

## ALLEGATO 8

### ***NOMINA RESPONSABILE DEL TRATTAMENTO***

**ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI** (*Allegato8 alle Linee di indirizzo per la realizzazione dell'integrazione scolastica, anche attraverso la Comunicazione Aumentativa Alternativa (CAA), in favore degli alunni con disabilità sensoriale visiva, uditiva e nella comprensione e produzione del linguaggio. Anno scolastico 2023-24" - Determinazione n. \_\_\_\_ del \_\_\_\_\_* (da compilare a cura dell'Ente proponente: Istituzione scolastica/formativa/Comune/Municipio).

### **TRA**

La Giunta Regionale del Lazio, con sede in Via R. Raimondi Garibaldi 7– 00147 Roma, nella persona del Direttore Regionale Istruzione, Formazione e Politiche per l'Occupazione Avvocato Elisabetta Longo;

### **E**

La < **indicare la denominazione dell'Istituzione Scolastica/Formativa/Ente Gestore Paritarie /Comune o Municipio** >, con sede in .....in persona del Dirigente scolastico/Direttore pro tempore/Legale Rappresentante dell'Ente richiedente .....

### **PREMESSO CHE**

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

svolge attività che comportano il trattamento di dati personali nell'ambito dei servizi 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 a 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 R.R. 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, disciplina i trattamenti affidati al responsabile, i compiti e le istruzioni secondo quanto previsto dall'articolo 28, paragrafo 3, del Regolamento (UE) 2016/679 (di seguito anche “RGPD”) 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 un sub-responsabile, secondo quanto previsto dall'articolo 28, paragrafi 2 e 4, del RGPD;

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

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 delle “Linee di indirizzo per la realizzazione dell’integrazione scolastica, anche attraverso la Comunicazione Aumentativa Alternativa (CAA), in favore degli alunni con disabilità sensoriale visiva, uditiva e nella comprensione e produzione del linguaggio. Anno scolastico 2023-24” - Determinazione n. \_\_\_\_ del \_\_\_\_\_, tra Regione Lazio e l’Ente richiedente **<indicare la denominazione dell’Istituzione Scolastica/Formativa/Ente Gestore Paritarie /Comune o Municipio >**, 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 prevede che “Titolare del Trattamento” sia “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’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 “Misure minime AgID”), il quale 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, l’Ente proponente suddetto 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 del Lazio è Titolare soddisfi i requisiti e il pieno rispetto delle disposizioni previste dal RGPD;

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

## Articolo 1

<indicare la denominazione dell'Istituzione Scolastica/Formativa/Ente Gestore Paritarie /Comune o Municipio > in qualità di **RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI** in virtù del presente atto di designazione, ai sensi e per gli effetti delle vigenti disposizioni normative di cui agli articoli 4, n. 8) e 28 del RGPD, con riguardo alle operazioni di trattamento connesse all'esecuzione del suddetto contratto, dichiara di essere edotto di tutti gli obblighi che incombono sul Responsabile del trattamento e si impegna a rispettarne e a consentirne ogni prerogativa, obbligo, onere e diritto che discende da tale posizione giuridica, attenendosi alle disposizioni operative contenute nel presente atto.

## Articolo 2

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:

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:

- il trattamento è svolto *per la realizzazione dell'integrazione scolastica, anche attraverso la Comunicazione Aumentativa Alternativa (CAA), in favore degli alunni con disabilità sensoriale visiva, uditiva e nella comprensione e produzione del linguaggio. Anno scolastico 2023-24"* - Determinazione n. \_\_\_\_ del \_\_\_\_\_;
- i dati personali trattati in ragione delle attività di cui alle suddette Linee hanno ad oggetto le attività relative alla programmazione degli interventi per l'integrazione scolastica degli alunni con disabilità sensoriale visiva, uditiva e nella comprensione e produzione del linguaggio, residenti nella regione e frequentanti le scuole pubbliche e paritarie di ogni ordine e grado, richiedenti il servizio di assistenza;
- il trattamento è svolto per le finalità di cui alle Linee di indirizzo e per:
  - consentire alle Istituzioni Scolastiche/Formative pubbliche e paritarie, Comuni e Municipi di effettuare la richiesta del servizio di assistenza sensoriale visiva, uditiva e di CAA nonché l'ammissione all'erogazione dei servizi stessi. In particolare, effettuare le necessarie attività amministrative/istruttorie e di controllo volte alla valutazione circa l'ammissibilità delle domande inoltrate;
  - consentire l'effettuazione di tutte le comunicazioni inerenti alle attività previste dalle linee di indirizzo;
  - effettuare le doverose attività di competenza dell'amministrazione regionale in ordine alla valutazione, attuazione, rendicontazione, controllo amministrativo e delle spese nel rispetto delle disposizioni normative applicabili in materia e del monitoraggio.

In particolare:

- le tipologie di dati trattati relativamente agli alunni sono dati personali (art. 4, punto 1 RGPD) e dati personali sensibili (art. 9 del RGPD) quali:
  - dati identificativi: nome, cognome, luogo e data di nascita, codice fiscale, residenza, numero del documento d'identità, contatti telefonici, altri elementi identificativi, dati relativi all'istruzione (codice meccanografico della scuola frequentata);
  - dati relativi alla composizione familiare e alla situazione reddituale (ISEE);
  - dati particolari c.d. "sensibili": stato di salute e di disabilità ex legge 104 degli allievi;
- le tipologie di dati trattati relativamente alle Istituzioni richiedenti il servizio Enti preposti ed Enti gestori sono dati personali (art. 4, punto 1 RGPD) e personali giudiziari (art. 10 del RGPD) quali:

- dati personali identificativi delle risorse umane coinvolte nel progetto: nome, cognome, luogo e data di nascita, codice fiscale, residenza, numero del documento d'identità, contatti telefonici;
- dati dell'ente richiedente: denominazione/ragione sociale, codice fiscale/partita IVA, sede legale e sede/i operativa/e, domicilio digitale e recapiti telefonici;
- informazioni relative all'impiego delle risorse umane coinvolte nel progetto, quali mansioni e ruolo ricoperto; qualifiche professionali, titoli di studio;
- copia di documenti di identità e informazioni correlate;
- dati bancari e finanziari (quali il numero di conto corrente e/o il codice IBAN, etc.), dati INPS, INAIL o altre casse, dati su CCNL applicato (per Istituzioni Formative non pubbliche);
- dichiarazioni rese dall'interessato o che abbiano ad oggetto l'interessato;
- dati particolari idonei a rivelare condanne penali e reati.

L'Istituzione richiedente è autorizzata 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.

L'Istituzione richiedente 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 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.

L'Istituzione richiedente dovrà eseguire i trattamenti funzionali alle attività ad essa 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, l'Istituzione richiedente dovrà informare il Titolare del trattamento ed il Responsabile della Protezione dei Dati (DPO) della Giunta Regionale del Lazio.

L'Istituzione richiedente – per quanto di propria competenza – è tenuta, in forza della normativa cogente e delle presenti Linee, a garantire – per sé, per i propri dipendenti e per chiunque collabori a qualunque titolo – il rispetto della riservatezza, integrità, disponibilità e qualità dei dati, nonché l'utilizzo dei predetti dati per le sole finalità specificate nel presente atto e nell'ambito delle attività di sicurezza di specifico interesse del Titolare.

L'Istituzione richiedente ha il compito di curare, in relazione alla fornitura del servizio di cui alle presenti Linee, l'attuazione delle misure prescritte dal Garante per la protezione dei dati personali in merito all'attribuzione delle funzioni di "Amministratore di Sistema" di cui al provvedimento del 27 novembre 2008, e successive modificazioni e, in particolare, di:

- 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 Regione Lazio è titolare;
- conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte all'interno della vostra Istituzione quali Amministratori di Sistema (in relazione ai dati personali del cui trattamento la Giunta Regionale del Lazio è titolare);
- porre in essere 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.

L'Istituzione richiedente 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.

L'Istituzione richiedente dovrà attivare le necessarie procedure 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. L'Istituzione richiedente garantirà, inoltre, che le persone autorizzate al trattamento siano vincolate da un obbligo, legalmente assunto, di riservatezza.

L'Istituzione richiedente 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, per garantire un livello di sicurezza adeguato al rischio. Tali misure, qualora necessario, comprendono, altresì, le seguenti:

- a) misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- b) misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
- c) 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, l'Istituzione richiedente 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.

L'Istituzione richiedente 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, 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, l'Istituzione richiedente dovesse ritenere che le misure adottate non siano più adeguate e/o idonee a prevenire/mitigare i rischi sopramenzionati, è tenuta 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 devono aver luogo prima di iniziare e/o continuare qualsiasi operazione di trattamento di dati.

L'Istituzione richiedente è tenuta 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.

Inoltre, l'Istituzione richiedente dovrà adottare le misure minime di sicurezza ICT per le PP.AA. di cui alla circolare AgID del 18 aprile 2017, n. 2/2017 ove applicabile, nonché le eventuali ulteriori misure specifiche stabilite dal Titolare, nel rispetto dei contratti vigenti.

L'Istituzione richiedente 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 da parte del Titolare stesso o di un altro soggetto da questi incaricato.

L'Istituzione richiedente 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.

L'Istituzione richiedente, ai sensi dell'articolo 30 del RGPD e nei limiti di quanto in esso previsto, è tenuta a tenere un Registro delle attività di Trattamento effettuate sotto la propria responsabilità per conto del Titolare e a cooperare con il Titolare e con il Garante per la protezione dei dati personali, laddove ne venga fatta richiesta ai sensi dell'articolo 30, paragrafo 4, del RGPD.

L'Istituzione richiedente è tenuta 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, al più presto, comunque non oltre 48 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 tale violazione al Garante per la protezione dei dati personali e/o a darne comunicazione agli interessati, entro il termine di 72 ore da quando il Titolare ne è venuto a conoscenza. Nel caso in cui il Titolare debba fornire informazioni aggiuntive alla suddetta Autorità, l'Istituzione richiedente supporterà il Titolare stesso 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.

L'Istituzione richiedente, su eventuale richiesta del Titolare, è tenuta inoltre ad assistere quest'ultimo nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente a quanto prescritto dall'articolo 35 del RGPD e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall'articolo 36 del RGPD.

L'Istituzione richiedente, qualora riceva istanze da parte degli interessati in esercizio dei loro diritti ai sensi degli articoli da 15 a 22 del RGPD, è tenuta a:

- darne tempestiva comunicazione scritta al Titolare e al Responsabile della Protezione dei Dati (DPO) della Regione Lazio, allegando copia della richiesta;
- valutare con il Titolare e con il DPO della Regione Lazio la legittimità delle richieste;
- coordinarsi con il Titolare e con il DPO della Regione Lazio al fine di soddisfare le richieste ritenute legittime.

Laddove fosse espressamente autorizzata dalla Regione Lazio la sub-fornitura/il sub-appalto, l'Istituzione richiedente è tenuta a procedere alla designazione di detti sub-fornitori/sub-appaltatori, preventivamente autorizzati dalla Regione stessa, quali Responsabili del trattamento, imponendogli, mediante contratto o altro atto giuridico, i medesimi obblighi in materia di protezione dei dati contenuti nella presente nomina, prevedendo, in particolare, garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del RGPD. Qualora l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, l'Istituzione richiedente conserverà nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile ai sensi dell'articolo 28, paragrafo 4 del RGPD.

L'Istituzione richiedente garantisce gli adempimenti e le incombenze anche formali verso il Garante 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, su specifica richiesta:

- 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.

L'Istituzione richiedente si impegna ad adottare, su richiesta del Titolare e nel rispetto degli obblighi assunti inerenti le presenti Linee, ulteriori garanzie quali l'applicazione di un codice di condotta 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.

L'Istituzione richiedente 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.

L'Istituzione richiedente è tenuta a comunicare al Titolare ed al DPO della Regione Lazio il nome ed i dati del proprio DPO, laddove la stessa 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.

Per "persone autorizzate al trattamento" ai sensi dell'articolo 4, punto 10 secondo quanto previsto 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.

L'Istituzione richiedente è tenuta 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.

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. In particolare, l'Istituzione richiedente garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

L'Istituzione richiedente è tenuta, altresì, a vigilare sulla puntuale osservanza delle proprie istruzioni.

### **Articolo 3**

In conformità a quanto prescritto dal Provvedimento del Garante del 27/11/2008 e successive modificazioni ed alle citate Misure minime AgID relativamente alle utenze Amministrative, laddove le prestazioni contrattuali implicino l'erogazione di servizi di amministrazione di sistema, l'Istituzione richiedente, in qualità di Responsabile del trattamento, si impegna a:

- 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;
- 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:
  - divieto di assegnazione di user id generiche e già attribuite anche in tempi diversi;

- 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 in capo a chi ne fa uso;
  - disattivazione delle user id attribuite agli Amministratori che non necessitano più di accedere ai dati;
  - associare alle user id assegnate agli Amministratori una password e garantire il rispetto delle seguenti regole:
  - utilizzare password con lunghezza minima di almeno 14 caratteri, qualora l'autenticazione a più fattori non sia supportata;
  - cambiare la password alla prima connessione e successivamente almeno ogni 30 giorni (password aging).
  - le password devono differire dalle ultime 5 utilizzate (password history);
  - conservare le password in modo da garantirne disponibilità e riservatezza;
  - 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;
  - assicurare che l'archiviazione di password o codici PIN su qualsiasi supporto fisico avvenga solo in forma protetta da sistemi di cifratura;
- assicurare la completa distinzione tra utenze privilegiate e non privilegiate di amministratore, alle quali devono corrispondere credenziali diverse;
  - 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;
  - mantenere aggiornato un inventario delle utenze privilegiate (Anagrafica AdS), anche attraverso uno strumento automatico in grado di generare un alert quando è aggiunta un'utenza amministrativa e quando sono aumentati i diritti di un'utenza amministrativa;
  - 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 l'Istituzione richiedente utilizzi sistemi messi a disposizione dalla Regione, comunicare agli Amministratori che la Regione stessa procederà alla registrazione e conservazione dei log;
  - impedire l'accesso diretto ai singoli sistemi con le utenze amministrative. In particolare, deve essere imposto l'obbligo per l'Amministratore di accedere con un'utenza normale e solo successivamente dargli la possibilità di eseguire, come utente privilegiato, i singoli comandi;
  - 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;
  - comunicare alla Regione, al momento della sottoscrizione del presente atto, e comunque con cadenza almeno annuale ed ogni qualvolta se ne verifichi la necessità, 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:
    - il nome e cognome;
    - la user id assegnata agli Amministratori;
    - il ruolo degli Amministratori (ovvero di Sistema, Base Dati, di Rete e/o di Software Complessi);
    - i sistemi che gli stessi gestiscono, specificando per ciascuno il profilo di autorizzazione assegnato;
  - 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;



- 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;
- durante l'esecuzione della procedura prevista dalle presenti Linee, 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), l'Istituzione richiedente 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.

La presente nomina ha efficacia fino al termine della procedura relativa al servizio di assistenza di cui alle presenti Linee, tra Regione Lazio e Istituzione richiedente.

Al termine della procedura in essere con la Regione Lazio, l'Istituzione richiedente, sulla base delle determinazioni della Regione stessa, restituirà i dati personali oggetto del trattamento oppure provvederà alla loro integrale distruzione, salvo che i diritti dell'Unione e degli Stati membri ne prevedano la conservazione. In entrambi i casi rilascerà un'attestazione scritta di non aver trattenuto alcuna copia dei dati.

Sottoscrivendo il presente atto, **<indicare la denominazione dell'Istituzione Scolastica/Formativa/Ente Gestore Paritarie /Comune o Municipio >**

☐ conferma di conoscere gli obblighi assunti in relazione alle disposizioni del RGPD e di possedere i requisiti di esperienza, capacità ed affidabilità idonei a garantire il rispetto di quanto disposto dal medesimo regolamento e sue eventuali modifiche ed integrazioni;

☐ conferma di aver compreso integralmente le istruzioni qui impartite e si dichiara competente e disponibile alla piena esecuzione di quanto affidato;

☐ accetta la nomina di Responsabile del trattamento dei dati personali e si impegna ad attenersi rigorosamente a quanto ivi stabilito, nonché alle eventuali successive modifiche ed integrazioni disposte dal Titolare, anche in ottemperanza alle modifiche normative in materia.

Data

Per il Responsabile del Trattamento

Firma Digitale del Legale Rappresentante

---