

**Direzione:** ISTRUZIONE FORMAZIONE E POLITICHE PER L'OCCUPAZIONE**Area:** OFFERTA PER IL DIRITTO ALLO STUDIO E DIMENSIONAMENTO ALLOGGIATIVO UNIVERSITARIO**DETERMINAZIONE (con firma digitale)**

N. G08695 del 01/07/2024

Proposta n. 22799 del 17/06/2024

Oggetto:**Presenza annotazioni contabili**

Linee guida per lo svolgimento del servizio di trasporto scolastico degli studenti con disabilità residenti nella Regione Lazio e frequentanti le Istituzioni Scolastiche secondarie di II grado statali o paritarie o i Percorsi triennali di IeFP. Anno scolastico 2024/25. Prenotazione impegno pluriennale di spesa di euro 1.800.000,00 in favore di creditori diversi a valere sul Capitolo U0000F11900 di cui euro 900.000,00 per l'esercizio finanziario 2024 e euro 900.000,00 per l'esercizio finanziario 2025.

Proponente:

Estensore	RECCHIA ANGELA PAOLA	_____firma elettronica_____
Responsabile del procedimento	RECCHIA ANGELA PAOLA	_____firma elettronica_____
Responsabile dell' Area	A D'ALESSIO	_____firma digitale_____
Direttore Regionale	E. LONGO	_____firma digitale_____

Firma di Concerto

Ragioneria:

Responsabile del procedimento		_____
Responsabile dell'Area Ragioneria	DELLARNO GIUSEPPE	_____firma digitale_____
Dir.Reg. Bil. Gov. Soc., Dem. e Patr.	MARCO MARAFINI	_____firma digitale_____

REGIONE LAZIO

Proposta n. 22799 del 17/06/2024

Annotazioni Contabili (con firma digitale)

PGC	Tipo	Capitolo	Impegno /	Mod.	Importo	Miss./Progr./PdC finanz.
	Mov.		Accertamento			

Descr. PdC finanz.**Azione****Beneficiario**

1)	P	U0000F11900	2024		900.000,00	04.07 1.04.01.02.000
----	---	-------------	------	--	------------	----------------------

Trasferimenti correnti a Amministrazioni Locali

1.02.02.25

CREDITORI DIVERSI

Tipo mov. : CRONOPROGRAMMA PLURIENNALE PRENOTAZIONE NO DL 50

2)	P	U0000F11900	2025		900.000,00	04.07 1.04.01.02.000
----	---	-------------	------	--	------------	----------------------

Trasferimenti correnti a Amministrazioni Locali

1.02.02.25

CREDITORI DIVERSI

Tipo mov. : CRONOPROGRAMMA PLURIENNALE PRENOTAZIONE NO DL 50

OGGETTO: Linee guida per lo svolgimento del servizio di trasporto scolastico degli studenti con disabilità residenti nella Regione Lazio e frequentanti le Istituzioni Scolastiche secondarie di II grado statali o paritarie o i Percorsi triennali di IeFP. Anno scolastico 2024/25. Prenotazione impegno pluriennale di spesa di euro 1.800.000,00 in favore di creditori diversi a valere sul Capitolo U0000F11900 di cui euro 900.000,00 per l'esercizio finanziario 2024 e euro 900.000,00 per l'esercizio finanziario 2025.

LA DIRETTRICE DELLA DIREZIONE REGIONALE ISTRUZIONE, FORMAZIONE E POLITICHE PER L'OCCUPAZIONE

SU PROPOSTA dell'Area Offerta per il Diritto allo Studio e Dimensionamento alloggiativo universitario;

VISTI gli articoli 3, 34, 117 terzo comma e 118 della Costituzione;

VISTO lo Statuto Regionale;

VISTA la Legge Regionale 18 febbraio 2002, n. 6 - Disciplina del sistema organizzativo della Giunta e del Consiglio e disposizioni relative alla dirigenza ed al personale regionale - e successive modificazioni;

VISTO il Regolamento Regionale 6 settembre 2002, n. 1 - Organizzazione degli uffici e dei servizi della Giunta Regionale - e successive modificazioni e integrazioni, ed in particolare il Capo I del Titolo III relativo alle strutture organizzative per la gestione;

VISTA la Deliberazione di Giunta Regionale del 18 gennaio 2024, n. 25 con la quale è stato conferito l'incarico di Direttore della Direzione Regionale Istruzione, Formazione e Politiche per l'occupazione all'Avv. Elisabetta Longo;

VISTO l'Atto di Organizzazione 1 maggio 2024, n. G05119 - Novazione del contratto reg. cron. n. 28901 del 24.11.2022 concernente: Contratto a tempo pieno e determinato per il conferimento dell'incarico di dirigente dell'Area "Diritto allo Studio Scolastico e Universitario della Direzione regionale Istruzione, Formazione e Lavoro" conferito alla dott.ssa Agnese D'ALESSIO;

VISTO il Decreto Legislativo 23 giugno 2011, n. 118 - Disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi, a norma degli articoli 1 e 2 della legge 5 maggio 2009, n. 42 - e successive modifiche;

VISTA la Legge regionale 12 agosto 2020, n. 11 - Legge di contabilità regionale;

VISTO il Regolamento regionale 9 novembre 2017, n. 26 - Regolamento regionale di contabilità che, ai sensi dell'articolo 56, comma 2, della l.r. n. 11/2020 e fino alla data di entrata in vigore del regolamento di contabilità di cui all'articolo 55 della citata l.r. n. 11/2020, continua ad applicarsi per quanto compatibile con le disposizioni di cui alla medesima l.r. n. 11/2020;

VISTO l'articolo 30, comma 2, del Regolamento regionale n. 26/2017, in riferimento alla predisposizione del piano finanziario di attuazione della spesa;

VISTA la Legge regionale 29 dicembre 2023, n. 23 - Legge di stabilità regionale 2024;

VISTA la Legge regionale 29 dicembre 2023, n. 24 - Bilancio di previsione finanziario della Regione Lazio 2024-2026;

VISTA la Deliberazione di Giunta regionale 28 dicembre 2023, n. 980 - Bilancio di previsione finanziario della Regione Lazio 2024-2026. Approvazione del “Documento tecnico di accompagnamento”, ripartito in titoli, tipologie e categorie per le entrate e in missioni, programmi, titoli e macroaggregati per le spese;

VISTA la Deliberazione di Giunta regionale 28 dicembre 2023, n. 981 - Bilancio di previsione finanziario della Regione Lazio 2024-2026. Approvazione del “Bilancio finanziario gestionale”, ripartito in capitoli di entrata e di spesa e assegnazione delle risorse finanziarie ai dirigenti titolari dei centri di responsabilità amministrativa;

VISTA la Deliberazione di Giunta regionale 14 febbraio 2024, n. 75 - Indirizzi per la gestione del bilancio regionale 2024-2026 e approvazione del bilancio reticolare, ai sensi degli articoli 30, 31 e 32, della legge regionale 12 agosto 2020, n. 11;

VISTA la Deliberazione della Giunta regionale del 24 aprile 2024 n. 284 - Bilancio di previsione finanziario della Regione Lazio 2024-2026. Aggiornamento del Bilancio finanziario gestionale in relazione all’assegnazione delle risorse finanziarie ai dirigenti titolari dei centri di responsabilità amministrativa, di cui alla D.G.R. n. 981/2023, ai sensi dell’articolo 13, comma 5, della legge regionale 12 agosto 2020, n. 11;

VISTO l’articolo 10 comma 3 lett. a) del Decreto legislativo del 23 giugno 2011, n. 118;

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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati - RGPD);

VISTO il Decreto Legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali;

VISTO il Decreto Legislativo 10 agosto 2018, n. 101 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni 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 - RGPD);

VISTI gli articoli 473 e ss. del R. R. 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della Giunta Regionale) che disciplinano le modalità organizzative di gestione delle attività di trattamento dei dati personali all’interno della Giunta regionale del Lazio;

VISTA la Decisione di Esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021 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 e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio;

VISTE le Linee guida funzioni crittografiche adottate dall’Agenzia per la Cybersicurezza Nazionale nel dicembre 2023;

VISTA la Legge 5 febbraio 1992, n. 104 - Legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate;

VISTA la Convenzione delle Nazioni Unite sui diritti delle persone con disabilità approvata dall'Assemblea Generale delle Nazioni Unite il 13 dicembre 2006;

VISTA la Legge 3 marzo 2009, n. 18 - Ratifica ed esecuzione della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, con Protocollo opzionale, fatta a New York il 13 dicembre 2006 e istituzione dell'Osservatorio nazionale sulla condizione delle persone con disabilità;

VISTA la Legge 10 marzo 2000, n. 62 - Norme per la parità scolastica e disposizioni sul diritto allo studio e all'istruzione;

VISTA la Legge 13 luglio 2015, n. 107 - Riforma del sistema nazionale di istruzione e formazione e delega per il riordino delle disposizioni legislative vigenti;

VISTO il Decreto Legislativo 13 aprile 2017, n. 66 - Norme per la promozione dell'inclusione scolastica degli studenti con disabilità, a norma dell'articolo 1, commi 180 e 181, lettera c), della legge 13 luglio 2015, n. 107;

VISTO il Decreto Legislativo 31 marzo 1998, n. 112 - Conferimento di funzioni e compiti amministrativi dello Stato alle regioni ed agli enti locali, in attuazione del capo I della legge 15 marzo 1997, n. 59;

VISTA la legge 7 aprile 2014, n. 56 - Disposizioni sulle città metropolitane, sulle province, sulle unioni e fusioni di comuni;

VISTA la Legge 28 dicembre 2015, n. 208 - Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge di stabilità 2016) – e in particolare l'art. 1, comma 947;

VISTA la nota prot. n. 354459 del 13/03/2024 recante il Calendario scolastico regionale 2024/25;

RILEVATO che la Legge n. 104/1992 ha tra le proprie finalità:

- garantire il pieno rispetto della dignità umana e dei diritti di libertà e di autonomia della persona con disabilità, promuovendone la piena integrazione nella famiglia, nella scuola, nel lavoro e nella società;
- predisporre interventi volti a superare stati di emarginazione e di esclusione sociale della persona con disabilità;

RILEVATO, inoltre, che la Convenzione delle Nazioni Unite sui diritti delle persone con disabilità all'art. 24 riconosce specificamente a tali persone il diritto all'istruzione prescrivendo agli Stati firmatari di realizzare un sistema educativo che preveda la loro integrazione scolastica a tutti i livelli e, in particolare, la possibilità di accedere all'istruzione secondaria e alla formazione professionale senza discriminazioni, sulla base dell'eguaglianza con gli altri e all'interno delle comunità di appartenenza;

CONSIDERATO che la Legge n. 104/1992 prevede l'obbligo per gli enti locali di fornire l'assistenza agli alunni con disabilità al fine di garantirne l'integrazione scolastica;

CONSIDERATO che l'articolo 1, comma 947 della Legge di stabilità 2016 prevede che, ai fini del completamento del processo di riordino delle funzioni delle province, di cui all'articolo 1, comma 89, della legge 7 aprile 2014, n. 56, le funzioni relative alle esigenze di cui all'articolo 139, comma 1, lettera c), del decreto legislativo 31 marzo 1998, n. 112, sono attribuite alle regioni a decorrere dal 1° gennaio 2016;

RAVVISATA la necessità di definire, sulla base del quadro normativo vigente, le modalità di organizzazione del servizio di trasporto scolastico degli studenti con disabilità frequentanti le Istituzioni Scolastiche secondarie di II grado al fine di garantirne l'attivazione per l'anno scolastico 2024/25;

VALUTATO opportuno, in base all'art. 89 della Legge Del Rio, individuare quale ambito territoriale ottimale per una efficace organizzazione e gestione del servizio di trasporto scolastico degli studenti disabili del II ciclo quello comunale;

CONSIDERATO che i Comuni del Lazio non sono ancora in grado di quantificare in maniera specifica e definitiva i fabbisogni relativi all'organizzazione e gestione del servizio di trasporto scolastico degli studenti disabili del II ciclo;

TENUTO CONTO dell'urgenza di accantonare immediatamente le risorse necessarie a garantire il corretto avvio del servizio;

TENUTO CONTO che saranno creditori i Comuni da individuarsi mediante la presentazione di apposita domanda corredata di tutte le informazioni necessarie;

VALUTATO necessario stabilire sin d'ora che il valore del contributo regionale per ciascuno studente disabile potrà coprire, di norma, un massimo di 30 chilometri complessivi tra andata e ritorno per ogni giornata di frequenza e che comunque non potrà essere superiore all'importo di euro 3.000,00 annui per utente;

VALUTATO opportuno prevedere la possibilità di erogare un contributo specifico nei limiti della disponibilità delle risorse in caso di interventi di trasporto estremamente complessi e onerosi a causa di situazioni territoriali di particolare isolamento e/o della gravità della disabilità certificata (art. 3, comma 3, della Legge n.104/1992);

RITENUTO necessario, a seguito di quanto esposto, prenotare l'impegno della somma complessiva di euro 1.800.000,00 di cui euro 900.000,00 nell'esercizio finanziario 2024 e euro 900.000,00 nell'esercizio finanziario 2025 in favore di creditori diversi a valere sul capitolo U0000F11900 Missione 04, Programma 07, Piano dei conti finanziario 1.04.01.02.000 che presenta la necessaria disponibilità;

RITENUTO, pertanto, di approvare le "Linee guida per lo svolgimento del servizio di trasporto scolastico degli studenti con disabilità residenti nella Regione Lazio e frequentanti le Istituzioni Scolastiche secondarie di II grado statali o paritarie o i Percorsi triennali di IeFP. Anno scolastico 2024/25" di cui all'Allegato A che costituisce parte integrante e sostanziale della presente determinazione;

RITENUTO di rinviare a successivi provvedimenti l'adozione del piano di riparto delle risorse tra i singoli Comuni, il relativo impegno di spesa e lo stanziamento di eventuali risorse aggiuntive ove necessarie e disponibili;

EVIDENZIATO che nel corso della procedura di raccolta delle domande di attivazione del servizio e di trasmissione delle stesse all'Amministrazione regionale, i Comuni agiranno in qualità di "Responsabili del trattamento dei dati" in conformità all'art. 28 del Regolamento generale sulla protezione dei dati - RGPD;

RITENUTO, pertanto, di approvare l'"Atto di nomina a Responsabile del trattamento dei dati personali" di cui all'Allegato B che costituisce parte integrante e sostanziale della presente determinazione;

TENUTO CONTO che in base all'art. 13 del Regolamento generale sulla protezione dei dati - RGPD il Titolare del trattamento, qualora i dati personali siano raccolti presso l'interessato, fornisce a quest'ultimo tutte le informazioni necessarie a garantire un trattamento corretto e trasparente;

RITENUTO di approvare, ai sensi dell'art. 13 del Regolamento generale sulla protezione dei dati - RGPD, l'"Informativa sul trattamento dei dati personali" di cui all'Allegato C che costituisce parte integrante e sostanziale della presente determinazione;

VALUTATO opportuno, in applicazione del principio di accountability di cui all'art 24 del Regolamento generale sulla protezione dei dati - RGPD, somministrare in via preliminare al Responsabile del trattamento un questionario di verifica del rispetto delle norme in materia di protezione dei dati personali nello svolgimento delle attività di trattamento da parte dello stesso;

RITENUTO, pertanto, di approvare, ai sensi dell'art. 24 del Regolamento generale sulla protezione dei dati - RGPD, il "Questionario per la verifica del rispetto del Regolamento (UE) 2016/679 - Regolamento generale sulla protezione dei dati - sulle attività di trattamento da parte del Responsabile del trattamento" di cui all'Allegato D che costituisce parte integrante e sostanziale della presente determinazione;

D E T E R M I N A

per le motivazioni illustrate in premessa,

- prenotare l'impegno della somma complessiva di euro 1.800.000,00 di cui euro 900.000,00 nell'esercizio finanziario 2024 e euro 900.000,00 nell'esercizio finanziario 2025 in favore di creditori diversi a valere sul capitolo U0000F11900 Missione 04, Programma 07, Piano dei conti finanziario 1.04.01.02.000 che presenta la necessaria disponibilità;

- di approvare le "Linee guida per lo svolgimento del servizio di trasporto scolastico degli studenti con disabilità residenti nella Regione Lazio e frequentanti le Istituzioni Scolastiche secondarie di II grado statali o paritarie o i Percorsi triennali di IeFP. Anno scolastico 2024/25" di cui all'Allegato A che costituisce parte integrante e sostanziale della presente determinazione;

- di rinviare a successivi provvedimenti l'adozione del piano di riparto delle risorse tra i singoli Comuni, il relativo impegno di spesa e lo stanziamento di eventuali risorse aggiuntive ove necessarie e disponibili;

- di approvare l'“Atto di nomina a Responsabile del trattamento dei dati personali” di cui all'Allegato B che costituisce parte integrante e sostanziale della presente determinazione;
- di approvare, ai sensi dell'art. 13 del Regolamento generale sulla protezione dei dati – RGPD, l'“Informativa sul trattamento dei dati personali” di cui all'Allegato C che costituisce parte integrante e sostanziale della presente determinazione;
- di approvare, ai sensi dell'art. 24 del Regolamento generale sulla protezione dei dati – RGPD, il “Questionario per la verifica del rispetto del Regolamento (UE) 2016/679 - Regolamento generale sulla protezione dei dati - sulle attività di trattamento da parte del Responsabile del trattamento” di cui all'Allegato D che costituisce parte integrante e sostanziale della presente determinazione;

Avverso la presente Determinazione è ammesso ricorso con le modalità e nei tempi previsti dalla normativa vigente.

La presente determinazione sarà pubblicata sul Bollettino Ufficiale della Regione Lazio e ne sarà data diffusione sul sito www.regione.lazio.it.

La Direttrice
(Avv. Elisabetta Longo)

Copia

ALLEGATO A

LINEE GUIDA PER LO SVOLGIMENTO DEL SERVIZIO DI TRASPORTO SCOLASTICO DEGLI STUDENTI CON DISABILITÀ RESIDENTI NELLA REGIONE LAZIO E FREQUENTANTI LE ISTITUZIONI SCOLASTICHE SECONDARIE DI II GRADO STATALI O PARITARIE O I PERCORSI TRIENNALI DI IeFP

ANNO SCOLASTICO 2024/25

INDICE

1. PREMESSA

2. QUADRO NORMATIVO DI RIFERIMENTO

3. SERVIZIO DI TRASPORTO SCOLASTICO

3.1 Finalità del servizio

3.2 Tipologia del servizio

3.3 Destinatari del servizio

4. MODALITA' OPERATIVE PER I COMUNI

5. RISORSE FINANZIARIE DISPONIBILI

5.1 Criteri, modalità e tempistiche di assegnazione del contributo

5.2 Adempimenti dei Comuni

1. PREMESSA

Legge Del Rio (legge 7 aprile 2014, n. 56 - Disposizioni sulle città metropolitane, sulle province, sulle unioni e fusioni di comuni), individua nelle Regioni e nei Comuni i due principali livelli territoriali di diretta rappresentanza delle rispettive comunità. Le Regioni e i Comuni, pertanto, insieme agli “enti territoriali di area vasta” denominati Città Metropolitane esercitano le funzioni amministrative preordinate alla tutela e al godimento dei diritti fondamentali.

In questo contesto la Regione Lazio, nell’ottica del principio di leale collaborazione e con l’obiettivo di garantire il fondamentale diritto all’istruzione degli studenti con disabilità frequentanti le scuole secondarie di II grado, adotta le presenti linee guida indirizzate ai Comuni del territorio.

2. QUADRO NORMATIVO DI RIFERIMENTO

La Regione Lazio, ai sensi dell’art. 1, comma 947 della legge di stabilità 2016, intende sostenere gli interventi che riguardano le funzioni relative ai servizi di supporto organizzativo di cui all’art.139, comma 1, lettera c) del decreto legislativo n.112/1998 tra cui il servizio di trasporto scolastico, consistente nel trasporto dello studente con disabilità nel tragitto casa/scuola e viceversa, al fine di agevolare la regolare frequenza scolastica e, più in generale, l’esercizio del diritto allo studio.

La Regione in base all’art. 89 della Legge Del Rio individua l’ambito comunale quale ambito territoriale ottimale per una efficace organizzazione e gestione del servizio di trasporto scolastico degli alunni con disabilità del II ciclo, promuovendo anche forme di esercizio associato di detta funzione da parte di più enti locali.

L’integrazione scolastica degli alunni con disabilità costituisce un punto di forza della scuola italiana, che vuole essere una comunità accogliente nella quale tutti gli alunni, a prescindere dalle loro diversità funzionali, possano realizzare esperienze di crescita individuale e sociale. Partendo dal percorso scolastico si mira al raggiungimento di una completa inclusione sociale e lavorativa della persona con disabilità, in quanto diritto fondamentale ed ineludibile di ciascun individuo.

Tale diritto è stato definitivamente riconosciuto dalla Legge 5 febbraio 1992, n. 104 - Legge-quadro per l’assistenza, l’integrazione sociale e i diritti delle persone handicappate - e successive modifiche con la quale è stato garantito il pieno rispetto della dignità umana e dei diritti di libertà e di autonomia della persona con disabilità al fine di promuoverne la piena integrazione nella famiglia, nella scuola, nel lavoro e nella società attraverso interventi volti a superare stati di emarginazione e di esclusione sociale.

Anche in ambito internazionale i diritti delle persone con disabilità sono riconosciuti dalla Convenzione ONU del 2006 che garantisce il diritto all’istruzione delle persone con disabilità senza discriminazioni e su base di pari opportunità, prevedendo un sistema di istruzione inclusivo a tutti i livelli ed un apprendimento continuo lungo tutto l’arco della vita. Tale Convenzione, ratificata dall’Italia con la legge 3 marzo 2009, n. 18, rappresenta il primo grande trattato sui diritti umani del nuovo millennio ed è un documento di grandissima importanza per la promozione di una nuova cultura riguardo alla condizione delle persone con disabilità e delle loro famiglie.

3. SERVIZIO DI TRASPORTO SCOLASTICO

Allo scopo di soddisfare in modo efficiente ed efficace le esigenze territoriali e garantire la continuità degli interventi ai soggetti destinatari, la Regione individua i Comuni quali enti gestori del servizio di trasporto in favore degli studenti con disabilità frequentanti le scuole del II ciclo.

3.1 Finalità del servizio

Le presenti Linee guida, nel dettare criteri e procedure operative da seguire nella realizzazione degli interventi di trasporto in favore degli studenti con disabilità frequentanti le scuole del II ciclo, hanno come obiettivo la creazione di una rete di collaborazione tra enti territoriali finalizzata a garantire ad ogni studente con disabilità il raggiungimento della propria sede scolastica.

3.2 Tipologia del servizio

Il servizio consiste nell'organizzazione del trasporto scolastico degli studenti con disabilità frequentanti le scuole del II ciclo in ambito urbano e interurbano, anche con mezzi privati. Per gli studenti con disabilità certificata ai sensi dell'art. 3, comma 3 della Legge n. 104/1992 il servizio dovrà prevedere mezzi di trasporto attrezzati con personale specializzato.

3.3 Destinatari del servizio

Sono destinatari del servizio di trasporto sopra descritto gli studenti con disabilità certificata residenti nei Comuni della Regione Lazio che frequentano le Istituzioni Scolastiche statali o paritarie o i Percorsi triennali finalizzati all'assolvimento del diritto dovere nell'istruzione e formazione professionale ai sensi dell'art. 28 del Decreto legislativo n. 226/2005. La persona con disabilità è colui che presenta minorazioni fisiche, mentali, intellettuali o sensoriali stabilizzate o progressive che in interazione con varie barriere possono impedirne la piena ed effettiva partecipazione alla società su una base di eguaglianza con gli altri e causare difficoltà di apprendimento, di relazione o di integrazione tali da determinare un processo di svantaggio e di emarginazione. Lo studente dovrà essere in possesso della certificazione di disabilità e di diagnosi funzionale rilasciata dalla ASL competente (verbale di accertamento dell'handicap ex Legge n. 104/1992 in corso di validità). Si specifica, inoltre, che: a) gli alunni ultra diciottenni che devono iscriversi al 1° anno di scuola superiore nell'ambito dei percorsi di II livello presso i CPIA (ex corsi serali) godono di tutti i diritti previsti per gli alunni con disabilità frequentanti le scuole superiori del mattino e quindi anche del servizio di trasporto scolastico; b) gli alunni ultra diciottenni che hanno già frequentato interamente un corso di istruzione secondaria superiore (sia pure di diversa tipologia) e siano in possesso del correlato titolo di studio non possono usufruire del servizio di trasporto sulla base delle presenti linee guida il cui quadro di riferimento normativo afferisce alla garanzia del diritto allo studio, realizzato con il conseguimento del titolo. I Comuni, nell'esercizio, della propria autonomia potranno individuare ulteriori requisiti per accedere al servizio.

4. MODALITA' OPERATIVE PER I COMUNI

I Comuni di residenza provvederanno a raccogliere le domande delle famiglie predisponendo apposita modulistica e definendo, nell'esercizio della propria autonomia, ulteriori requisiti, modi e tempi per accedere al servizio.

In ogni caso il servizio di trasporto dovrà rispettare le seguenti condizioni:

- su richiesta della famiglia potrà essere erogato, nei periodi di lezione previsti dal calendario scolastico regionale, in forma completa (andata e ritorno dello studente) o parziale (solo andata, solo ritorno, solo in alcuni giorni, solo in alcuni periodi dell'anno scolastico);
- verrà garantito anche nei giorni in cui è previsto lo svolgimento degli esami di Stato o di qualifica;
- di norma coprirà il tragitto dall'indirizzo di residenza dell'alunno alla sede dell'Istituto Scolastico e viceversa salvo particolari richieste che il Comune si riserverà di valutare;
- per gli studenti con disabilità certificata ai sensi dell'art. 3, comma 3, della Legge n.104/1992 dovrà prevedere mezzi di trasporto attrezzati con personale specializzato.

I Comuni potranno organizzare il servizio direttamente (in forma singola o associata) o attraverso l'affidamento a soggetti terzi.

In alternativa i Comuni potranno decidere di gestire il servizio attraverso la concessione di contributi economici forfettari alle famiglie degli utenti da calcolare su base chilometrica e **in funzione del numero dei giorni di presenza a scuola certificati dall'istituto di riferimento.**

I Comuni dovranno garantire l'espletamento del servizio nell'intero ambito territoriale di loro competenza non potendo circoscriverlo ad ambiti territoriali di ampiezza subcomunale (municipi, frazioni, ecc.).

5. RISORSE FINANZIARIE DISPONIBILI

La Regione eroga ai Comuni un contributo per l'organizzazione del servizio di trasporto scolastico degli studenti con disabilità residenti nella Regione Lazio e frequentanti le scuole secondarie di secondo grado. A questo scopo stanZIA risorse pari a 1.800.000,00 euro a valere sul capitolo U0000F11900 Missione 04, Programma 07, Piano dei conti finanziario 1.04.01.02.000 – di cui euro 900.000,00 per l'esercizio finanziario 2024 e euro 900.000,00 per l'esercizio finanziario 2025.

5.1 Criteri, modalità e tempistiche di assegnazione del contributo

Il valore del contributo regionale per ciascuno studente disabile potrà coprire, di norma, un massimo di 30 chilometri complessivi tra andata e ritorno dello studente per ogni giornata di frequenza e comunque non potrà essere superiore all'importo di euro 3.000,00 annui per utente. Tale stima è effettuata calcolando una spesa media di 0,50 euro al chilometro.

Si precisa che in caso di interventi di trasporto estremamente complessi e onerosi a causa di situazioni territoriali di particolare isolamento e/o della gravità della disabilità certificata (art. 3, comma 3, della Legge n.104/1992) verrà valutata la possibilità di erogare un contributo specifico nei limiti della disponibilità delle risorse.

I Comuni provvederanno alla raccolta e alla valutazione delle richieste, alla compilazione dell'elenco degli aventi diritto e all'attivazione del servizio.

Per accedere al contributo regionale i Comuni dovranno trasmettere all'indirizzo di posta elettronica certificata programmazione.istruzione@pec.regione.lazio.it **entro e non oltre il 31 luglio 2024** una nota riepilogativa con l'indicazione del numero degli utenti assistiti specificando per ciascuno il numero complessivo dei chilometri percorsi giornalmente e se si tratta di studente con disabilità grave (certificata ai sensi dell'art. 3, comma 3, della Legge n.104/1992). **La nota riepilogativa non dovrà contenere elementi di identificazione personale e altri dati sensibili in quanto non necessari ai fini della quantificazione del contributo.**

Nel corso della procedura di raccolta delle domande di attivazione del servizio e di trasmissione della nota riepilogativa all'Amministrazione regionale, i Comuni agiranno in qualità di "Responsabili del trattamento dei dati" in conformità all'art. 28 del Regolamento generale sulla protezione dei dati – RGPD. I Comuni, pertanto, sono tenuti a sottoscrivere l'"Atto di nomina a Responsabile del trattamento dei dati personali" di cui al successivo Allegato B e a trasmetterlo all'indirizzo di posta elettronica certificata programmazione.istruzione@pec.regione.lazio.it **entro e non oltre il 31 luglio 2024** insieme con la nota riepilogativa.

I Comuni che non trasmetteranno la documentazione sopra descritta entro il termine stabilito non potranno accedere al contributo regionale.

La Regione entro il termine di 90 giorni dall'inizio dell'anno scolastico provvederà ad adottare il piano di riparto delle risorse tra i singoli Comuni e ad impegnare e a liquidare una prima quota pari al 50% del contributo totale assegnato. In questa fase l'importo del contributo potrà essere rideterminato rispetto ai parametri di calcolo sopra indicati in base alla stima effettiva della spesa comunicata dai Comuni in rapporto alle risorse regionali disponibili.

La restante quota del contributo - nei limiti delle spese sostenute e sino all'importo massimo riconoscibile - verrà erogata a saldo previa presentazione **entro e non oltre il 29 agosto 2025** di una relazione di rendicontazione finale contenente tutte le specifiche dei singoli interventi realizzati.

N.B.: nella relazione di rendicontazione dovranno essere indicati necessariamente i giorni di effettiva frequenza scolastica degli alunni che hanno usufruito del servizio di trasporto su attestazione della scuola di riferimento che il Comune avrà cura di acquisire.

5.2 Adempimenti dei Comuni

Si ribadiscono a titolo riepilogativo i principali adempimenti dei Comuni:

- acquisizione delle domande e attivazione del servizio di trasporto entro l'inizio dell'anno scolastico;
- trasmissione all'indirizzo PEC programmazione.istruzione@regione.lazio.legalmail.it **entro e non oltre il 31 luglio 2024** della nota riepilogativa con l'indicazione del numero degli utenti assistiti specificando per ciascuno il numero complessivo dei chilometri percorsi giornalmente e se si tratta di studente con disabilità grave (certificata ai sensi dell'art. 3, comma 3, della Legge n.104/1992);
- trasmissione all'indirizzo PEC programmazione.istruzione@pec.regione.lazio.it **entro e non oltre il 31 luglio 2024** (insieme alla nota riepilogativa) dell'Atto di nomina a Responsabile del trattamento dei dati personali debitamente compilato e sottoscritto;
- acquisizione per ogni utente dell'attestazione dei giorni di effettiva frequenza scolastica da parte dell'istituto di riferimento al termine dell'anno scolastico;
- presentazione **entro e non oltre il 29 agosto 2025** di una relazione di rendicontazione finale giustificativa contenente tutte le specifiche dei singoli interventi realizzati.

I Comuni saranno tenuti a conservare la documentazione giustificativa del servizio erogato ed i relativi atti contabili al fine consentire verifiche - anche a campione - che la Regione Lazio potrà eventualmente disporre.

I contributi inutilizzati in tutto o in parte dovranno essere restituiti alla Regione Lazio.

Allegato B

**LINEE GUIDA PER LO SVOLGIMENTO DEL SERVIZIO DI TRASPORTO SCOLASTICO
DEGLI STUDENTI CON DISABILITÀ RESIDENTI NELLA REGIONE LAZIO E
FREQUENTANTI LE ISTITUZIONI SCOLASTICHE SECONDARIE DI II GRADO STATALI
O PARITARIE O I PERCORSI TRIENNALI DI IeFP**

ANNO SCOLASTICO 2024/25

ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

Copia

La nomina sottostante va compilata secondo le seguenti indicazioni:

- in azzurro le parti che vanno compilate da parte del Responsabile del trattamento;
- in grigio le parti da attenzionare.

SCHEMA G
(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 B ALLA DETERMINAZIONE REGIONALE N. _____ DEL _____

TRA

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

E

Il Comune di <indicare la denominazione del Comune _____>, (di seguito, per brevità, anche il Responsabile o il Responsabile del trattamento) con sede in _____ nella persona del Legale Rappresentante _____;

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 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 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 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 al fine di garantire il servizio di trasporto scolastico agli studenti con disabilità del II ciclo residenti nella Regione Lazio implicano da parte del Comune di **<indicare la denominazione del Comune >**, il trattamento dei dati personali di cui è Titolare la Giunta Regionale Lazio, ai sensi di quanto previsto dal Regolamento (UE) 2016/679;

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

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

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

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

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

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

RITENUTO che, ai sensi dell'articolo 28, paragrafo 1 del RGPD il Comune di **<indicare la denominazione del Comune >** 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 Comune di **<indicare la denominazione del Comune _____>**, 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 - *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 (l'elenco dei sub-sub responsabili deve essere indicato nell'allegato IV). 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 de 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

- a) 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:
 - 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 (art. 4, punto 1 RGPD): Nome, Cognome, indirizzo, numero del documento di identità, dati relativi all'istruzione (indirizzo della scuola frequentata), dati di contatto, informazioni demografiche (sesso, età, nazionalità)
 - dati bancari e finanziari (quali il numero di conto corrente e/o il codice IBAN)
 - dati personali sensibili (art. 9 del RGPD) stato di salute e di disabilità ex legge 104 degli allievi
 - le categorie di interessati sono indicate nell'allegato II;
- 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 e, in particolare, di:
- 1) designare come amministratore di sistema, con le modalità previste dal provvedimento del 27 novembre 2008, le persone fisiche autorizzate ad accedere in modo privilegiato, ai sensi dello stesso provvedimento, ai dati personali del cui trattamento la Giunta regionale del Lazio è titolare;
 - 2) conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte all'interno del Comune, 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 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@pec.regione.lazio.it e dpo@pec.regione.lazio.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

Firma digitale del Direttore regionale

Il Responsabile del trattamento

Firma digitale Dirigente/Legale Rappresentante

Copia

ALLEGATO I - ELENCO DELLE PARTI

Titolare del trattamento:

Giunta Regionale del Lazio
Sede: Via R. Raimondi Garibaldi 7– 00147 Roma,
nella persona dell'Avv. Elisabetta Longo, Direttrice della Direzione Regionale Istruzione, Formazione e Politiche per l'Occupazione

Dati di contatto del Responsabile della Protezione dei Dati personali (DPO): **dpo@pec.regione.lazio.it**

Data

Il Titolare del trattamento

Firma digitale del Direttore regionale

Responsabile del trattamento:

Sede legale:
via, n.
CAP, località, Provincia Tel. (+39) ## PEC: _____

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

Nome, qualifica e dati di contatto del referente: _____

CONTESTO DI RIFERIMENTO

La Regione Lazio con determinazione regionale n..... del..... al fine di garantire il servizio di trasporto scolastico agli studenti con disabilità del II ciclo residenti nella Regione Lazio ha definito i rapporti fra le parti.

ALLEGATO II - DESCRIZIONE DEL TRATTAMENTO –

Il trattamento, su larga scala, riguarda le attività relative all' erogazione dei contributi per lo svolgimento del servizio di trasporto scolastico destinato agli alunni con disabilità residenti nella Regione Lazio e frequentanti le Istituzioni Scolastiche di II grado statali o paritarie e i percorsi triennali di IeFP.

L'Area predispone annualmente le Linee Guida indirizzate ai Comuni che prevedono i criteri per l'organizzazione del servizio ed il calcolo del contributo.

In base a tale provvedimento la Regione affida ai Comuni i seguenti compiti:

- la raccolta delle domande degli studenti residenti nel proprio territorio;
- la valutazione formale della loro ammissibilità;
- la trasmissione degli elenchi delle domande ammissibili alla Direzione Regionale competente in materia tramite PEC in modalità riservata.

In base al numero di domande presentate l'Area predispone la ripartizione delle risorse tra i comuni richiedenti.

Categorie di interessati i cui dati personali sono trattati

- Alunni con disabilità residenti nella Regione Lazio e frequentanti una scuola secondaria di secondo grado o un centro di formazione professionale.

Categorie di dati personali trattati

Le tipologie di dati trattati sono:

Dati personali (art. 4, punto 1 RGPD): Nome, Cognome, indirizzo, numero del documento di identità, altri elementi identificativi, dati relativi all'istruzione (indirizzo della scuola frequentata), dati di contatto, informazioni demografiche (sesso, età, nazionalità) dati bancari e finanziari (quali il numero di conto corrente e/o il codice IBAN);

Dati personali sensibili (art. 9 del RGPD) stato di salute e di disabilità ex legge 104 degli allievi.

Natura del trattamento

Tutti i dati personali comunicati dai soggetti interessati come sopra specificati, acquisiti nel rispetto delle disposizioni legislative vigenti e connessi allo svolgimento delle funzioni istituzionali, sono trattati dal Titolare del trattamento e dai Responsabili del trattamento per l'esecuzione di compiti di interesse pubblico (art. 6 co 1 lettera e).

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

Finalità amministrative relative al procedimento di erogazione del servizio di trasporto scolastico degli studenti con disabilità del secondo ciclo.

Durata del trattamento

Salva la necessità di conservazione ulteriore in caso di contenzioso legale ed esigenze difensive, i dati saranno conservati ai sensi di leggi specifiche in materia di conservazione di atti e documenti amministrativi e/o in materia di finanziamenti pubblici e per il tempo necessario al conseguimento delle finalità del trattamento, salvo richiesta di cancellazione, nel rispetto di obblighi legali ed amministrativi e nel rispetto del principio di minimizzazione di cui all'art. 5 del RGPD e comunque non oltre il termine di 5 anni dall'ultimo atto o comunicazione inerente al procedimento stesso.

Sub-responsabili

Nel caso di trattamento da parte di sub-responsabili del trattamento, vanno specificate anche le materie disciplinate, la natura e la durata del trattamento:

Copia

ALLEGATO III
MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE
LA SICUREZZA DEI TRATTAMENTI E DEI DATI

Descrivere le misure di sicurezza tecniche e organizzative messe in atto dal responsabile del trattamento o dai responsabili (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 tecniche e organizzative devono essere descritte in modo concreto e non genericamente.

Le misure applicate al trattamento sono:

Barrare in caso di applicazione della misura	MISURA
<input type="checkbox"/>	designazione degli incaricati
<input type="checkbox"/>	tenuta del registro delle attività di trattamento
<input type="checkbox"/>	misure di cifratura dei dati personali
<input type="checkbox"/>	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
<input type="checkbox"/>	misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
<input type="checkbox"/>	procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento
<input type="checkbox"/>	misure di identificazione e autorizzazione dell'utente
<input type="checkbox"/>	misure di protezione dei dati durante la trasmissione
<input type="checkbox"/>	misure di protezione dei dati durante la conservazione
<input type="checkbox"/>	misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati
<input type="checkbox"/>	misure per garantire la registrazione degli eventi
<input type="checkbox"/>	misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita
<input type="checkbox"/>	misure di informatica interna e di gestione e governance della sicurezza informatica
<input type="checkbox"/>	misure di certificazione/garanzia di processi e prodotti
<input type="checkbox"/>	misure per garantire la minimizzazione dei dati
<input type="checkbox"/>	misure per garantire la qualità dei dati
<input type="checkbox"/>	misure per garantire la conservazione limitata dei dati
<input type="checkbox"/>	misure per garantire la responsabilità

<input type="checkbox"/>	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:

Barrare in caso di applicazione della misura	MISURA
<input type="checkbox"/>	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
<input type="checkbox"/>	Separazione dei database e degli ambienti di sviluppo, test da quelli di produzione
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	Registrazione dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni mediante log management
<input type="checkbox"/>	Sottoposizione a log e riconducibilità alla singola persona delle attività degli amministratori, dei database e dei server
<input type="checkbox"/>	Utilizzo di un unico server NTP interno come riferimento per tutte le sincronizzazioni
<input type="checkbox"/>	Svolgimento delle attività di installazione e in generale di manutenzione solo da personale preventivamente formato, competenteed autorizzato
<input type="checkbox"/>	<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 eWPA2 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, appositosoftware 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. Infine, ci sono specifiche reti (vpn sistemistica e rete della control room) che sono le uniche a poter aver accesso alla rete digestione degli apparati. Tali apparati hanno una rete di management dedicata e fisicamente separata.</p>

<input type="checkbox"/>	Le reti interne al datacenter sono protette da firewall perimetrale. Inoltre, è previsto un firewall interno al datacenter per la segregazione delle reti interne.
<input type="checkbox"/>	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.
<input type="checkbox"/>	Tutte le comunicazioni tramite posta elettronica si basano sulla sicurezza data dal server di posta, le comunicazioni in rete (nei casi ritenuti necessari) avvengono in https. Quando necessario scambiare file si usano canali sicuri in STFP
<input type="checkbox"/>	Le informazioni coinvolte nelle trasmissioni dei servizi applicativi sono protette mediante l'utilizzo di canali sicuri (firewall, VPN), e mediante certificato o cifratura
<input type="checkbox"/>	Gli ambienti di test applicativi, gestiti direttamente dai gruppi di progetti che ne sono responsabili, non contengono mai dati reali, ma solo dati fittizi
<input type="checkbox"/>	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
<input type="checkbox"/>	Le operazioni di amministrazione remota sui server sono eseguite con protocolli sicuri ad esempio SSH ed RDP
<input type="checkbox"/>	Eventuali eventi di cambiamento della configurazione e dei permessi di sicurezza del sistema sono inviati al SIEM
<input type="checkbox"/>	Le credenziali di amministratore di dominio sono conservate in un wallet protetto da password
<input type="checkbox"/>	Per i messaggi di posta è attivo il servizio antispam di Microsoft in Cloud (EOP)
<input type="checkbox"/>	Impostazione della scadenza delle password su base trimestrale su tutti gli account con inibizione globale della possibilità di non far scadere le password.
<input type="checkbox"/>	Definizione interna dei processi di gestione delle password impostate su account impersonali o di servizio, al fine di favorirne un'opportuna rotazione periodica. 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.
<input type="checkbox"/>	Previsione di elevati requisiti di complessità delle password su tutti gli account, quali: requisito di lunghezza minima di 8 caratteri
<input type="checkbox"/>	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
<input type="checkbox"/>	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.
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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)
<input type="checkbox"/>	Aggiornamento, all'occorrenza, dei sistemi operativi risultanti in stato end of life o end of support.

<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	Utilizzo di apparati "Next generation Firewall" periferici, segregazione dei siti, attivazione dei moduli IDS/IPS
<input type="checkbox"/>	Utilizzo di politiche restrittive sulla navigazione in internet degli utenti, favorendo il principio del privilegio minimo
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	Utilizzo di un servizio di Security Awareness & Training finalizzato all'educazione degli utenti in ambito Cyber Security
<input type="checkbox"/>	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.
<input type="checkbox"/>	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).
<input type="checkbox"/>	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**

Inserire gli eventuali sub-responsabili individuati

Ragione sociale del sub-responsabile: _____

Sub-trattamento delegato: _____

Copia

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, il Comune di _____, 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;
- 3) assicurare la completa distinzione tra utenze privilegiate e non privilegiate di amministratore, alle quali devono corrispondere credenziali diverse;
- 4) 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;
- 5) 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;
- 6) 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;

- 7) 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;
- 8) 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;
- 9) 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;
- 10) 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;
- 11) 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;
- 12) 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 allo 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.”.

Copia

Allegato C
INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI
ai sensi dell'art. 13 del Regolamento (UE) 2016/679

Trasporto scolastico degli studenti con disabilità del II ciclo

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 agli utenti che accedono e usufruiscono del servizio di trasporto scolastico degli studenti con disabilità residenti nella Regione Lazio e frequentanti le Istituzioni Scolastiche secondarie di II grado statali o paritarie o i Percorsi triennali di IeFP.

Il trattamento riguarda le attività relative all'acquisizione e successiva valutazione delle domande finalizzate a consentire agli interessati di accedere al servizio di trasporto scolastico degli studenti con disabilità residenti nella Regione Lazio e frequentanti le Istituzioni Scolastiche secondarie di II grado statali o paritarie o i Percorsi triennali di IeFP per l'anno scolastico 2024/25.




I Comuni di residenza degli interessati (nominati responsabili del trattamento) acquisiscono e valutano le domande degli interessati. Gli stessi Comuni trasmettono all'Area uno schema riepilogativo delle domande acquisite (privo dell'indicazione di dati personali), in base a tale schema l'Area procede al calcolo del contributo complessivo necessario a ciascun Comune per organizzare e gestire il servizio di trasporto e all'adozione del conseguente provvedimento di assegnazione delle risorse.


Il trattamento dei dati personali degli utenti per le finalità istituzionali connesse alla gestione degli adempimenti inerenti al presente provvedimento rispetta i principi di correttezza, liceità, trasparenza e riservatezza e le disposizioni europee e nazionali in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679 (di seguito Regolamento o RGPD) e al Decreto legislativo 30 giugno 2003, n. 196 in versione vigente (c.d. Codice in materia di protezione dei dati personali) il cui obiettivo è quello di proteggere i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

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 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 style="text-align: center;">CATEGORIE DI DATI PERSONALI TRATTATI</p> <ul style="list-style-type: none"> • Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale) • Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile) • Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...) • Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente,

	<p>CNS, altro...)</p> <ul style="list-style-type: none"> Dati relativi alla salute 						
	<table border="1"> <thead> <tr> <th colspan="2" data-bbox="350 321 1565 363">FINALITÀ E BASE GIURIDICA DEL TRATTAMENTO</th> </tr> <tr> <th data-bbox="350 363 954 405">FINALITÀ</th> <th data-bbox="954 363 1565 405">BASE GIURIDICA</th> </tr> </thead> <tbody> <tr> <td data-bbox="350 405 954 989"> <p>Consentire ai Soggetti interessati di accedere al servizio di trasporto scolastico degli studenti con disabilità residenti nella Regione Lazio e frequentanti le Istituzioni Scolastiche secondarie di II grado statali o paritarie o i Percorsi triennali di IeFP e, allo scopo, svolgere le necessarie attività amministrative volte alla valutazione dell'ammissibilità delle domande presentate; a provvedere a tutte le comunicazioni inerenti alle attività previste dal provvedimento; a fornire riscontro alle richieste di informazioni inerenti alle attività previste dal provvedimento e ad effettuare i doverosi controlli prescritti dalla legge, con particolare riferimento alla veridicità delle Dichiarazioni Sostitutive ai sensi del DPR n. 445/2000.</p> </td> <td data-bbox="954 405 1565 989"> <ol style="list-style-type: none"> condizione di liceità del trattamento: <ul style="list-style-type: none"> art 6 lett. c) ed e) e par. 3, lett. b) del Regolamento UE 2016/679 base giuridica: <ul style="list-style-type: none"> Legge 5 febbraio 1992, n. 104; Legge 3 marzo 2009, n. 18; Legge 10 marzo 2000, n. 62; Legge 13 luglio 2015, n. 107; Decreto Legislativo 13 aprile 2017, n. 66; Determinazione di riferimento </td> </tr> </tbody> </table>	FINALITÀ E BASE GIURIDICA DEL TRATTAMENTO		FINALITÀ	BASE GIURIDICA	<p>Consentire ai Soggetti interessati di accedere al servizio di trasporto scolastico degli studenti con disabilità residenti nella Regione Lazio e frequentanti le Istituzioni Scolastiche secondarie di II grado statali o paritarie o i Percorsi triennali di IeFP e, allo scopo, svolgere le necessarie attività amministrative volte alla valutazione dell'ammissibilità delle domande presentate; a provvedere a tutte le comunicazioni inerenti alle attività previste dal provvedimento; a fornire riscontro alle richieste di informazioni inerenti alle attività previste dal provvedimento e ad effettuare i doverosi controlli prescritti dalla legge, con particolare riferimento alla veridicità delle Dichiarazioni Sostitutive ai sensi del DPR n. 445/2000.</p>	<ol style="list-style-type: none"> condizione di liceità del trattamento: <ul style="list-style-type: none"> art 6 lett. c) ed e) e par. 3, lett. b) del Regolamento UE 2016/679 base giuridica: <ul style="list-style-type: none"> Legge 5 febbraio 1992, n. 104; Legge 3 marzo 2009, n. 18; Legge 10 marzo 2000, n. 62; Legge 13 luglio 2015, n. 107; Decreto Legislativo 13 aprile 2017, n. 66; Determinazione di riferimento
FINALITÀ E BASE GIURIDICA DEL TRATTAMENTO							
FINALITÀ	BASE GIURIDICA						
<p>Consentire ai Soggetti interessati di accedere al servizio di trasporto scolastico degli studenti con disabilità residenti nella Regione Lazio e frequentanti le Istituzioni Scolastiche secondarie di II grado statali o paritarie o i Percorsi triennali di IeFP e, allo scopo, svolgere le necessarie attività amministrative volte alla valutazione dell'ammissibilità delle domande presentate; a provvedere a tutte le comunicazioni inerenti alle attività previste dal provvedimento; a fornire riscontro alle richieste di informazioni inerenti alle attività previste dal provvedimento e ad effettuare i doverosi controlli prescritti dalla legge, con particolare riferimento alla veridicità delle Dichiarazioni Sostitutive ai sensi del DPR n. 445/2000.</p>	<ol style="list-style-type: none"> condizione di liceità del trattamento: <ul style="list-style-type: none"> art 6 lett. c) ed e) e par. 3, lett. b) del Regolamento UE 2016/679 base giuridica: <ul style="list-style-type: none"> Legge 5 febbraio 1992, n. 104; Legge 3 marzo 2009, n. 18; Legge 10 marzo 2000, n. 62; Legge 13 luglio 2015, n. 107; Decreto Legislativo 13 aprile 2017, n. 66; Determinazione di riferimento 						
	<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 per la finalità sopra indicata, sono conservati ai sensi di leggi specifiche in materia di conservazione di atti e documenti amministrativi e/o in materia di finanziamenti pubblici e per il tempo necessario al conseguimento e all'espletamento di tutte le attività connesse alla realizzazione dell'intervento di cui al presente Avviso, salvo richiesta di cancellazione, nel rispetto di obblighi legali ed amministrativi e nel rispetto del principio di minimizzazione di cui all'art. 5 del GDPR e comunque non oltre il termine di 5 anni dall'ultimo atto o comunicazione inerente al procedimento stesso.</p> <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, 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 suoi dati personali sono:</p> <ul style="list-style-type: none"> Responsabili del trattamento: Comuni di residenza degli interessati, 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. 						

	<p>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) a mettere in atto misure tecniche e organizzative adeguate alla 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 (dirigenti e dipendenti) 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>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 AL DI FUORI DELL'UNIONE EUROPEA</p> <p>Non è intenzione del Titolare trasferire i suoi dati personali verso Paesi terzi (extra UE) o organizzazioni internazionali che possano pregiudicare il livello di protezione delle persone fisiche garantito dal GDPR.</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>

In persona della Direttore della Direzione Regionale "Istruzione, Formazione e Politiche per l'Occupazione"
Soggetto Designato al trattamento dal Titolare

[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."

Allegato D

QUESTIONARIO PER LA VERIFICA DEL RISPETTO DEL REGOLAMENTO (UE) 2016/679 "REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI" SULLE ATTIVITA' DI TRATTAMENTO DA PARTE DEL RESPONSABILE DEL TRATTAMENTO

A	ASPETTI GENERALI	SI	NO	N/A
A1	Sono state/sono effettuate le operazioni di trattamento nel rispetto delle disposizioni operative del Titolare?			
A2	Sono stati/sono effettuati trattamenti su dati personali diversi rispetto a quelli normalmente eseguiti nell'ambito della designazione?			
A2.1	In caso di risposta affermativa alla domanda A2, si è provveduto, all'insorgere dell'esigenza, ad informare preventivamente il Titolare del trattamento e il RPD della Regione Lazio?			
A3	Sono stati/sono effettuati trattamenti su dati personali diversi rispetto a quelli normalmente eseguiti nell'ambito della designazione?			
B	REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO	SI	NO	N/A
B1	E' stato presidposto il registro delle attività di trattamento svolte per conto del Titolare, in forma scritta, anche in formato elettronico, da esibire in caso di verifiche e/o ispezioni del Titolare o dell'Autorità?			
B2	Il Registro contiene le seguenti informazioni:			
B2.1	il nome e i dati di contatto del responsabile o dei responsabili del trattamento, del titolare del trattamento per conto del quale agisce il responsabile del trattamento e, ove nominato, del RPD			
B2.2	le categorie/attività dei trattamenti effettuati			
B2.3	i trasferimenti di dati personali verso Paesi terzi o organizzazioni al di fuori dello Spazio Economico Europeo, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del RGPD, la documentazione delle garanzie adeguate;			
B2.4	ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.			
B3	Il Registro viene regolarmente aggiornato?			
C	RPD DEL RESPONSABILE DEL TRATTAMENTO	SI	NO	N/A
C1	E' stato designato un RPD?			
C2	In caso di risposta affermativa:			
C2.1	Il RPD è stato designato con atto formale?			
C2.3	I dati ed i punti di contatto del RPD sono stati comunicati al Titolare?			
D	SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI	SI	NO	N/A
D1	Sono stati designati soggetti autorizzati al trattamento dati all'interno della struttura?			
D2	In caso di risposta affermativa alla domanda D1:			
D2.1	sono stati autorizzati con atto formale?			
D2.2	sono stati adeguatamente istruiti sul tema della protezione dei dati personali?			
D2.3	sono previste attività formative con aggiornamenti periodici in tema di protezione di dati personali?			
D2.4	le istruzioni operative impartite ai soggetti autorizzati sono idonee a garantire il rispetto delle finalità per cui i dati sono stati raccolti e trattati?			
D2.5	i soggetti autorizzati al trattamento sono vincolati ad un obbligo, legalmente assunto, di riservatezza?			
D3	Alcune attività vengono svolte in modalità di "lavoro agile"?			
D4	Il "lavoro agile" è disciplinato da regolamenti e/o procedure interne?			
E	AMMINISTRATORI DI SISTEMA	SI	NO	N/A
E1	Sono stati individuati i soggetti ai quali affidare il ruolo di Amministratori di Sistema (<i>System Administrator</i>), Amministratori di Base Dati (<i>Database Administrator</i>), Amministratori di Rete (<i>Network Administrator</i>) e/o Amministratori di <i>Software</i> complessi?			
E2	In caso di risposta affermativa alla domanda E1:			
E2.1	Sono stati sottoscritti appositi atti di designazione individuale?			
E2.2	Sono state impartite adeguate istruzioni ai designati secondo i ruoli assegnati?			
E2.3	Sono state adottate adeguate misure di controllo e di vigilanza sul loro operato?			
E2.4	E' stato aggiornato l'elenco degli ADS con l'indicazione delle relative utenze?			
E2.5	Le nomine degli Amministratori sono aggiornate ad ogni modifica della normativa vigente?			
E3	È stata assegnata ai suddetti soggetti una <i>user id</i> agevolmente riconducibile all'identità degli Amministratori?			
E4	In caso di risposta affermativa alla domanda E3 sono rispettate le seguenti regole?			
E4.1	divieto di assegnazione di <i>user id</i> generiche e già attribuite anche in tempi diversi;			
E4.2	utilizzo di utenze amministrative anonime, quali " <i>root</i> " di <i>Unix</i> o " <i>Administrator</i> " di <i>Windows</i> , solo per situazioni di emergenza;			
E4.3	le credenziali utilizzate assicurano sempre l'imputabilità delle operazioni a chi ne fa uso;			
E4.4	disattivazione delle <i>user id</i> attribuite agli Amministratori che, per qualunque motivo, non necessitano più di accedere ai dati.			
E5	Le password associate alle <i>user id</i> assegnate agli Amministratori prevedono il rispetto delle seguenti regole?			
E5.1	<i>password</i> con lunghezza minima di almeno 14 caratteri, qualora l'autenticazione a più fattori non sia supportata;			
E5.2	cambio <i>password</i> alla prima connessione e successivamente almeno ogni 30 giorni (<i>password again</i>);			

E5.3	le <i>password</i> devono differire dalle ultime 5 utilizzate (<i>password history</i>);			
E5.4	le <i>password</i> sono conservate in modo da garantirne disponibilità e riservatezza;			
E5.5	registrazione di tutte le immissioni errate di <i>password</i> ;			
E6	Gli <i>account</i> degli Amministratori sono bloccati dopo un numero massimo di tentativi falliti di <i>login</i> , ove tecnicamente possibile?			
E7	L'archiviazione di <i>password</i> o codici PIN, su qualsiasi supporto fisico avvenga, è protetta da sistemi di cifratura?			
E8	È assicurata la completa distinzione, in capo al medesimo utente, tra utenze privilegiate (amministratore) e non privilegiate, alle quali devono corrispondere credenziali diverse?			
E9	I profili di accesso per le utenze di ADS rispettano il principio del <i>need-to-know</i> , ovvero che non siano attribuiti diritti oltre a quelli realmente necessari per eseguire le attività di lavoro?			
E10	I sistemi sono dotati di strumenti automatici tipo <i>alert</i> che si attivano ad esempio quando viene aggiunta una utenza amministrativa e/o quando sono aumentati i diritti di una utenza amministrativa già attiva?			
E11	Sono stati adottati sistemi di registrazione degli accessi logici (<i>log</i>) degli Amministratori ai sistemi?			
E12	La conservazione dei registri degli accessi logici è garantita per un periodo non inferiore a 6 mesi?			
E13	In caso di utilizzo di sistemi messi a disposizione dalla Regione, è stato comunicato agli Amministratori che la Regione stessa procederà alla registrazione e conservazione dei <i>log</i> ?			
E14	Sono state adottate idonee misure finalizzate ad obbligare l'Amministratore ad accedere ai sistemi con una utenza normale e solo successivamente eseguire i singoli comandi come ADS?			
E15	Sono stati comunicati al momento della sottoscrizione dell'atto di designazione e con cadenza almeno annuale o ogni qualvolta se ne verifichi la necessità alla Regione Lazio gli estremi identificativi dei soggetti nominati Amministratori di Sistema?			
E16	Sono state eseguite, con cadenza almeno annuale, le attività di verifica dell'operato degli ADS?			
E17	Sono state adottate idonee misure per consentire di mettere a disposizione del Titolare e del RPD della Regione Lazio le informazioni relative ai <i>log</i> delle operazioni per un periodo di 6 mesi, qualora necessario?			
F	PRIVACY BY DESIGN E BY DEFAULT	SI	NO	N/A
F1	Sono state adottate le politiche aziendali di protezione dati fin dalla progettazione (<i>privacy by design</i>)?			
F2	È stato adottato sistema di monitoraggio delle politiche aziendali di <i>privacy by design</i> e <i>by default</i> affinché le stesse possano adeguarsi ai mutamenti tecnologici e all'insorgere di nuovi rischi?			
F3	Sono state eseguite le valutazioni del rischio per ciascun trattamento?			
F4	Sono state strutturate le operazioni in modo da minimizzare il trattamento dei dati personali?			
F5	Sono state adottate tutte le misure necessarie per perseguire la massima trasparenza dei trattamenti di dati personali rendendo accessibile agli interessati idonea documentazione?			
G	MISURE DI SICUREZZA	SI	NO	N/A
G1	Sono stati definiti i ruoli e le responsabilità relativi al trattamento dei dati personali?			
G2	I soggetti di cui alla domanda G1 agiscono secondo procedure interne definite per la gestione degli adempimenti sulla protezione dei dati personali?			
G3	Sono state messe in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio?			
G4	In caso di risposta affermativa alla domanda G3, le misure adottate comprendono:			
G4.1	la pseudonimizzazione e/o la cifratura dei dati personali?			
G4.2	misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento?			
G4.3	misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico?			
G4.4	procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento?			
G5	Sono state predisposte misure tecniche che consentono l'accesso ai dati personali unicamente ai soggetti autorizzati?			
G6	Sono state adottate almeno le misure minime di sicurezza ICT per le PP.AA. di cui alla circolare AgID del 18 aprile 2017, n. 2/2017?			
G7	È stata predisposta idonea documentazione tecnica relativa alle misure di sicurezza in atto?			
G8	In caso di risposta affermativa alla domanda G7:			
G.8.1	la documentazione tecnica tiene traccia delle eventuali modifiche delle misure di sicurezza in atto?			
G.8.2	la documentazione è disponibile e producibile a richiesta del Titolare?			
G9	È stato adottato un approccio alla sicurezza dei dati basato sul rischio?			
G10	È presente un impianto antintrusione?			
G11	Sono presenti procedure di controllo per l'accesso dei visitatori?			
G12	È prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, associazioni ecc)?			
G13	Gli operatori autorizzati possono accedere ai dati trattati con strumenti informatici soltanto dopo almeno uno o due processi di autenticazione (ad esempio il primo accesso al sistema operativo e il secondo accesso all'applicativo specifico)?			
G14	Gli operatori autorizzati utilizzano credenziali di accesso individuali?			

G15	Gli operatori autorizzati utilizzano dispositivi personali (PC portatili, tablet, smartphone, etc) per il trattamento dei dati?			
G16	L'accesso ai collegamenti VPN avviene dopo l'autenticazione a due fattori di cui uno è OTP?			
G17	È presente una procedura interna, nel caso sia permesso ai soggetti incaricati l'utilizzo di risorse informatiche (es. PC, Tablet, smartphone) di proprietà di terzi?			
G18	I sistemi informativi sono gestiti in proprio?			
G19	In caso di risposta affermativa alla domanda G18:			
G19.1	è installato sui dispositivi un sistema antivirus e <i>antimalware</i> aggiornato?			
G19.2	sono conservati i dati in <i>tenant</i> diversi e separati per ciascun Titolare che li ha rispettivamente forniti?			
G19.3	è aggiornato costantemente il Sistema Operativo installato sugli elaboratori elettronici?			
G19.4	è prevista una mappatura del proprio sistema informatico (hardware, software, dati, procedure)?			
G19.5	è presente un Piano di Continuità Operativa?			
G19.6	è effettuato con cadenza temporale programmata un test sul Piano di Continuità Operativa?			
G19.7	è presente un Piano di <i>Disaster Recovery</i> ?			
G19.8	è effettuata con cadenza temporale programmata <i>penetration test</i> sul sistema di elaborazione dei dati?			
G19.9	è presente un impianto di videosorveglianza negli spazi dove sono collocati dispositivi di elaborazione e conservazione dei dati?			
G19.10	è presente un impianto antintrusione?			
G19.11	sono presenti delle procedure per l'accesso controllato dei visitatori?			
G19.12	sono presenti dei sistemi di valutazione interni delle misure di sicurezza?			
G19.13	sono presenti i sistemi a valutazione esterna (certificazione)?			
G19.14	sono stati adottati i sistemi di crittografia per proteggere i dati memorizzati?			
G19.15	sono stati adottati i sistemi di crittografia per proteggere i dati in transito?			
G19.16	è presente di un SOC?			
G19.17	è presente sistema SIEM?			
G19.18	è prevista una regolare formazione degli operatori sui temi dell'utilizzo sicuro del Sistema?			
G19.19	sono protette le connessioni ad Internet con sistemi di <i>firewall</i> , <i>intrusion detenction sistem</i> ecc.?			
G19.20	Sono in uso dispositivi (PC o Server) dotati di sistemi operativi obsoleti (ad esempio per ragioni tecniche o di compatibilità con sistemi <i>legacy</i>)?			
G19.21	nell'ambito di test di sviluppo del software, sono usati dati anonimizzati?			
G19.22	sono utilizzati ambienti di sviluppo software, test, collaudo e di produzione fisicamente e logicamente separati?			
G20	I sistemi utilizzati sono gestiti da terzi?			
G21	In caso di risposta affermativa alla domanda G20 si è certi che il soggetto terzo:			
G21.1	abbia installato sui dispositivi un sistema antivirus e <i>antimalware</i> aggiornato?			
G21.2	conservi i dati in <i>tenant</i> diversi e separati per ciascun Titolare che li ha rispettivamente forniti?			
G21.3	provveda ad aggiornare costantemente il Sistema Operativo installato sugli elaboratori elettronici?			
G21.4	disponga di una mappatura del proprio sistema informatico (hardware, software, dati, procedure)?			
G21.5	disponga di un Piano di Continuità Operativa?			
G21.6	effettui con cadenza temporale programmata test sul Piano di Continuità Operativa?			
G21.7	disponga di un Piano di Disaster Recovery?			
G21.8	effettui con cadenza temporale programmata <i>penetration test</i> sul sistema di elaborazione dei dati?			
G21.9	sia dotato di un impianto di videosorveglianza negli spazi dove sono collocati dispositivi di elaborazione e conservazione dei dati?			
G21.10	sia dotato di impianto antintrusione?			
G21.11	sia dotato di procedure per l'accesso controllato dei visitatori?			
G21.12	sia dotato di sistemi di valutazione interni delle misure di sicurezza?			
G21.13	sottoponga i sistemi a valutazione esterna (certificazione)?			
G21.14	abbia adottato sistemi di crittografia per proteggere i dati memorizzati?			
G21.15	abbia adottato sistemi di crittografia per proteggere i dati in transito?			
G21.16	sia dotato di un SOC?			
G21.17	sia dotato di un sistema SIEM?			
G21.18	proceda alla regolare formazione degli operatori sui temi dell'utilizzo sicuro del Sistema?			
G21.19	protegga le connessioni ad Internet con sistemi di <i>firewall</i> , <i>intrusion detenction sistem</i> ecc.?			
G21.20	non abbia in uso dispositivi (PC o Server) dotati di sistemi operativi obsoleti (ad esempio per ragioni tecniche o di compatibilità con sistemi <i>legacy</i>)?			
G21.21	nell'ambito di test di sviluppo del software, usi dati anonimizzati?			
G21.22	utilizzi ambienti di sviluppo software, test, collaudo e di produzione fisicamente e logicamente separati?			
H	PROCEDURE DI GESTIONE DEL SISTEMA INFORMATIVO AZIENDALE	SI	NO	N/A
H1	Esiste una procedura per la gestione e l'utilizzo del Sistema Informativo Aziendale?			
H2	In caso di risposta affermativa alla domanda H1:			
H2.1	è conforme a standard internazionali?			
H2.2	prevede regole per la gestione delle credenziali di accesso ai database?			
H2.3	prevede regole per la gestione delle password e per l'accesso alle applicazioni?			
H2.4	prevede regole per la gestione degli accessi ad Internet?			

H2.5	prevede regole per la gestione degli accessi a <i>social media</i> (es: <i>Facebook</i> , <i>You Tube</i> , <i>Twitter</i> ecc)?			
H2.6	prevede regole per la gestione e l'utilizzo della posta elettronica?			
H2.7	prevede regole per la gestione dei diritti di accesso ai dati?			
H2.8	prevede regole per la gestione degli incidenti informatici?			
H2.9	prevede regole per l'assistenza agli utenti?			
H2.10	prevede regole per la protezione antivirus?			
H2.11	prevede regole per la gestione dei dispositivi mobili utilizzati per il trattamento dei dati (PC portatili, smartphone, tablet, chiavi USB, dischi esterni di memorizzazione dei dati)?			
H2.12	prevede regole per autorizzare i dipendenti a trasferire, archiviare o trattare dati personali al di fuori dei locali dell'organizzazione?			
H2.13	prevede regole per il salvataggi di backup dei dati?			
H2.14	prevede regole per la gestione delle stampe protette?			
H2.15	prevede regole per la custodia e gestione degli archivi cartacei?			
I	DATA BREACH	SI	NO	N/A
I1	È stata adottata una procedura per la gestione delle violazioni di dati personali (<i>data breach</i>)?			
I2	Sono state predisposte misure organizzative idonee a garantire la tempestiva informazione al Titolare ed al RPD della Regione Lazio, (entro 24 ore dall'avvenuta conoscenza dell'evento), di ogni violazione di dati personali (<i>data breach</i>)?			
I3	Sono state adottate misure organizzative idonee a garantire che l'informazione sulla violazione dei dati personali (<i>data breach</i>), sia corredata da tutta la documentazione utile per permettere al Titolare la tempestiva valutazione sulla necessità di notifica di violazione all'Autorità Garante per la protezione dei dati personali e/o di comunicazione agli interessati, entro i termini stabiliti dal RGPD?			
I4	Sono stati subiti attacchi informatici con violazione di dati personali?			
I5	Sono stati notificati nell'ultimo anno violazioni di dati personali al Garante?			
L	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI	SI	NO	N/A
L1	Sono state adottate misure tecniche ed organizzative idonee a garantire adeguata assistenza al Titolare nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente a quanto prescritto dall'articolo 35 del RGPD, qualora lo stesso ne faccia richiesta?			
M	RICORSO AD ALTRO RESPONSABILE (di seguito SUB-RESPONSABILE)	SI	NO	N/A
M1	È stato effettuato ricorso ad altro/i responsabile/i (sub-responsabili) per gestire le attività di trattamento?			
M2	In caso di risposta affermativa alla domanda M1:			
M2.1	È stata rilasciata autorizzazione scritta, specifica o generale, del Titolare del Trattamento?			
M2.2	È stato informato il Titolare del trattamento di eventuali modifiche riguardanti l'aggiunta di altri sub-responsabili o la sostituzione sub-responsabili già nominati?			
M2.3	La nomina del sub-responsabile è avvenuta mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri contenente gli stessi obblighi in materia di protezione dei dati contenuti nel contratto (o in altro atto giuridico) tra il Titolare del trattamento e il Responsabile del trattamento?			
M2.4	Nel contratto (o altro atto giuridico) di nomina è stato previsto che il sub-responsabile fornisca sufficienti garanzie per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del RGPD?			
M2.5	Il sub-responsabile nominato detiene un registro con le medesime caratteristiche formali ed i medesimi contenuti sopra indicati relativamente ai trattamenti di competenza?			
M2.6	Nel contratto/altro atto giuridico sono state fornite adeguate istruzioni al sub-responsabile?			
M3	Sono effettuate periodiche verifiche sull'adeguatezza delle misure tecniche e organizzative adottate dal sub-responsabile?			
M4	Il sub-responsabile si attiene alla sua politica di sicurezza con particolare riferimento all'accesso ai dati dell'amministrazione?			
N	CANCELLAZIONE E/O RESTITUZIONE DEI DATI PERSONALI TRATTATI	SI	NO	N/A
N1	Sono state adottate misure tecniche ed organizzative idonee a garantire la cancellazione o la restituzione di tutti i dati personali nei termini stabiliti per la prestazione dei servizi o, comunque, a richiesta del Titolare?			
N2	È presente una procedura operativa per la dismissione dei supporti dei dati?			
N3	Sono presenti i dispositivi per la distruzione dei documenti cartacei?			
O	TRASFERIMENTO DI DATI PERSONALI VERSO UN PAESE TERZO O UN'ORGANIZZAZIONE INTERNAZIONALE	SI	NO	N/A
O1	Sono effettuati trasferimenti di dati personali verso Paesi terzi o organizzazioni al di fuori dello Spazio Economico Europeo?			
O2	In caso di risposta affermativa alla domanda O1:			
O2.1	è stata ottenuta l'autorizzazione scritta da parte del Titolare?			
O2.2	sono state adottate idonee misure per il rispetto del Capo V (artt. 44 - 50) del RGPD?			
P	CODICI DI CONDOTTA E CERTIFICAZIONI	SI	NO	N/A
P1	è prevista l'adesione a un codice di condotta ai sensi dell'art. 40 del RGPD?			
P2	Si è in possesso della certificazione ISO 9001?			
P3	Si è in possesso della certificazione ISO 27001?			

P4	è presente altra certificazione rilasciata da organismi di certificazione di cui all'articolo 43 del RGPD o dall'autorità di controllo, come previsto dall'art. 42 del RGPD, che dimostri la conformità al RGPD?			
Q	ESERCIZIO DEI DIRITTI DEGLI INTERESSATI	SI	NO	N/A
Q1	Sono state adottate procedure atte a consentire l'esercizio dei diritti degli interessati?			
Q2	In caso di risposta affermativa alla domanda Q1 sono previste procedure per:			
Q2.1	la limitazione del trattamento?			
Q2.2	la portabilità dei dati?			
Q2.3	la cancellazione dei dati su richiesta dell'interessato?			
Q2.4	la cancellazione dei dati al termine del periodo previsto?			
Q2.5	l'estrazione dei dati su richiesta dell'interessato?			
Q2.6	la rettifica dei dati?			
Q2.7	la gestione dell'opposizione al trattamento?			
Q3	Sono state adottate misure tecniche ed organizzative idonee ad assistere il Titolare nel dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui agli articoli da 15 a 22 del RGPD?			
Q4	Sono state ricevute istanze degli interessati in esercizio ai diritti di cui agli articoli da 15 a 22 del RGPD?			
Q5	In caso di risposta affermativa alla domanda Q4:			
Q5.1	è stata effettuata tempestiva comunicazione scritta al Titolare e al RPD della Regione Lazio, allegando copia della richiesta?			
Q5.2	è stato effettuato il coordinamento con il Titolare e con il RPD della Regione Lazio al fine di soddisfare le richieste?			
R	FUNZIONI CRITTOGRAFICHE - CONSERVAZIONE DELLE PASSWORD	SI	NO	N/A
R1	È utilizzato un sistema di autenticazione federato (es. LDAP, Spid, ecc.)?			
R2	In caso di risposta negativa alla domanda R1:			
R2.1	Sono state adottate le misure tecniche previste nelle <i>Linee Guida Funzioni Crittografiche – Conservazione delle Password</i> approvate con provvedimento del Garante registro n. 594 del 7 dicembre 2023 al fine di proteggere in modo efficace le password e conservarle nell'ambito di sistemi di autenticazione informatica, o di altri sistemi, secondo le istruzioni impartite dal Titolare?			
R3	In caso di risposta affermativa alla domanda R2.1:			
R3.1	Sono state adottate totalmente le misure tecniche previste?			
R3.2	Sono state adottate parzialmente le misure tecniche previste?			
R3.3	Sono state fornite idonee istruzioni agli Amministratori di sistema?			
R3.4	Sono state fornite idonee istruzioni ai sub-responsabili ove nominati?			
R3.5	In caso di affidamenti di nuovi servizi, è stato previsto previsto l'inserimento di apposite clausole nei capitolati tecnici di gara?			
R4	In caso di risposta negativa alla domanda R2.1:			
R4.1	Sono state comunicate la circostanze al Titolare del trattamento?			
R4.2	È possibile comprovare che le misure tecniche adottate garantiscano comunque un livello di sicurezza adeguato al rischio per i diritti e le libertà delle persone fisiche?			
R4.3	nel determinare il periodo di conservazione delle password, è previsto l'adeguato alle indicazioni sui criteri da utilizzare fornite dal Garante nel provvedimento registro n. 594 del 7 dicembre 2023?			
R4.4	le password sono tempestivamente cancellate, anche in modo automatico, laddove non siano più necessarie per verificare l'identità degli utenti ai fini dell'accesso a sistemi informatici o servizi online?			
R4.5	le password sono tempestivamente cancellate, anche in modo automatico, laddove non siano più necessarie per garantirne la sicurezza dei sistemi informatici o servizi online?			
R4.6	le password sono tempestivamente cancellate, anche in modo automatico in caso di cessazione dei sistemi informatici o servizi online?			
R4.7	le password sono tempestivamente cancellate, anche in modo automatico in caso di disattivazione delle relative credenziali di autenticazione?			
S	REQUISITI GENERALI DI SICUREZZA (Linee Guida Agid_Sicurezza nel procurement ICT)	SI	NO	N/A
S1	È effettuato annualmente un audit sul sistema di sicurezza da una società specializzata scelta previa approvazione della stazione appaltante?			
S2	Il personale che presta supporto operativo nella sicurezza, possiede le necessarie certificazioni?			
S3	Sono condivise le informazioni necessarie per il monitoraggio della qualità e della sicurezza?			
S4	In caso di risposta affermativa alla domanda S3:			
S4.1	Sono state pubblicate dette informazioni all'interno del portale della fornitura?			
S5	È stata sottoscritta una clausola di non divulgazione (NDA) relativa ai dati e alle informazioni dell'Amministrazione Appaltante?			
S6	Le soluzioni e i servizi di sicurezza proposti sono aggiornati da un punto di vista tecnologico?			
S7	Le soluzioni e i servizi di sicurezza proposti sono conformi alle normative e agli standard di riferimento?			
S8	Le soluzioni e i servizi di sicurezza proposti sono adattabili alle normative future senza oneri aggiuntivi?			
T	REQUISITI SPECIFICI PER FORNITURE DI SERVIZI DI SVILUPPO APPLICATIVO	SI	NO	N/A
T1	Sono effettuate forniture di servizi di sviluppo applicativo?			
T2	In caso di risposta affermativa alla domanda T1:			
T2.1	In fase di progettazione e codifica, sono implementate le specifiche di sicurezza nel codice e nella struttura della base dati, con particolare riferimento alle "Linee Guida per lo sviluppo del software sicuro" di AgID?			

T3	È stata rilasciata tutta la documentazione necessaria all'Amministrazione al termine del progetto, incluso quanto riguarda la sicurezza?			
U	REQUISITI SPECIFICI PER FORNITURE DI OGGETTI CONNESSI IN RETE	SI	NO	N/A
U1	Sono effettuate forniture di oggetti connessi in rete?			
U2	In caso di risposta affermativa alla domanda T1:			
U2.1	Sono utilizzati protocolli sicuri e cifrati (HTTPS,SSH v2, ecc.)?			
U2.2	È effettuato il filtraggio degli indirizzi IP?			
U2.3	Sono offerti processi, unità organizzative e strumenti dedicati alla gestione delle vulnerabilità scoperte sui prodotti oggetto della fornitura?			
V	REQUISITI SPECIFICI PER FORNITURE DI SERVIZI DI GESTIONE REMOTA	SI	NO	N/A
V1	Sono effettuate forniture di servizi di gestione remota?			
V2	In caso di risposta affermativa alla domanda V1			
V2.1	Sono utilizzati meccanismi che permettano di garantire l'integrità di quanto trasmesso?			
V3	In caso di necessità, da parte degli operatori, di accesso a Internet, è utilizzato un proxy centralizzato e dotato di configurazione?			
V4	Su richiesta dell'amministrazione, è effettuata la consegna alla stessa dei log di sistema generati dai dispositivi di sicurezza utilizzati, almeno in formato CSV o TXT?			
V5	In caso di risposta affermativa alla domanda V4			
V5.1	Sono inviati i log all'amministrazione entro il giorno successivo a quello in cui è avvenuta la richiesta?			
V6	è monitorata la pubblicazione di upgrade/patch/hotfix necessari a risolvere eventuali vulnerabilità presenti nei dispositivi utilizzati per erogare i servizi e nelle infrastrutture gestite?			

Copia