurezza per limitare il rischio di attacchi informatici.
Per il tramite degli Amministratori di Sistema designati, si impegna a garantire di default le modalità tecniche previste dall'Allegato B del Codice Privacy (Disciplinare tecnico in materia di misure di sicurezza), seppur oggi abrogato.
Il Responsabile si impegna ad installare e mantenere aggiornate, sugli strumenti elettronici oggetto del contratto, tutte le misure e gli accorgimenti eventualmente prescritti dai Provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali (GPDP), dall'Agenzia per l'Italia Digitale (AGID) e dall'Agenzia per la Cybersicurezza Nazionale (ACN), applicabili al servizio commissionato, nonché le ulteriori misure di sicurezza previste nel contratto di fornitura.
Nello specifico, il Responsabile si impegna al rispetto e alla dimostrazione di quanto previsto dall'AGID con:
le Linee guida - Sicurezza nel Procurement ICT (Pubblicato il 19/05/2020 - Aggiornato il 19/05/2020)
Linee guida per lo sviluppo del software sicuro (Ultimo aggiornamento 06-05-2020), disponibile alla seguente url: https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro
le «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)». (17A03060) (G.U Serie Generale n.103 del 05-05-2017), disponibili anche alla seguente url: https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

7) MISURE ULTERIORI:

NOTA ESPLICATIVA: adattare alla singola fattispecie – eliminare le misure non pertinenti e non applicabili.

Il Responsabile del trattamento, ferma la dimostrazione della loro adozione, si impegna a mettere in atto e adottare le seguenti ulteriori e più specifiche misure tecniche e organizzative:
a) mezzi che permettono di garantire la confidenzialità, l'integrità, la disponibilità e la resilienza costante dei sistemi e dei servizi di trattamento.
a.1) la capacità di assicurare la riservatezza dei dati trattati, facendo in modo che le password relative alle utenze dei soggetti autorizzati siano di lunghezza non inferiore a otto caratteri e siano sottoposte a un controllo automatico di qualità che impedisca l'uso di password "deboli" e che le medesime password siano modificate almeno al primo utilizzo;
a.2) la capacità di assicurare la riservatezza dei dati trattati, facendo in modo che l'autenticazione dei soggetti autorizzati avvenga tramite un processo di autenticazione multifattoriale (MFA);

a.3) la capacità di contrastare efficacemente attacchi informatici di tipo brute force sul sistema di autenticazione online, anche introducendo limitazioni al numero di tentativi infruttuosi di autenticazione;
a.4) crittografia dei dati che i dispositivi del fornitore/Responsabile (computer, portatili, tablet, ecc.) devono rispettare;
a.5) l'accesso alla rete locale dell'amministrazione da parte del fornitore/Responsabile deve essere configurato con le abilitazioni strettamente necessarie alla realizzazione di quanto contrattualizzato, vale a dire consentendo l'accesso esclusivamente alle risorse necessarie. L'accesso dall'esterno mediante VPN deve essere consentito, solo se strettamente necessario, utilizzando account VPN personali configurati e abilitati opportunamente. Gli accessi dovranno poter essere tracciati per eventuali successivi audit;
a.6) nelle forniture di sviluppo e manutenzione, l'utilizzo dei dati dell'amministrazione per la realizzazione di quanto contrattualizzato deve essere consentito esclusivamente su server/database di sviluppo nei quali sono stati importati i dati necessari per gli scopi del progetto. Tale misura consiste nel gestire l'accesso ai server e ai DB in modo da rispettare questa regola generale, tracciando le eventuali eccezioni che dovessero verificarsi.
b) mezzi che permettono di ristabilire la disponibilità dei dati a carattere personale e l'accesso a questi nei tempi appropriati in caso di incidente fisico o tecnico;
c) rilevare e detenere a norma di legge copia dei log di accesso all'applicativo e di sistema;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
e) nomina di un DPO, nei casi previsti dall'art. 37 GDPR ovvero per i soggetti privati obbligati alla sua designazione. Nel caso in cui il Responsabile del trattamento ritenesse tale nomina non obbligatoria, alla luce del principio di accountability è tenuto a dare la prova della mancanza dei criteri di nomina (cfr. Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato, punto nn. 3 e 4);
f) poter dimostrare che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati, se non è istruito in tal senso dal Responsabile del trattamento e non abbia ricevuto idonea formazione;
g) una procedura per la gestione degli incidenti di sicurezza e delle violazioni di dati personali (cd. "Data Breach");
h) sottoscrizione di polizze assicurative che tengano conto dei risarcimenti danni di cui all'art. 82 del GDPR con massimali adeguati;
i) una Valutazione del Rischio per la sicurezza dei dati che tenga in considerazione i rischi presentati dal trattamento come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati (cfr. considerando 83 GDPR).
l) Sulle reti messe a disposizione dal fornitore devono essere presenti di dispositivi di sicurezza perimetrale con funzioni di sicurezza (ad esempio Firewall e sistemi di Network Detection ed Event & Log Monitoring, SIEM, ecc.) necessari a rilevare e contenere eventuali incidenti di sicurezza ICT e in grado di gestire gli IoC (Indicator of Compromise);
m) Il fornitore deve usare protocolli cifrati e meccanismi di autenticazione nell'ambito dei servizi erogati;
n) Qualora il fornitore subisca un attacco, in conseguenza del quale vengano compromessi sistemi del committente da lui gestiti, deve farsi carico delle bonifiche del caso, e riportare i sistemi in uno stato di assenza di vulnerabilità.
o) Il fornitore si impegna a trattare, trasferire e conservare le eventuali repliche dei dati oggetto di fornitura, ove autorizzate dalle amministrazioni, sempre all'interno del territorio dell'UE.

7.1) Verificare la documentazione finale di progetto

Alla fine di ogni singolo progetto, il Titolare verifica che il fornitore/Responsabile rilasci la seguente documentazione:

- documentazione finale e completa del progetto;
- manuale di installazione/configurazione;
- report degli Assessment di Sicurezza eseguiti con indicazione delle vulnerabilità riscontrate e le azioni di risoluzione/mitigazione apportate;
- "libretto di manutenzione" del prodotto (software o hardware), con l'indicazione delle attività da eseguire per mantenere un adeguato livello di sicurezza del prodotto realizzato o acquistato. In particolare, nel libretto di manutenzione deve essere indicato:
    - produttore e versione dei prodotti software utilizzati (ad esempio web server, application server, CMS, DBMS), librerie, firmware;
    - indicazioni per il reperimento dei Bollettini di Sicurezza dei singoli produttori di hardware/software;
    - indicazioni sul processo di installazione degli aggiornamenti sicurezza;
    - documento di EoL (documento che contiene indicazione dei prodotti utilizzati e relativo fine vita/rilascio aggiornamenti sicurezza).

7.2) Distruzione del contenuto logico (wiping) dei dispositivi che vengono sostituiti

Nelle acquisizioni di attività di conduzione CED o di gestione di parchi di PC (fleet management), occorre verificare che l'hardware dismesso venga cancellato e distrutto in modo sicuro, evitando rischi che dati critici possano restare erroneamente memorizzati sull'hardware dismesso stesso.
Nei rapporti contrattuali col Responsabile va definito un processo di verifica strutturato che deve almeno prevedere:

- la consegna di un verbale di avvenuta distruzione da parte del fornitore;
- nel caso di sistemi critici, la programmazione di una azione ispettiva o di altri sistemi di monitoraggio o controllo.

7.3) Manutenzione - aggiornamento dei prodotti:

È fatto obbligo agli amministratori di sistema di eseguire gli aggiornamenti ogni qualvolta sui siti dei produttori vengono rilasciati patch e correzioni per problemi di vulnerabilità.

7.4) Vulnerability Assessment

Il Fornitore/Responsabile deve eseguire, su beni e servizi classificati critici ed esposti sul web, un Vulnerability Assessment a cadenza almeno annuale, e ogniqualvolta si apportano modifiche alla configurazione software/hardware.

7.5) Altre misure tecniche e organizzative:

NOTA ESPLICATIVA: eliminare quelle non pertinenti e aggiungere quelle mancanti:

- 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;
- 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.

8) PERSONALE AUTORIZZATO:

Il Responsabile del trattamento si impegna a produrre e aggiornare in caso di modifiche l'elenco degli operatori autorizzati singolarmente e opportunamente formati in materia di privacy (ivi inclusi gli opportuni aggiornamenti normativi), impartendo per iscritto specifiche istruzioni per trattare i dati degli utenti, nell'ambito della propria attività e con i limiti di legge, curando, in particolare, il profilo della sicurezza di accesso e dell'integrità dei dati ai sensi dell'art. 29 del GDPR. Inoltre, il Responsabile s'impegna a stabilire le modalità di accesso ai dati e l'organizzazione del lavoro degli autorizzati al trattamento, avendo cura di adottare preventivamente misure organizzative adeguate al rischio per diritti e libertà delle persone fisiche. Inoltre, deve garantire che le persone autorizzate siano state istruite sulla procedura di gestione degli incidenti di sicurezza e sulla gestione delle violazioni di dati personali. Il Titolare può richiedere una prova documentata, al fine di verificare tali adempimenti.

9) REGISTRO DEL TRATTAMENTO:

Il Responsabile del trattamento, anche laddove non rientri nelle casistiche definite dall'art. 30, parr. 2 e 5, del GDPR, tiene per iscritto un Registro delle attività relative ai trattamenti svolti per conto del Titolare.

10) ASSISTENZA AL TITOLARE:

In generale, il Responsabile del trattamento è tenuto ad assistere il Titolare nel garantire il rispetto degli obblighi a cui è vincolato quest'ultimo e a rispondere prontamente e comunque non oltre 72 ore dalle richieste di informazioni del Titolare del trattamento.
Il Responsabile comunicherà ogni informazione utile al fine di assistere il Titolare nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti. Qualora il Responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti, informa senza indugio e comunque non oltre 72 ore il Titolare affinché possa garantire che i dati personali siano esatti e aggiornati.

Nel caso in cui riceva richieste degli interessati per l'esercizio dei loro diritti, il Responsabile notifica prontamente e comunque non oltre 72 ore al Titolare del trattamento qualunque richiesta ricevuta dall'interessato in quanto non è autorizzato a rispondere egli stesso alla richiesta.
Inoltre, il Responsabile del trattamento assiste il Titolare nel garantire il rispetto degli obblighi imposti a quest'ultimo ai sensi dell'articolo 32 del GDPR, fornendogli, tra l'altro, le informazioni riguardanti le misure tecniche e organizzative da questi adottate in conformità all'articolo 32 medesimo, unitamente a tutte le altre informazioni necessarie al Titolare del trattamento per conformarsi agli obblighi a lui imposti per garantire un livello di sicurezza adeguato al rischio.
Il Responsabile si impegna a predisporre, condividere e aggiornare periodicamente la valutazione del rischio per la sicurezza dei dati e la valutazione di impatto sulla protezione dei dati e, comunque, a redigere uno o più atti di documentazione delle scelte, dando atto della conformità alla normativa sulla protezione delle persone con riguardo al trattamento dei dati e alla circolazione dei dati., ovvero indicando che il trattamento presenterebbe un rischio elevato.
Laddove la valutazione di impatto sulla protezione dei dati presentasse un rischio elevato, anche in fase di consultazione con la/le autorità di controllo competenti, il Responsabile assisterà il Titolare del trattamento per adottare le misure adeguate per attenuare il rischio.
Il Responsabile si impegna ad adibire apposito ufficio/referente, segnalando un punto di contatto diretto al Titolare del trattamento, alle incombenze relative alla notificazione e comunicazioni previste dal GDPR.

11) COMUNICAZIONE E REGISTRO DI INCIDENTI DI SICUREZZA E DI VIOLAZIONI DI DATI PERSONALI

In caso di incidente di sicurezza e/o di violazione dei dati personali (cd. Data Breach), senza indugio il Responsabile del trattamento coopera con il Titolare e lo assiste nell'adempimento degli obblighi, ai sensi degli artt. 33 e 34 GDPR.
Nel caso di incidente di sicurezza e/o di una violazione dei dati personali trattati dal Responsabile del trattamento, quest'ultimo ne dà comunicazione al Titolare senza ingiustificato ritardo e comunque non oltre 24 ore dopo esserne venuto a conoscenza. La comunicazione iniziale contiene le informazioni disponibili in quel momento e le altre informazioni sono fornite non appena disponibili, senza ingiustificato ritardo. Il Responsabile documenta qualsiasi incidente di sicurezza e/o di violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.
Il Responsabile deve mantenere un Registro degli incidenti di sicurezza, anche qualora non vi siano delle violazioni dei dati personali, per coadiuvare il Titolare nel suo obbligo relativo al paragrafo 5 dell'art. 33 del GDPR.

A seguito del verificarsi di detti incidenti il Titolare può:
- effettuare le succitate attività di revisione, comprese le ispezioni;
- prescrivere l'adozione di misure di sicurezza aggiornate e/o ulteriori anche rispetto a quelle previste dal presente accordo;
- attivare azioni di rivalsa nei confronti del Responsabile;
- applicare le penali contrattuali;
- risolvere il contratto (cfr. la succitata Clausola 10).

Il Responsabile deve adottare procedure tecniche e organizzative volte alla gestione di eventuali incidenti di sicurezza e di violazioni di dati personali; deve disporre altresì di una struttura per la prevenzione e gestione degli incidenti informatici e delle violazioni di dati personali con il compito d'interfacciarsi con le analoghe strutture del Titolare.

12) LINEE GUIDA E PROVVEDIMENTI DELL'AUTORITA' GARANTE PRIVACY:

NOTA ESPLICATIVA: eliminare i provvedimenti non pertinenti e aggiungere quelli applicabili alla fattispecie ove esistenti:

Il Responsabile del trattamento s'impegna a mettere in atto le misure tecniche e organizzative previste da Linee Guida e provvedimenti adottati dalle Autorità europee in materia di protezione dei dati personali, con particolare riferimento a quelli adottati dal Garante Privacy italiano quali:
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015 ((Pubblicato sulla Gazzetta Ufficiale n. 179 del 4 agosto 2015);
- Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008 (G.U. n. 287 del 9 dicembre 2008);
- Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali - 27 novembre 2008 (G.U. n. 287 del 9 dicembre 2008);
- Posta elettronica e internet – 1° marzo 2007;

_____
- Altro

In materia di protezione di dati personali il Responsabile del trattamento si impegna a rispettare e mettere in atto:

☐ Linee guida in materia di conservazione delle password (ACN & GPDP, Provvedimento n. 594 del 7 dicembre 2023)
☐ Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021
☐ Provvedimento in materia di videosorveglianza - 8 aprile 2010;
☐ Adempimenti semplificati per il customer care (inbound) - 15 novembre 2007
☐ RFID Etichette intelligenti: prescrizioni - 9 marzo 2005;
☐ Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014;
☐ Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro - 4 ottobre 2011;
☐ Sistemi di videosorveglianza per il controllo della procedura di raccolta del campione urinario a fini certificatori o di cura della salute 15 maggio 2013;
☐ Trattamento di dati personali per profilazione on line - 19 marzo 2015;
☐ Provvedimento generale in materia di trattamento dei dati personali nell'ambito dei servizi di mobile remote payment – 22 maggio 2014 (Pubblicato sulla Gazzetta Ufficiale n. 137 del 16 giugno 2014)
☐ Trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati – 15 maggio 2014;
☐ Dossier sanitario - 4 giugno 2015
☐ Svolgimento di indagini di customer satisfaction in ambito sanitario - 5 maggio 2011;
☐ Le norme del Codice Privacy non in contrasto con il Regolamento Europeo e non oggetto di abrogazione/modifica
☐ per i trattamenti di dati sensibili svolti dai soggetti pubblici (quelli di cui all'art. 6.1.c) ed e) del GDPR), in considerazione dell'art. 6.2 del GDPR saranno valutate le

misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 del Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

☐ Le buone prassi in materia di sicurezza o Privacy proposte da ENISA (Agenzia europea per la sicurezza delle reti e dell'informazione);

☐ Le buone prassi in materia di sicurezza o Privacy proposte da associazioni:
(Esempio:
- Center for Internet Security;
- Critical Security Controls for Effective Cyber Defense;
- CIS Benchmarks;
- Altro)

☐ Altro_____

13) CERTIFICAZIONI PERTINENTI:

Per attestare l'adeguatezza delle misure di sicurezza adottate (cfr. art. 28.5 del GDPR), il Responsabile del trattamento aderisce a specifici codici di condotta o a schemi di certificazione come di seguito:

NOTA ESPLICATIVA: valorizzare le certificazioni possedute ed eliminare quelle non pertinenti.

a) visto l'art. 43.1.b) del GDPR, che prevede una certificazione accreditata IS0 17065, il Responsabile del trattamento ha ottenuto il rilascio delle seguenti certificazioni:

[ ] ISDP©10003 (ITA);
[ ] Carpa (LU);
[ ] Europrivacy (LU);
[ ] Europrice (D);
[ ] altra certificazione accreditata IS0 17065 in materia di protezione dei dati personali;

b) visto l'art. 32 (nonché l'art. 25) del GDPR, anche se la norma di accreditamento ISO 17021-1 non è da considerarsi valida ai fini del GDPR, pur tuttavia molti argomenti trattati hanno riscontro in specifici requisiti di legge europei e nazionali, il Responsabile del trattamento possiede le seguenti certificazioni:

[ ] ISO/IEC 27001;
[ ] ISO/IEC 22301;
[ ] ISO/IEC 20000-1;
[ ] ISO/IEC 27701;
[ ] ISO/IEC 27017 e ISO/IEC 27018, integrate, come addendum alla Norma ISO/IEC 27001;
[ ] altra certificazione accreditata (e/o integrata) come addendum alla Norma ISO/IEC 27001;
[ ] altra certificazione accreditata in materia di privacy e gestione della sicurezza delle informazioni;

c) il Responsabile del trattamento ha ottenuto inoltre le seguenti certificazioni:

[ ] ISO 9001;
[ ] ISO 13485;

[ ] altra certificazione accreditata in materia di gestione della qualità;

[ ] ALTRO_____.

d) visto l'art. 106, comma 8, del D. Lgs. n. 36/2023, "Garanzie per la partecipazione alla procedura", ai fini del presente affidamento il Responsabile del trattamento ha ottenuto tra le norme di certificazione ivi previste le seguenti:

[ ] ALTRO_____.

14) INFORMAZIONI SUL TRATTAMENTO E CONSENSO DELL"INTERESSATO:

Nel caso in cui il/i trattamenti oggetto del presente contratto si basino sul consenso l'informativa redatta dal Titolare del trattamento deve essere:
☐ Consegnata a mano all'interessato;
☐ Pubblicata online sul sito XXXX;
☐ Non applicabile;
☐ Consegnata dal Titolare stesso;
☐ Altro (specificare nello spazio sottostante).

Gestione del consenso.

Quando il trattamento si fonda sulla base giuridica del consenso "libero" dell'interessato viene fornita dal Titolare specifica informativa e viene richiesto apposito consenso in mancanza del quale non si procederà al relativo trattamento.
Il consenso va raccolto e registrato tramite:
☐ Informativa e modulo raccolta consenso cartaceo redatto, reso e raccolto a cura del Titolare del trattamento;
☐ Informativa e modulo raccolta consenso cartaceo redatto a cura del Titolare e reso/raccolto da XXXX che dovrà consegnare la modulistica firmata al Titolare del trattamento;
☐ Raccolta e registrazione del consenso tramite sistema informatico XXXX;
☐ Altro;
☐ Non applicabile.

ALLEGATO IV

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

Il Responsabile del Trattamenti si avvale dei seguenti sub-Responsabili del trattamento:

***Sub* Responsabile del trattamento (Nome, ragione sociale, sede legale)**	**Descrizione del trattamento** (compresa la delimitazione delle responsabilità, qualora siano	**Attività svolte per conto del primo Responsabile**	**Dati di contatto del referente**

	autorizzati più sub-Responsabili)		

ALLEGATO V
Disciplina dei servizi di Amministratore di Sistema

NOTA ESPLICATIVA: da utilizzare quando le prestazioni contrattuali implichino l'erogazione di servizi di amministrazione di sistema

Quando le prestazioni contrattuali implichino l'erogazione di servizi di amministrazione di sistema le persone fisiche designate AdS sono individuate in base ai criteri forniti nel provvedimento del Garante Privacy del 27 novembre 2008 [doc. web n. 1577499] (G.U. n. 300 del 24 dicembre 2008), come modificato in base al provvedimento del 25 giugno 2009, che considera come tali le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti nonché altre figure equiparabili quali gli amministratori di base dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
Il Responsabile del trattamento tiene un registro aggiornato di tutti gli Amministratori di Sistema (AdS) nonché di quegli Amministratori di Sistema la cui attività riguarda anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori (AdS/L) nominati al momento della sottoscrizione del presente contratto. Ciò anche al fine di consentire al Titolare di rendere nota o conoscibile l'identità degli AdS/L in relazione ai diversi servizi informatici cui questi sono preposti.
Il Responsabile tiene costantemente aggiornato il registro nella forma di seguito indicata e informa per iscritto il Titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di Amministratori di Sistema.

Col. 1 Cognome e Nome della persona fisica designata AdS	**Col. 2** Società e Organizzazione di appartenenza	**Col. 3** Ubicazione di lavoro dell'Ads	**Col. 4** Funzioni attribuite all'AdS: ambito di operatività per settori o per aree operative (*job description*)	**Col. 5** Banca dati gestita e trattamenti consentiti	**Col. 6** La persona in questione tratta informazioni di carattere personale dei lavoratori (AdS/L)?	
					SI	NO

Legenda:
Colonna 1: Cognome e Nome: cognome e nome della persona fisica che è stata designata, per iscritto, Amministratore di Sistema
Colonna 2: *Organizzazione di appartenenza*: indica la ragione sociale della Società di appartenenza dell'AdS e gli estremi identificativi dell'unità organizzativa nella quale l'AdS opera.
Colonna 3: Ubicazione: indica l'ubicazione di lavoro nella quale l'AdS svolge normalmente la sua attività
Colonna 4: Funzioni attribuite: descrive l'elenco dei servizi informatici assegnati alla persona, l'ambito di operatività per settori o per aree operativa. Vale a dire la *job description* dell'AdS.
Colonna 5: *Banca dati gestita e trattamenti consentiti:* indica le banche dati a cui l'AdS è autorizzato ad accedere e il tipo di operazioni consentite sui dati ivi contenuti. Vale adire il "profilo di autorizzazione" dell'AdS.
Colonna 6: Trattamento di informazioni dei lavoratori (AdS/L): la colonna "SI" indica quegli AdS la cui attività, in relazione ai diversi servizi informatici cui sono preposti, riguarda anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori (per brevità: "AdS/L"). Il dato viene fornito in adempimento a quanto prescritto dal Provvedimento del Garante che pone a carico dei Titolari del trattamento l'obbligo di rendere nota, nell'ambito della propria organizzazione, l'identità degli AdS/L al fine di richiamare l'attenzione sulla rilevanza e la criticità insite nello svolgimento della loro mansione.

Il Responsabile del trattamento, si impegna più specificamente 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 una 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 Lazio, 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

Privacy by design e by default

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (privacy by design e by default)

Nel trattare i dati per conto del Titolare, o nel fornire al Titolare soluzioni di trattamento, il Responsabile deve rispettare i principi di protezione dei dati fin dalla progettazione (privacy by design) e protezione dei dati per impostazione predefinita (privacy by default) di cui all'art. 25 GDPR comunicando al Titolare le soluzioni individuate e adottate per rispettare tali principi (cfr. Considerando 78 GDPR).

Al riguardo il Titolare fornisce al Responsabile del trattamento le seguenti 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;
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; 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;
7. 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;
8. le tecnologie di rafforzamento della protezione dei dati (PET, privacyenhancing 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;
9. 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;

10. 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.
11. 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.

SCHEMA H

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"

SCHEMA I

CLAUSOLE DISCIPLINARI DI GARA

“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 seguitoRGPD), 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 disposizioninormative 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 contrattotutte 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.

Inparticolare 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 I bis([9])

(art. 474-bis, c. 1)

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 RGDP 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-

[9] 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 allefinalità 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 attivitàconcretamente 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 divalutazione 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 egestione di un modello organizzativo.

2. La contitolarità è riferita al trattamento dei dati personali ed ha ad oggetto il trattamento di tutti i dati giàpresenti, 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 superiorea 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 verifichino 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 sè, 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, e quanto ne consegue, 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 idati 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 suoeventuale 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 lapredisposizione 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 quelliinerenti 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 dicui 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 legale <*inserire nome e cognome*>