



INVESTIMENTI PER L'OCCUPAZIONE E LA CRESCITA

Programma della Regione Lazio

Fondo Sociale Europeo Plus Programmazione 2021-2027

SCHEMA DI CONVENZIONE

TRA

REGIONE LAZIO - Direzione regionale Istruzione, Formazione e Politiche per l'Occupazione, Autorità di Gestione (di seguito AdG) del Programma Regionale Lazio FSE+ 2021-2027 "Investimenti per l'occupazione e la crescita", con sede in _____, rappresentata dal Direttore protempore, _____, domiciliato per la carica presso la stessa sede.

E

CITTA' METROPOLITANA DI ROMA CAPITALE - Dipartimento _____ - con sede in _____, in qualità e indenticata di seguito Organismo Intermedio (di seguito OI), come da Determinazione Dirigenziale n. G07490 del 30/05/2023, per la realizzazione di operazioni specifiche nell'ambito dei "Piani Annuali degli Interventi del Sistema Educativo Regionale" nell'ambito del Programma Regionale Lazio FSE+ 2021-2027, rappresentata da _____, in qualità di _____ domiciliato per la sua carica presso la stessa sede.

VISTI

- lo Statuto della Regione Lazio;
- lo Statuto vigente della Città Metropolitana di Roma Capitale e gli atti di organizzazione interna;
- la Legge Regionale 6 agosto 1999, n. 14 "Organizzazione delle funzioni a livello regionale e locale per la realizzazione del decentramento amministrativo" e successive modifiche ed integrazioni;
- la Legge Regionale del 18 febbraio 2002, n. 6 recante "Disciplina del sistema organizzativo della Giunta e del Consiglio e disposizioni relative alla dirigenza ed al personale regionale" e successive modifiche ed integrazioni;
- il Regolamento Regionale del 6 settembre 2002, n. 1 "Regolamento di organizzazione degli uffici e dei servizi della Giunta Regionale" e successive modifiche e integrazioni;
- il Regolamento Regionale 23 ottobre 2023, n. 9, concernente: "Modifiche al regolamento regionale 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della giunta regionale) e successive modifiche. Disposizioni transitorie", come modificato dal Regolamento Regionale 28 dicembre 2023, n. 12, concernente: "Modifiche al regolamento regionale 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della giunta regionale) e successive modifiche. Disposizioni transitorie";
- la Deliberazione di Giunta Regionale del 18 gennaio 2024, n. 25, con la quale è stato conferito l'incarico di Direttrice della Direzione Regionale Istruzione, Formazione e Politiche per l'Occupazione all'Avv. Elisabetta Longo;



- l'Atto di Organizzazione n. G01484 del 14 febbraio 2024 avente ad oggetto "Organizzazione della Direzione regionale Istruzione, Formazione e Politiche per l'Occupazione", così come modificato dagli Atti di Organizzazione n. G02244 del 29 febbraio 2024 e n. G02718 dell'11 marzo 2024, con il quale si è provveduto a riorganizzare le strutture organizzative di base della Direzione regionale Istruzione, Formazione e Politiche per l'Occupazione;
- la Direttiva del Direttore Generale prot. n. 573860 del 30 aprile 2024, recante le indicazioni per l'operatività della riorganizzazione dell'apparato amministrativo disposta dal Regolamento Regionale 23 ottobre 2023, n. 9, con decorrenza 1° maggio 2024;

VISTI inoltre

- il Regolamento n. 240/2014 della Commissione recante un Codice europeo di condotta sul partenariato nell'ambito dei fondi strutturali e d'investimento europeo;
- il Regolamento (UE) n. 651/2014 che dichiara alcune categorie di aiuti compatibili con il mercato interno in applicazione degli articoli 107 e 108 del trattato;
- il Regolamento (UE) n. 1407/2013 relativo all'applicazione degli articoli 107 e 108 del trattato sul funzionamento dell'Unione europea agli aiuti «de minimis»;
- il Regolamento (UE) n. 2016/679 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 (GDPR - Regolamento generale sulla protezione dei dati);
- il Regolamento (UE) n. 2093/2020 del Consiglio del 17 dicembre 2020 che stabilisce il Quadro Finanziario Pluriennale (QFP) per il periodo 2021-2027;
- il Regolamento (UE) n. 972/2020 che modifica il Regolamento (UE) n. 1407/2013 per quanto riguarda la sua proroga e il Regolamento (UE) n. 651/2014 per quanto riguarda la sua proroga e gli adeguamenti pertinenti;
- il Regolamento delegato (UE) n. 702/2021 recante modifica del Regolamento delegato (UE) n. 2195/2015 che integra il Regolamento (UE) n. 1304/2013 del Parlamento europeo e del Consiglio relativo al Fondo sociale europeo, per quanto riguarda la definizione di tabelle standard di costi unitari e di importi forfettari per il rimborso da parte della Commissione agli Stati membri delle spese sostenute;
- il Regolamento (UE) n. 2021/1060 del Parlamento Europeo e del Consiglio del 24 giugno 2021 recante le disposizioni comuni applicabili al Fondo europeo di sviluppo regionale, al Fondo sociale europeo Plus;
- il Regolamento (UE) n. 2021/1057 del Parlamento Europeo e del Consiglio del 24 giugno 2021 (Regolamento FSE+) che istituisce il Fondo sociale europeo Plus (FSE+) e che abroga il Regolamento (UE) n. 1296/2013;
- il Regolamento (UE) n. 2024/795 del Parlamento Europeo e del Consiglio del 29 febbraio 2024 che istituisce la piattaforma per le tecnologie strategiche per l'Europa (STEP) e modifica la direttiva 2003/87/CE e i Regolamenti (UE) n. 2021/1058, n. 2021/1056, n. 2021/1057, n. 1303/2013, n. 223/2014, n. 2021/1060, n. 2021/523, n. 2021/695, n. 2021/697 e n. 2021/241;
- la nota EGESIF_14-0021-00 del 16 giugno 2014 "Valutazione dei rischi di frode e misure antifrode efficaci e proporzionate" e s.m.i;
- la nota EGESIF_14-0017 "Guida alle opzioni semplificate in materia di costi (OSC): Finanziamento a tasso forfettario, Tabelle standard di costi unitari, importi forfettari";
- la Legge n. 241 del 1990 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" e s.m.i.;
- il Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e s.m.i.;
- il Decreto legislativo 18 aprile 2016, n. 50 "Codice dei contratti pubblici" e s.m.i.;
- il Decreto legislativo 31 marzo 2023, n. 36 "Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici";
- la Direttiva n. 2014/24/UE del Parlamento Europeo e del Consiglio del 26 febbraio 2014 sugli appalti pubblici



e che abroga la direttiva 2004/18/CE;

- la Decisione di esecuzione della Commissione C (2022) 4787 final del 15 luglio 2022 che approva l'Accordo di Partenariato con la Repubblica italiana (CCI 2021IT16FFPA001);
- la Decisione di esecuzione della Commissione Europea C (2022) 5345 final del 19 luglio 2022 che approva il programma "PR Lazio FSE+ 2021-2027" per il sostegno a titolo del Fondo sociale europeo Plus nell'ambito dell'obiettivo "Investimenti a favore dell'occupazione e della crescita" per la regione Lazio in Italia (CCI 2021IT05SFPR006);
- la Deliberazione di Giunta Regionale n. 835 del 6 ottobre 2022, avente ad oggetto "Presenza d'atto della Decisione C (2022) 5345 del 19 luglio 2022 della Commissione Europea che approva il Programma PR Lazio FSE+ 2021-2027" - CCI 2021IT05SFPR006 - nell'ambito dell'obiettivo "Investimenti a favore dell'occupazione e della crescita";
- la Deliberazione di Giunta Regionale n. 682 del 1 ottobre 2019 "Revoca della D.G.R. 29 novembre 2007, n. 968 e s.m.i. Approvazione nuova Direttiva concernente l'accreditamento dei soggetti che erogano attività di formazione e di orientamento nella Regione Lazio";
- la Metodologia e criteri di selezione delle operazioni finanziate dal FSE+ approvati nella riunione del Comitato di Sorveglianza congiunto del PR Lazio FSE+ 2021-2027 e del POR FSE Lazio 2014-2020 del 15 dicembre 2022;
- la Determinazione Dirigenziale n. G04128 del 28 marzo 2023, avente ad oggetto l'approvazione della "Direttiva Regionale per l'attuazione e la rendicontazione delle attività cofinanziate con il Fondo Sociale Europeo, Fondo Sociale Europeo+ e altri Fondi. Programmazione 2014-2020 (FSE) e Programmazione 2021-2027 (FSE+). Sistema delle regole per accompagnare la chiusura del POR 2014-2020 e l'attuazione del PR 2021-2027";
- la Determinazione Dirigenziale n. G07490 del 30 maggio 2023 avente ad oggetto "Individuazione dell'Organismo Intermedio Città Metropolitana di Roma Capitale, per la gestione delle attività delegate nell'ambito del PR FSE+ 2021-2027 della Regione Lazio, ai sensi dell'art. 71, paragrafo 3, del Regolamento (UE) n. 2021/1060 del Parlamento Europeo e del Consiglio del 24 giugno 2021";
- la Deliberazione di Giunta Regionale n. 317 del 20 giugno 2023 concernente "Approvazione del documento "Sistema di Gestione e Controllo – Descrizione delle funzioni e delle procedure in atto per l'Autorità di Gestione e l'Organismo che svolge la Funzione contabile" - Programma Lazio FSE Plus (FSE+) 2021-2027, Ob. "Investimenti a favore dell'occupazione e della crescita";
- la Determinazione Dirigenziale n. G17381 del 18 dicembre 2024, avente ad oggetto "Aggiornamento del documento "Sistema di Gestione e Controllo - Descrizione delle funzioni e delle procedure in atto per l'Autorità di Gestione e l'Organismo che svolge la Funzione contabile" - Programma Lazio FSE Plus (FSE+) 2021-2027, Ob. "Investimenti a favore dell'occupazione e della crescita" - approvato con Deliberazione di Giunta Regionale n. 317 del 20/06/2023";
- la Determinazione Dirigenziale n. G17404 18 dicembre 2024 avente ad oggetto "Aggiornamento del documento "Manuale delle procedure dell'AdG/OOII per la gestione ed il controllo degli interventi finanziati Programma Fondo Sociale Europeo Plus (FSE+) 2021-2027" - Programma Lazio FSE Plus (FSE+) 2021-2027, Ob. "Investimenti a favore dell'occupazione e della crescita" - approvato con Determinazione Dirigenziale n. G11407 del 28/08/2023 e successivamente modificato con Determinazione Dirigenziale n. G17189 del 20 dicembre 2023 - e dei relativi allegati";
- i provvedimenti regionali in materia di programmazione e finanziamento dell'offerta formativa di Istruzione e Formazione Professionale (IeFP), adottati annualmente con Deliberazione di Giunta Regionale, ai sensi dell'articolo 8 e dell'articolo 11, comma 2, della Legge regionale 20 aprile 2015 n. 5, in base ai quali la Regione deve emanare il "Piano annuale degli interventi del sistema educativo regionale" che disciplina gli aspetti programmatici, organizzativi e gestionali dei percorsi triennali di Istruzione e Formazione Professionale (IeFP) realizzati dal sistema della Formazione Professionale (a gestione diretta e in regime convenzionale), individuando anche le risorse disponibili e i criteri di ripartizione delle stesse;

TUTTO CIÒ PREMESSO SI CONVIENE QUANTO SEGUE

Art. 1

Oggetto della Convenzione

1. Con la presente Convenzione vengono disciplinati i rapporti giuridici tra la Regione Lazio - Direzione regionale Istruzione, Formazione e Politiche per l'Occupazione, Autorità di Gestione del Programma Regionale Lazio FSE+ 2021-2027, e la Città Metropolitana di Roma Capitale, in qualità di Organismo Intermedio per la realizzazione nell'ambito del PR Lazio FSE+ 2021-2027 di operazioni specifiche nell'ambito dei "Piani Annuali degli Interventi del Sistema Educativo Regionale", approvati, per ogni anno scolastico e formativo, con Deliberazione di Giunta Regionale, che stabiliscono, tra l'altro, i principali aspetti programmatici, organizzativi e gestionali dei percorsi di leFp realizzati dal sistema della Formazione Professionale e forniscono le indicazioni metodologiche e procedurali per l'operatività degli stessi.
2. La Città Metropolitana di Roma Capitale, nell'ambito della realizzazione dei percorsi integrativi di leFp a valere sul PR Lazio FSE+ 2021-2027, opera in qualità di OI, conformemente a quanto previsto nei suddetti "Piani Annuali degli Interventi del Sistema Educativo Regionale", in virtù delle funzioni ad essa attribuite dalla Legge Regionale del 31 dicembre 2015, n. 17 e con specifico riferimento alle funzioni di selezione e gestione delle operazioni come specificato al successivo articolo 5.

Art. 2

Risorse finanziarie

1. Allo scopo di attuare gli interventi previsti, le risorse attribuite all'OI sono stabilite annualmente con Deliberazione di Giunta Regionale che approva il "Piano Annuale degli Interventi del Sistema Educativo Regionale" e stabilisce l'assegnazione delle risorse alla Città Metropolitana di Roma Capitale, le modalità di trasferimento delle stesse e le fonti di finanziamento, con indicazione delle risorse FSE che concorrono al finanziamento dei percorsi integrativi di leFp. In particolare, per l'attuazione delle attività oggetto della presente Convenzione, il trasferimento delle risorse finanziarie all'OI Città Metropolitana di Roma Capitale, avviene con Determinazione Dirigenziale della Direzione regionale Istruzione, Formazione e Politiche per l'Occupazione - AdG del PR Lazio FSE+ 2021-2027, in forma di acconto, di pagamento intermedio e saldo.
2. L'OI Città Metropolitana di Roma Capitale si impegna ad effettuare la restituzione all'AdG delle somme non utilizzate e/o non riconosciute secondo modalità e termini stabiliti da quest'ultima.

Art. 3

Compiti dell'OI

La Città Metropolitana di Roma Capitale viene individuata con il ruolo di Organismo Intermedio del PR ai sensi dell'art 71, paragrafo 3, del Regolamento (UE) n. 2021/1060.

L'OI inoltre:

- a) partecipa ai momenti di coordinamento, in particolare alle riunioni del Comitato di Sorveglianza del PR;
- b) fornisce i dati di monitoraggio relativi ai progressi degli interventi finanziati a valere sul PR nel raggiungimento degli obiettivi e dei target fisici e finanziari, nel rispetto delle scadenze stabilite dall'AdG, utilizzando il sistema informativo di monitoraggio regionale del PR FSE+ 2021-2027;
- c) fornisce e rende disponibili ai soggetti preposti allo svolgimento delle attività di valutazione del PR tutte le informazioni necessarie per verificarne l'efficacia, l'efficienza e l'impatto, previste dal Piano di valutazione;
- d) contribuisce all'elaborazione della relazione finale in materia di performance di cui all'articolo 43 del Regolamento (UE) n. 2021/1060;

- e) osserva nell'ambito del proprio ruolo e degli interventi in essere i dispositivi in materia d'informazione e pubblicità previsti dall'art. 50 del Regolamento (UE) n. 2021/1060;
- f) si adegua, nella progettazione e realizzazione delle azioni di comunicazione, a quanto previsto dalla Linee di indirizzo per la comunicazione unitaria dei Fondi europei 2021-2027;
- g) collabora all'assolvimento di ogni altro onere ed adempimento previsto a carico dell'AdG e dalla normativa comunitaria in vigore, per tutta la durata della presente Convenzione.

Art. 4

Sistema di gestione e controllo

Per quanto concerne l'adozione del Sistema di gestione e controllo, l'OI:

- a) adotta un sistema di gestione e controllo adeguato, nel rispetto delle procedure adottate dall'AdG, dei principi stabiliti dall'articolo 69 e dell'allegato XI e XVI del Regolamento (UE) n. 2021/1060 che prevedono i requisiti fondamentali dei sistemi di gestione e controllo e il modello per la descrizione del sistema di gestione e controllo corredato delle procedure interne (manuali) e dalle piste di controllo;
- b) adotta modalità di semplificazione dei costi, in base a quanto disposto dagli articoli 53, 54 e 55 del Regolamento (UE) n. 2021/1060, in accordo con procedure e modalità definite dall'AdG all'interno della manualistica del PR;
- c) informa l'AdG in merito ad eventuali aggiornamenti del Sistema di gestione e controllo adottato, intervenuti a seguito di cambiamenti del contesto organizzativo e normativo-procedurale;
- d) dovrà far riferimento al Si.Ge.Co. ed alla manualistica vigenti;
- e) garantisce che i beneficiari coinvolti nell'attuazione di operazioni rimborsate sulla base dei costi ammissibili effettivamente sostenuti mantengano un sistema di contabilità separata o una codificazione contabile adeguata per tutte le transazioni relative a un'operazione;
- f) collabora, su richiesta dell'AdG, per la presentazione della documentazione necessaria alla chiusura annuale dei conti, nel rispetto della tempistica stabilita dall'articolo 98, del Reg (UE) n. 2021/1060;
- g) collabora con l'AdG all'applicazione delle procedure stabilite dall'AdG in caso di irregolarità e frodi e predisporre tutti gli atti per il recupero di importi indebitamente versati;
- h) partecipa al gruppo per l'autovalutazione del rischio di frode per il PR FSE+ 2021-2027.

Art. 5

Funzioni delegate: Selezione e gestione delle operazioni

Le funzioni delegate all'OI attengono alla selezione e alla gestione delle operazioni. In particolare, l'OI:

- a) applica le metodologie e i criteri di selezione approvati dal Comitato di Sorveglianza;
- b) trasmette all'AdG, prima della loro adozione, gli atti concernenti le procedure di affidamento (bandi, avvisi, etc.), ai fini dello svolgimento dei compiti di coordinamento e supervisione dell'attuazione del PR ad essa affidati;
- c) fornisce ai beneficiari, prima dell'approvazione delle operazioni, un documento contenente le condizioni per il sostegno relative a ciascuna operazione, compresi i requisiti specifici concernenti i prodotti o servizi da fornire nell'ambito dell'operazione, il piano finanziario e il termine per l'esecuzione;
- d) si accerta che i beneficiari abbiano la capacità amministrativa, finanziaria e operativa prima dell'approvazione dell'operazione;



- e) garantisce il rispetto di tutti i vincoli stabiliti dal Regolamento (UE) n. 2021/1060 e dal Regolamento (UE) n. 2021/1057 e, in particolare per quanto riguarda l'ammissibilità della spesa (artt. 63 e 64 del Regolamento UE n. 2021/1060);
- f) adotta procedure di conservazione di tutti i documenti relativi alle spese e ai controlli necessari a garantire una pista di controllo adeguata secondo quanto disposto dall'articolo 69, paragrafo 6, e dall'Allegato XIII Elementi per la pista di controllo del Reg. (UE) n. 2021/1060;
- g) stabilisce procedure idonee ad assicurare che tutti i documenti relativi alle spese e agli audit necessari per garantire una pista di controllo adeguata siano conservati anche dai beneficiari e dai soggetti attuatori, sotto forma di originali o di copie autenticate, secondo quanto disposto dall'art. 82 del Reg. (UE) n. 2021/1060, per un periodo di cinque anni a decorrere dal 31 dicembre dell'anno in cui è effettuato l'ultimo pagamento al beneficiario;
- h) acquisisce e comunica alla Regione il CUP (Codice Unico di Progetto) entro 30 giorni dall'approvazione del finanziamento, come stabilito nei "Piani Annuali degli Interventi del Sistema Educativo Regionale", approvati per ogni anno scolastico e formativo, con Deliberazione di Giunta Regionale;
- i) emette gli atti di impegno contabile e di erogazione dell'anticipazione e del saldo nei confronti dei soggetti attuatori responsabili della realizzazione delle attività corsuali, nel rispetto del termine di 80 giorni per i pagamenti ai beneficiari a norma dell'articolo 74 del Regolamento (UE) n. 2021/1060;
- j) garantisce, anche da parte dei beneficiari il rispetto degli obblighi in materia di informazione e pubblicità previsti all'articolo 50 del Regolamento (UE) n. 2021/1060;
- k) fornisce la necessaria collaborazione all'Autorità di Audit per lo svolgimento dei compiti a questa assegnati dai regolamenti UE, in particolare la verifica dei sistemi di gestione e controllo, l'esecuzione dei controlli di II livello sulle operazioni necessarie per la predisposizione del parere annuale e la relazione annuale di controllo;
- l) assicura tutte le azioni di follow-up sui controlli effettuati da parte dell'AdG, dell'OFC, dell'AdA, della CE o degli altri soggetti abilitati;
- m) alimenta, per quanto di competenza, del sistema informativo SIGEM, con tutte le necessarie informazioni, assumendone la responsabilità in merito alla loro correttezza e veridicità.
- n) assicura, anche presso i beneficiari, l'utilizzo del sistema di registrazione e conservazione informatizzata dei dati SIGEM, istituito dall'Autorità di Gestione, necessario alla sorveglianza, alla valutazione, alla gestione finanziaria, ai controlli di primo livello, al monitoraggio, e agli audit, garantendo un costante e immediato aggiornamento dei dati;

Art. 6

Previsioni di spesa

L'OI si impegna ad elaborare le previsioni di spesa e ad inoltrarle all'AdG, secondo modalità e tempi definiti da quest'ultima, affinché siano rispettate le scadenze del 31 gennaio e 31 luglio di ogni anno come previsto dall'art. 69, paragrafo 10, del Regolamento (UE) n. 2021/1060, e a rispettarle al fine di garantire il perseguimento degli obiettivi prefissati ed evitare il disimpegno automatico delle risorse, consapevole che il mancato rispetto potrà comportare la decurtazione delle risorse assegnate, di cui all'art. 2 della presente Convenzione.

Art. 7

Impegni dell'AdG

1. Conformemente all'articolo 71, paragrafo 3, del Regolamento (UE) n. 2021/1060, l'AdG designa l'OI sotto la propria responsabilità. A tal fine, fornisce indicazioni strategiche ed operative alle quali l'OI deve conformarsi.
2. L'AdG, in qualità di delegante, si impegna nei confronti dell'OI, a:



- a) rendere disponibili le risorse finanziarie di cui all'articolo 2;
 - b) fornire le informazioni pertinenti per l'esecuzione dei compiti dell'OI;
 - c) garantire la disponibilità di un sistema informatizzato per la raccolta e lo scambio elettronico dei dati, relativi a ciascuna operazione, necessari per la sorveglianza, la valutazione, la gestione finanziaria, la verifica e l'audit;
 - d) fornire le informazioni riguardanti il Sistema di Gestione e Controllo attraverso il documento descrittivo dell'organizzazione e delle procedure adottate dall'AdG stessa in coerenza con il modello di cui all'Allegato XVI del Regolamento (UE) n. 2021/1060;
 - e) eseguire ai sensi dell'articolo 74, paragrafo 1, del Regolamento (UE) n. 2021/1060, i controlli di primo livello documentali e in loco, al fine di verificare che i prodotti e i servizi cofinanziati siano stati forniti, che i beneficiari abbiano pagato le spese dichiarate e che queste ultime siano conformi al diritto applicabile, al programma operativo e alle condizioni per il sostegno dell'operazione;
 - f) per i controlli in loco, garantire l'applicazione di un'adeguata metodologia di campionamento, che tenga conto dell'analisi dei rischi sulla base del valore dei progetti finanziati, del livello di rischio individuato per la tipologia di operazione e di beneficiario, dei risultati delle verifiche effettuate dai diversi soggetti abilitati e di ogni ulteriore elemento significativo;
 - g) trasmettere all'OI gli esiti provvisori del Controllo di I livello per l'attivazione del successivo contraddittorio;
 - h) esaminare eventuali controdeduzioni presentate dal beneficiario ed emanare i provvedimenti relativi al definitivo riconoscimento delle spese sostenute;
 - i) trasmettere all'OI gli esiti definitivi del controllo per l'attivazione da parte dello stesso delle procedure di erogazione degli importi dovuti ai soggetti attuatori responsabili delle attività corsuali;
 - j) alimentare, per quanto di competenza, del sistema informativo SIGEM, con tutte le necessarie informazioni, assumendone la responsabilità in merito alla loro correttezza e veridicità.
 - k) esaminare le risultanze dei controlli effettuati dall'Autorità di Audit e predisposizione di tutte le informazioni e la documentazione necessarie per il successivo contraddittorio;
 - l) informare l'OI in merito alle irregolarità riscontrate nel corso dell'attuazione del PR che possano avere ripercussioni sugli ambiti gestiti all'OI;
 - m) istituire misure anti frode efficaci e proporzionate tenendo conto dei rischi individuati;
 - n) assolvere ad ogni altro onere ed adempimento, previsto a carico della AdG dalla normativa comunitaria in vigore, per tutta la durata della presente Convenzione.
3. L'AdG effettua controlli periodici presso l'OI per verificare la corretta attuazione degli interventi nel rispetto delle procedure previste.

Art. 8

Tutela della Privacy

1. Tutti i dati forniti per la redazione del presente atto saranno trattati dalla Regione nel rispetto del Reg. UE n. 679/2016.
2. I dati forniti (o caricati) in SIGEM, nell'ambito del finanziamento saranno inseriti nel sistema ARACHNE, uno strumento informatico integrato sviluppato dalla Commissione Europea per l'individuazione degli indicatori di rischio di frode. I dati contenuti nel sistema ARACHNE, finalizzati al calcolo del rischio, saranno soggetti ai vincoli di protezione dei dati e non saranno pubblicati né dall'Autorità di Gestione né dai Servizi della Commissione Europea.
3. A tal riguardo, si rimanda all'Informativa sul trattamento dei dati personali di cui all'Allegato A.



Art. 9

Modifiche e durata della Convenzione

1. La presente Convenzione ha efficacia, salvo ipotesi di revoca totale o parziale per giustificati motivi, fino ad esaurimento di tutti gli effetti giuridici ed economici relativi alla programmazione dei fondi 2021-2027.
2. Eventuali modifiche e/o integrazioni alla presente Convenzione sono apportate con atto scritto a firma dell'AdG e dell'OI.

Art. 10

Clausola di chiusura

1. Per tutto quanto non disciplinato dalla presente Convenzione, si farà riferimento a quanto disposto dalla normativa comunitaria, nazionale e regionale vigente.

Letto, confermato e sottoscritto per accettazione,

Regione Lazio	Città Metropolitana di Roma Capitale
Direzione regionale Istruzione, Formazione e Politiche per l'Occupazione	Dipartimento _____ Servizio _____
Autorità di Gestione PR Lazio FSE+ 2021-2027 Il Direttore _____	Organismo intermedio PR Lazio FSE+ 2021-2027 Il/La Dirigente _____

La presente Convenzione viene firmata digitalmente, ai sensi e per gli effetti del D.P.R. 28 dicembre 2000, n. 445 e del D.lgs. 7 marzo 2005, n. 82 e norme collegate, con sostituzione del testo cartaceo e della firma autografa.



ALLEGATO A: INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

ai sensi dell'art. 13 del Regolamento (UE) 2016/679

TITOLO

Programma Regionale Lazio FSE+ 2021-2027, Convenzione tra Regione Lazio - Direzione regionale Istruzione, Formazione e Politiche per l'Occupazione (AdG) e la Città Metropolitana di Roma Capitale, in qualità di Organismo Intermedio (OI) per la realizzazione di operazioni specifiche dei "Piani Annuali degli Interventi del Sistema Educativo Regionale", approvati, per ogni anno scolastico e formativo, con Deliberazione di Giunta Regionale.

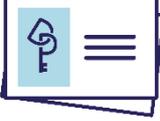
Gentile cittadino/a,

nel rispetto del principio di trasparenza previsto dal Regolamento europeo 2016/679 in materia di protezione dei dati personali ("RGPD", anche cd. "GDPR"), con questa informativa la Giunta Regionale del Lazio (in seguito anche il "Titolare" del trattamento) Le fornisce notizie sulle modalità con le quali vengono trattati informazioni e dati che riguardano la sua persona (di seguito anche "interessato").

Si descrivono pertanto le modalità e le finalità di trattamento dei dati personali relativi alla realizzazione delle operazioni previste nell'ambito del Programma Regionale Lazio FSE+ 2021-2027, con particolare riferimento ai "Piani Annuali degli Interventi del Sistema Educativo Regionale." Il trattamento dei dati personali avviene in conformità ai principi di correttezza, liceità, trasparenza, riservatezza e minimizzazione, come previsto dal Regolamento (UE) 2016/679 (di seguito RGPD) e dal Decreto legislativo 30 giugno 2003, n. 196 e s.m.i. (Codice in materia di protezione dei dati personali). L'obiettivo del trattamento è garantire la protezione dei diritti e delle libertà fondamentali degli interessati, assicurando il diritto alla protezione dei dati personali. Le attività di trattamento comprendono: (i) Gestione amministrativa e operativa: raccolta, elaborazione, conservazione e trasmissione dei dati personali necessari per l'attuazione dei percorsi di Istruzione e Formazione Professionale (IeFP), inclusa l'assegnazione dei contributi e la verifica dell'ammissibilità delle operazioni; (ii) Monitoraggio e rendicontazione: utilizzo di strumenti informatici, come il sistema SIGEM, per monitorare lo stato di avanzamento delle operazioni, garantire la tracciabilità dei flussi finanziari e redigere la documentazione di rendicontazione richiesta; (iii) Verifiche di controllo e valutazione: i dati saranno trattati per consentire lo svolgimento di attività di controllo amministrativo e contabile da parte delle Autorità competenti, in particolare per accertare la correttezza e la conformità delle operazioni finanziate; (iv) Comunicazione e trasparenza: i dati personali saranno trattati per adempiere agli obblighi di comunicazione e pubblicità degli interventi cofinanziati, come previsto dal Regolamento (UE) 2021/1060, e per assicurare la trasparenza nell'utilizzo delle risorse; (v) Inserimento nel sistema ARACHNE: i dati, caricati nel sistema SIGEM, potranno essere inseriti nel sistema ARACHNE, un tool della Commissione Europea per la rilevazione degli indicatori di rischio di frode, garantendo la protezione dei dati personali e il rispetto delle disposizioni normative; (vi) Supporto e assistenza agli interessati: i dati saranno trattati per fornire supporto agli utenti e rispondere a richieste di chiarimenti, assistenza tecnica e gestione delle comunicazioni relative agli interventi.

La Regione Lazio è impegnata a proteggere e a salvaguardare qualsiasi dato personale; agisce nell'interesse delle persone e tratta i loro dati con correttezza e trasparenza, per fini leciti e tutelando la loro riservatezza ed i loro diritti.

Per queste ragioni Le fornisce i recapiti necessari per contattare il Titolare o il DPO in caso di domande sui suoi dati personali.

	<p style="text-align: center;">TITOLARE DEL TRATTAMENTO E DATI DI CONTATTO</p> <p>il Titolare del trattamento è la Regione Lazio, con sede in Via Rosa Raimondi Garibaldi 7, 00145 Roma, contattabile come di seguito:</p> <ul style="list-style-type: none"> - telefono URP-Ufficio Relazioni con il Pubblico: 06/99500 - modulo di contatto disponibile alla seguente url: https://scriviurpnur.regione.lazio.it/ - e-mail: urp@regione.lazio.it - PEC: urp@pec.regione.lazio.it <p>Designato allo svolgimento di specifici compiti e funzioni connessi trattamento di dati personali, individuati dall'art. 474 ter del Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale R.R. 1/2002 s.m.i, è il Direttore pro tempore della Direzione Regionale Istruzione, Formazione e Politiche per l'Occupazione, con sede in Via R. Raimondi Garibaldi 7, 00145 Roma (e-mail: elongo@regione.lazio.it; PEC: formazione@pec.regione.lazio.it; Telefono 06/51684949).</p>
	<p style="text-align: center;">RESPONSABILE DELLA PROTEZIONE DEI DATI ("DPO")</p> <p>La Regione Lazio ha incaricato un Responsabile della Protezione dei Dati (RPD), più comunemente conosciuto con l'acronimo inglese "DPO" (Data Protection Officer), che è contattabile alla e-mail istituzionale: dpo@regione.lazio.it.</p>
	<p>Dati anagrafici o di contatto del rappresentante legale/soggetto delegato munito dei poteri di firma del Soggetto Proponente: (es. cognome, nome, indirizzo, numero di telefono, codice fiscale, e-mail, altri dati contenuti nel suo documento di identità etc.) – v. art. 6, par. 1, n. 1 GDPR;</p> <p>Dati anagrafici o di contatto del rappresentante legale del mandatario/capofila dell'ATI/ATS: (es. cognome, nome, indirizzo, numero di telefono, codice fiscale, e-mail, altri dati contenuti nel suo documento di identità etc.) – v. art. 4, par. 1, n. 1 GDPR;</p> <p>Dati anagrafici o di contatto del rappresentante legale del/dei mandante/i dell'ATI/ATS: (es. cognome, nome, indirizzo, numero di telefono, codice fiscale, e-mail, altri dati contenuti nel suo documento di identità etc.) – v. art. 4, par. 1, n. 1 GDPR;</p> <p>Dati personali e Curriculum Vitae dei docenti conformemente a quanto previsto dalla DGR 682/2019 "Approvazione nuova Direttiva concernente l'accreditamento dei soggetti che erogano attività di formazione e di orientamento nella Regione Lazio" (es. cognome, nome, indirizzo, numero di telefono, codice fiscale, e-mail, titolo di studio, altri dati contenuti nel suo documento di identità etc.) - v. art. 6, par. 1, n. 1 GDPR;</p> <p>Dati anagrafici o di contatto del Referente del progetto: (es. cognome, nome, indirizzo, numero di telefono, codice fiscale, e-mail, altri dati contenuti nel suo documento di identità etc.) – v. art. 6, par. 1, n. 1 GDPR;</p>

	<p>Dati personali dei destinatari: allievi dei percorsi formativi leFP;</p> <p>Dati finanziari: (es. pagamenti, coordinate bancarie, numero conto corrente, IBAN, etc.);</p> <p>Ai sensi dell'art. 9 del Regolamento (UE) 2016/679, si darà informazione ai destinatari di essere tenuti a conferire dati qualificabili come "categorie particolari di dati personali" e cioè quei dati che rivelano "l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, 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". Tali categorie di dati potranno essere trattate solo previo libero ed esplicito consenso dei destinatari, manifestato in calce all' informativa che sarà loro fornita dai soggetti attuatori.</p>						
	<p style="text-align: center;">LIBERTA' O OBBLIGO DI FORNIRE I DATI E CONSEGUENZE</p> <p>Il conferimento dei dati personali sopra indicati è necessario per la partecipazione e la gestione delle attività previste nell'ambito del Programma Regionale Lazio FSE+ 2021-2027, inclusa la verifica di conformità e la rendicontazione delle operazioni finanziate. Tali operazioni comprendono, a titolo esemplificativo ma non esaustivo: (i) l'esame delle domande di partecipazione e la verifica dei requisiti di ammissibilità; (ii) l'assegnazione delle risorse finanziarie ai soggetti aventi diritto; (iii) l'attuazione, il monitoraggio e la verifica delle attività formative e amministrative previste; (iv) la rendicontazione delle spese in conformità alla normativa applicabile.</p> <p>La mancata indicazione dei dati personali necessari potrebbe pertanto precludere la partecipazione al Programma, l'accesso ai benefici previsti, nonché l'espletamento dei procedimenti amministrativi correlati.</p>						
	<p style="text-align: center;">FINALITÀ E BASE GIURIDICA DEL TRATTAMENTO</p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 50%;">FINALITÀ</th> <th style="width: 50%;">BASE GIURIDICA</th> </tr> </thead> <tbody> <tr> <td data-bbox="427 1301 943 1805"> <p>1. Gestione delle attività progettuali: il trattamento dei dati personali è necessario per la gestione delle attività progettuali, tra cui la valutazione delle proposte, la rendicontazione e il monitoraggio degli interventi finanziati nell'ambito del Programma Regionale Lazio FSE+ 2021-2027.</p> </td> <td data-bbox="943 1301 1430 1805"> <p>Art. 6, par. 1, lett. e) GDPR: il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; Regolamento (UE) 2021/1060, artt. 68 e 74: obbligo di gestione delle operazioni finanziate nell'ambito dei fondi europei; Decreto Legislativo n. 118/2011: principi per l'armonizzazione contabile degli enti pubblici.</p> </td> </tr> <tr> <td data-bbox="427 1805 943 2022"> <p>2. Adempimenti normativi e obblighi di legge: I dati personali sono trattati per adempiere a obblighi previsti dalla normativa comunitaria, nazionale e</p> </td> <td data-bbox="943 1805 1430 2022"> <p>Art. 6, par. 1, lett. c) GDPR: il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; Decreto Legislativo n. 33/2013, artt. 26 e 27: obblighi di trasparenza nella</p> </td> </tr> </tbody> </table>	FINALITÀ	BASE GIURIDICA	<p>1. Gestione delle attività progettuali: il trattamento dei dati personali è necessario per la gestione delle attività progettuali, tra cui la valutazione delle proposte, la rendicontazione e il monitoraggio degli interventi finanziati nell'ambito del Programma Regionale Lazio FSE+ 2021-2027.</p>	<p>Art. 6, par. 1, lett. e) GDPR: il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; Regolamento (UE) 2021/1060, artt. 68 e 74: obbligo di gestione delle operazioni finanziate nell'ambito dei fondi europei; Decreto Legislativo n. 118/2011: principi per l'armonizzazione contabile degli enti pubblici.</p>	<p>2. Adempimenti normativi e obblighi di legge: I dati personali sono trattati per adempiere a obblighi previsti dalla normativa comunitaria, nazionale e</p>	<p>Art. 6, par. 1, lett. c) GDPR: il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; Decreto Legislativo n. 33/2013, artt. 26 e 27: obblighi di trasparenza nella</p>
FINALITÀ	BASE GIURIDICA						
<p>1. Gestione delle attività progettuali: il trattamento dei dati personali è necessario per la gestione delle attività progettuali, tra cui la valutazione delle proposte, la rendicontazione e il monitoraggio degli interventi finanziati nell'ambito del Programma Regionale Lazio FSE+ 2021-2027.</p>	<p>Art. 6, par. 1, lett. e) GDPR: il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; Regolamento (UE) 2021/1060, artt. 68 e 74: obbligo di gestione delle operazioni finanziate nell'ambito dei fondi europei; Decreto Legislativo n. 118/2011: principi per l'armonizzazione contabile degli enti pubblici.</p>						
<p>2. Adempimenti normativi e obblighi di legge: I dati personali sono trattati per adempiere a obblighi previsti dalla normativa comunitaria, nazionale e</p>	<p>Art. 6, par. 1, lett. c) GDPR: il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; Decreto Legislativo n. 33/2013, artt. 26 e 27: obblighi di trasparenza nella</p>						

	<p>regionale, con particolare riferimento ai regolamenti sui fondi europei e alle disposizioni in materia di trasparenza amministrativa e tracciabilità dei flussi finanziari.</p>	<p>gestione di risorse pubbliche; Decreto Legislativo n. 50/2016, art. 3: tracciabilità dei flussi finanziari per contratti pubblici; Regolamento (UE) 2021/1057: disposizioni per il Fondo sociale europeo Plus.</p>
	<p>3. Monitoraggio, controllo e verifica: il trattamento è finalizzato al monitoraggio, controllo e verifica delle operazioni finanziate, nonché alla valutazione dei risultati ottenuti in relazione agli obiettivi previsti dal Programma.</p>	<p>Art. 6, par. 1, lett. e) GDPR: il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; Regolamento (UE) 2021/1060, art. 77: obblighi di controllo e monitoraggio dei fondi SIE; Regolamento (UE) 2021/1058, art. 9: Disposizioni specifiche per la valutazione dei risultati del FSE+.</p>
	<p>4. Prevenzione di frodi e irregolarità: il trattamento necessario per prevenire frodi, irregolarità o utilizzi impropri delle risorse pubbliche, in conformità alle disposizioni normative e alle linee guida comunitarie.</p>	<p>Art. 6, par. 1, lett. e) GDPR: il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; Regolamento (UE) 2021/1060, art. 69: disposizioni per la prevenzione di irregolarità e frodi; Nota EGESIF_14-0021-00: valutazione dei rischi di frode e misure antifrode proporzionate; Codice della Privacy, art. 2-sexies: trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante.</p>
	<p>5. Comunicazioni istituzionali: i dati personali possono essere utilizzati per la gestione delle comunicazioni tra l'Amministrazione e i beneficiari, nonché per la diffusione di informazioni sugli interventi cofinanziati, nel rispetto delle norme di informazione e pubblicità previste dal Regolamento (UE) 2021/1060.</p>	<p>Art. 6, par. 1, lett. e) GDPR: il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; Regolamento (UE) 2021/1060, art. 50: obblighi di informazione e comunicazione sugli interventi cofinanziati; Decreto Legislativo n. 33/2013, art.</p>

		12: trasparenza nelle comunicazioni pubbliche.
	<p style="text-align: center;">PERIODO DI CONSERVAZIONE</p> <p>Salva la necessità di conservazione ulteriore in caso di contenzioso legale ed esigenze difensive, i dati trattati sono conservati:</p> <ul style="list-style-type: none"> - Per la finalità di cui al n. 1 (Gestione delle attività progettuali): per un periodo pari a 10 anni dalla conclusione delle attività progettuali, in conformità agli obblighi di conservazione amministrativa; - Per la finalità di cui al n. 2 (Adempimenti normativi e obblighi di legge): per un periodo pari a 10 anni dall'ultimo pagamento, come previsto dalla normativa contabile e fiscale vigente; - Per la finalità di cui al n. 3 (Monitoraggio, controllo e verifica): per un periodo di 5 anni; - Per la finalità di cui al n. 4 (Prevenzione di frodi e irregolarità): per un periodo pari a 10 anni, salvo termini più lunghi previsti da eventuali procedimenti giudiziari o amministrativi pendenti; - Per la finalità di cui al n. 5 (Comunicazioni istituzionali): per un periodo pari a 5 anni dalla conclusione del Programma o fino al termine previsto dalla normativa in materia di comunicazione e trasparenza. <p>In ogni caso, in ossequio al principio di limitazione della conservazione (art. 5.1, lett. e) del RGPD), i suoi dati saranno conservati per un periodo non superiore a quello necessario per il perseguimento delle finalità sopra menzionate. Verrà verificata costantemente l'adeguatezza, la pertinenza e l'indispensabilità dei dati rispetto al rapporto, alla prestazione, all'incarico o al servizio in corso, da instaurare o cessati, anche con riferimento ai dati che Lei fornisce di propria iniziativa. Pertanto, anche a seguito di verifiche, le informazioni e i dati che risultano eccedenti o non pertinenti o non indispensabili non saranno utilizzati, salvo che per l'eventuale conservazione a norma di legge del documento che li contiene.</p>	
	<p style="text-align: center;">DESTINATARI</p> <p>Il trattamento dei Suoi dati personali avverrà a cura delle persone preposte al relativo procedimento, in maniera manuale/cartacea, con procedure anche informatizzate e con l'intervento umano, nei modi e nei limiti necessari per perseguire le predette finalità. L'elenco dei destinatari, riportato nel registro delle attività di trattamento, è mantenuto aggiornato e disponibile in caso di accertamenti anche da parte del Garante per la Privacy.</p> <p>I soggetti che possono essere destinatari dei sui dati personali sono:</p> <ul style="list-style-type: none"> - Responsabili del trattamento: Il Titolare si avvale di soggetti esterni per l'esecuzione di specifiche attività connesse alla gestione del Programma Regionale Lazio FSE+ 2021-2027, come ad esempio fornitori di servizi informatici o altri sistemi di gestione documentale. In ossequio all'art. 28 GDPR, tra le parti vengono stipulati per iscritto dei contratti giuridici specifici sulla protezione dei dati nell'ambito dei quali il Titolare fornisce istruzioni, compiti ed oneri in capo a tali soggetti. [Nota: se 	

	<p>si vuole ridurre il volume dell’informativa quanto segue si può espungere] Al fine di rispettare il GDPR e tutelare i diritti e le libertà delle persone, il Titolare ricorre unicamente a Responsabili del trattamento che presentino garanzie sufficienti (conoscenza specialistica, esperienza, capacità e affidabilità) per mettere in atto misure tecniche e organizzative adeguate per la sicurezza di informazioni e dati personali e garantire la protezione degli interessati.</p> <p>- Autorizzati al trattamento: i suoi dati personali saranno trattati da persone interne all’organizzazione del Titolare (es. dirigenti, dipendenti e ausiliari, componenti degli organi di governo e di controllo) previamente individuati e nominati quali “Autorizzati” al trattamento, a cui sono impartite idonee istruzioni in ordine a misure, accorgimenti, modus operandi, tutti volti alla concreta protezione dei dati personali. La possibilità di accedere ai dati è limitata ai soli soggetti effettivamente legittimati.</p> <p>- Eventuali altri destinatari: In specifici casi e nei limiti delle finalità descritte, i Suoi dati personali potranno essere comunicati a: (i) altre autorità pubbliche, enti locali (province, comuni) o organizzazioni regionali coinvolte nel Programma Regionale FSE+ 2021-2027 per l’esecuzione delle loro funzioni amministrative; (ii) forze di polizia e autorità giudiziarie per l’adempimento di obblighi di legge o per esigenze legate a indagini o procedimenti legali; (iii) organi di controllo e audit nazionali ed europei, come l’autorità di audit e la Corte dei conti europea, ai fini delle verifiche di conformità.</p> <p>Nei casi di “contitolarità” con altri enti pubblici, in conformità all’art. 26 GDPR, verrà reso disponibile un accordo che definisce le rispettive responsabilità e finalità, consultabile nella sezione privacy del sito istituzionale.</p> <p>Altre volte i suoi dati personali potranno essere comunicati a soggetti che li tratteranno in “completa autonomia” quali: ASL, Aziende ospedaliere e Regioni, assicurazioni, etc.</p> <p>In ogni caso, i dati personali potranno essere comunicati o diffusi solo in adempimento a obblighi di legge o di regolamento o di atti amministrativi generali (es.: L. 241/1990; D.lgs. n. 33/2013; etc.)</p>
	<p style="text-align: center;">TRASFERIMENTO VERSO PAESI TERZI (EXTRA UE) O ORGANIZZAZIONI INTERNAZIONALI</p> <p>Non è intenzione del Titolare trasferire i suoi dati personali verso Paesi non appartenenti allo Spazio Economico Europeo (SEE) o organizzazioni internazionali che possano pregiudicare il livello di protezione delle persone fisiche garantito dal GDPR.</p> <p>In ogni caso, in considerazione degli obblighi di cui al capo V del GDPR, i trasferimenti internazionali saranno consentiti in presenza di una decisione di adeguatezza (cfr. https://www.garanteprivacy.it/temi/trasferimento-di-dati-all-estero).</p>

	<p style="text-align: center;">DIRITTI DEGLI INTERESSATI</p> <p>Ai sensi degli articoli da 15 a 22 del GDPR, in relazione ai suoi dati personali, nei casi previsti, Lei ha il diritto di: accedere e chiederne copia; richiedere la rettifica; richiedere la cancellazione; ottenere la limitazione del trattamento; opporsi al trattamento; portabilità¹; non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato.</p> <p>Per qualsiasi ulteriore informazione relativa al trattamento dei suoi dati personali, anche a seguito dell'aggiornamento della presente informativa, e per far valere i diritti a Lei riconosciuti dal GDPR, non esiti a contattare il Titolare o il DPO.</p>
	<p style="text-align: center;">RECLAMI</p> <p>È sempre possibile proporre reclamo al Garante per la protezione dei dati personali o di adire le opportune sedi giudiziarie (rispettivamente ai sensi degli artt. 77 e 79 GDPR).</p>

Il Direttore

della Direzione
Regionale

n.q. di Soggetto
Designato al trattamento
dal Titolare

____nome e
cognome_____

[FIRMA DIGITALE]

Icone realizzate da Osservatorio679 Lic CC BY

FINE INFORMATIVA

LA GIUNTA REGIONALE DEL LAZIO LA RINGRAZIA DELLA CONSULTAZIONE

¹ Ai sensi dell'art. 20, par. 3, del GDPR: "Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento."

SCHEMA G⁽⁶⁾

(art. 474, c. 2)

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

ALLEGATO ALLA DETERMINAZIONE REGIONALE N. ___ DEL ____

TRA

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

E

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

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

PREMESSO CHE

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

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

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

VISTO il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito anche “RGPD” o “Regolamento (UE) 2016/679”), il quale

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

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

VISTO il decreto legislativo 196/2003 “*Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*” e successive modificazioni;

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

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

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

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

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

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

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

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

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

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

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

SEZIONE I

1. Clausola 1

Scopo e ambito di applicazione

- a) scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati);
- b) il Titolare del trattamento ed il responsabile del trattamento di cui all'allegato I accettano le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del Regolamento (UE) 2016/679;
- c) le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.
- d) gli allegati da I a VI costituiscono parte integrante delle clausole;
- e) le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il Titolare del trattamento a norma del Regolamento (UE) 2016/679;
- f) le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del Regolamento (UE) 2016/679.

2. Clausola 2

Invariabilità delle clausole

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

3. Clausola 3

Interpretazione

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

4. Clausola 4

Gerarchia

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

5. Clausola 5 (facoltativa)

Clausola di adesione successiva

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

SEZIONE II OBBLIGHI DELLE PARTI

6. Clausola 6

Descrizione del trattamento

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

7. Clausola 7

Obblighi delle parti

7.1. Istruzioni

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

7.2. Limitazione delle finalità

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

7.3. Durata del trattamento dei dati personali

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

7.4. Sicurezza del trattamento

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

7.5. Dati “sensibili” o “particolari”

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

7.6. Documentazione e rispetto

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

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

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

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

7.8. Trasferimenti internazionali

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

8. Clausola 8

Assistenza al titolare del trattamento

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

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

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

9. Clausola 9

Notifica di una violazione dei dati personali

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

9.1. Violazione riguardante dati trattati dal Titolare del trattamento

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

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

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

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

9.2. Violazione riguardante dati trattati dal responsabile del trattamento

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

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

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

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

SEZIONE III
DISPOSIZIONI FINALI

10. Clausola 10

Inosservanza delle clausole e risoluzione

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

SEZIONE IV

ULTERIORI DISPOSIZIONI

11. Clausola 11

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

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

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

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

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

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

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

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

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

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

Lazio;

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

Il Titolare del trattamento

Il Responsabile del trattamento

ALLEGATO I

Elenco delle parti

**Titolare del trattamento:
Giunta Regionale del Lazio**

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

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

.....

Data _____

Firma

.....

Responsabile del trattamento Ragione sociale

Sede legale:

via, n.

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

PEC: laziocrea@legalmail.it

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

.....

Nome, qualifica e dati di contatto del referente:

Inserire nome referente interno

CONTESTO DI RIFERIMENTO

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

ALLEGATO II
Descrizione del trattamento

Categorie di interessati i cui dati personali sono trattati

Categorie di dati personali trattati

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

Natura del trattamento

....

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

Durata del trattamento

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

ALLEGATO III

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

NOTA ESPLICATIVA:

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

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

Le misure applicate al trattamento sono:

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

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

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

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

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

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

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

21	Previsione di elevati requisiti di complessità delle password su tutti gli account, quali: requisito di lunghezza minima di 8 caratteri; Invito a non utilizzare password comuni; educazione degli utenti a non utilizzare le password già utilizzate in ambito aziendale per scopi non legati al lavoro.
22	Razionalizzazione degli account di dominio, evitando l'annidamento di gruppi di utenti all'interno di altri gruppi amministrativi. Riduzione degli account amministrativi ad un numero essenziale, secondo i seguenti approcci: - Applicazione di restrizioni agli account locali per l'accesso remoto. - Limitazione dell'accesso di rete a tutti gli account di amministratore locale.
23	Segmentazione delle reti evitando subnet eccessivamente ampie e limitando, di fatto, la possibilità per un potenziale attaccante di eseguire movimenti laterali, favorendo il principio del privilegio minimo
24	Ove necessario, aggiornamento di firmware o SO di tutti i sistemi e i dispositivi di protezione perimetrale (Firewall, IDS/IPS, Proxy /Reverse Proxy) alle ultime release rilasciate dai rispettivi produttori
25	Individuazione di un'unica tipologia di accesso e gestione remota dei sistemi (ad esempio RDP), evitando l'utilizzo esteso di strumenti di terze parti sfruttabili anche da utenti malintenzionati (ad esempio Dameware, AnyDesk, LogMeIn)
26	Aggiornamento, all'occorrenza, dei sistemi operativi risultanti in stato end of life o end of support.
27	In caso di intrusione o minaccia, reinstallazione completa di tutti i sistemi server e contestuale posizionamento in segmenti di rete suddivisi per layer di sicurezza (Tier), ad accesso limitato e amministrabili solo da un numero limitato di workstation, a loro volta isolate dalle altre reti
28	Standardizzazione della configurazione dei Domain Controller, evitando di adibire gli stessi a ruoli secondari come ad esempio Print Server. Limitazione dell'accesso ai sistemi critici solo ad un numero ristretto di utenti, e solo da specifiche postazioni
29	Utilizzo di apparati "Next generation Firewall" periferici, segregazione dei siti, attivazione dei moduli IDS/IPS
30	Utilizzo di politiche restrittive sulla navigazione in internet degli utenti, favorendo il principio del privilegio minimo
31	Dissuasione rispetto all'utilizzo di account di servizio per accedere in modo interattivo. Monitoraggio costante dell'utilizzo degli account di servizio ed indagini circa eventuali accessi interattivi, ad esempio utilizzando il servizio offerto da Active Directory e le Group Policy ai fini della registrazione dettagliata degli eventi
32	Utilizzo di tecnologia SIEM e/o di un servizio di Cyber Detection & Protection, essenziale per la sicurezza dell'infrastruttura e per la raccolta e razionalizzazione centralizzata di log ed eventi di sicurezza provenienti da diverse sorgenti
33	Utilizzo di un servizio di Security Awareness & Training finalizzato all'educazione degli utenti in ambito Cyber Security
34	Esecuzione di assessment periodici sui livelli di maturità dei controlli di sicurezza previsti dai principali standard nazionali ed internazionali. Definizione di diversi domini di intervento analizzando gli obiettivi dell'ente e le informazioni relative ad incidenti pregressi correlati. Valutazione di possibili ulteriori azioni a fronte dei risultati dell'assessment. Consolidamento della propensione al rischio minimo e definizione di soglie di tolleranza del rischio in ciascun dominio individuate.

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

ALLEGATO IV

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

(ove applicabile indicare eventuali subappaltatori del fornitore)

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

Ragione sociale del sub-responsabile

SUB-TRATTAMENTO DELEGATO: Gestione xxxxxxxxxxxxxx.

ALLEGATO V**Disciplina dei servizi di Amministratore di Sistema**

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

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

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

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

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

ALLEGATO VI

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

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

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

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

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

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