Regione Lazio

Regolamenti Regionali

Regolamento regionale 11 aprile 2024, n. 4

MODIFICHE AL REGOLAMENTO REGIONALE 6 SETTEMBRE 2002, N. 1 (REGOLAMENTO DI ORGANIZZAZIONE DEGLI UFFICI E DEI SERVIZI DELLA GIUNTA REGIONALE) E SUCCESSIVE MODIFICAZIONI

LA GIUNTA REGIONALE

ha adottato

IL PRESIDENTE DELLA REGIONE

e m a n a

il seguente regolamento:

Art. 1

(Modifica all'articolo 4 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. Dopo il comma 9 bis dell'articolo 4 del r.r. 1/2002 e successive modificazioni è aggiunto, in fine, il seguente:

"9 ter) Per lo svolgimento delle proprie funzioni il capo dell'Ufficio stampa è coadiuvato da un vice capo, che svolge, tra l'altro, funzioni vicarie in sua assenza.".

Art. 2

(Modifiche all'articolo 9 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. Al comma 1 dell'articolo 9 del r.r. 1/2002 e successive modificazioni sono apportate le seguenti modifiche:

a) all'alinea le parole: "è stabilito in complessive n. 234 unità" sono sostituite dalle seguenti: "è stabilito in complessive n. 232 unità";

b) alla lettera a) le parole: "massimo n. 138 unità" sono sostituite dalle seguenti: "massimo n. 136 unità".

Art. 3

(Modifica all'articolo 10 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. Al comma 2 dell'articolo 10 del r.r. 1/2002 e successive modificazioni dopo le parole: "il capo dell'ufficio legislativo." sono aggiunte in fine le seguenti: "L'incarico di vice capo dell'Ufficio stampa è conferito con provvedimento del Presidente, su proposta del capo dell'Ufficio stampa.".

Art. 4

(*Modifica all'articolo 17 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni*)

1. Alla lettera f), del comma 1, dell'articolo 17 del r.r. 1/2002 e successive modificazioni dopo le parole: "a responsabilità dirigenziale" sono inserite le seguenti: "e non dirigenziale".

Art. 5

(Modifica all'articolo 20 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. Al numero 7) del comma 1 dell'articolo 20 del r.r. 1/2002 e successive modificazioni dopo le parole: "Ragioneria generale" sono inserite le seguenti: ", alla quale è preposto il Ragioniere generale".

Art. 6

(*Modifica all'articolo 24 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni*)

1. L'articolo 24 del r. r. 1/2002 e successive modificazioni è sostituito dal seguente:

"**Art. 24**

Istituzione ed organizzazione del servizio "Relazioni con l'Unione europea"

1. Per le finalità di cui all'articolo 17, comma 1, lettere e) ed f), è istituito, nell'ambito della direzione regionale competente in materia di affari della Presidenza, il servizio denominato "Relazioni con l'Unione europea" per la cura degli interessi della Regione in sede europea.

2. La responsabilità e l'organizzazione del servizio "Relazioni con l'Unione europea" sono stabilite dal direttore della direzione regionale competente in materia di affari della Presidenza, secondo le modalità di cui all'articolo 23. L'individuazione del responsabile del servizio e del personale da assegnare alla sede di Bruxelles, in possesso di professionalità adeguata alle funzioni da svolgere, è effettuata dal suddetto direttore, sentiti il direttore generale e il direttore regionale competente in materia di personale, sulla base dei criteri definiti in sede di contrattazione decentrata. Al responsabile del servizio "Relazioni con l'Unione europea" e al personale che presta servizio presso la sede di Bruxelles, si applicano le disposizioni di cui agli articoli 334 e 335.".

Art. 7

(Modifica all'articolo 181 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. Il comma 1 dell'articolo 181 del r.r. 1/2002 e successive modificazioni è sostituito dal seguente:

"1. In attuazione dell'articolo 16 della legge di organizzazione, sulla base della programmazione dei fabbisogni di personale di cui all'articolo 202 del presente regolamento e fermi restando, relativamente alle modalità di accesso all'impiego regionale, i requisiti generali indicati nell'Allegato "O", punto 2, la copertura dei posti vacanti nella qualifica dirigenziale nell'amministrazione regionale avviene:

a) mediante concorso per esami o per titoli ed esami, al quale possono partecipare:

1) i dipendenti di ruolo delle pubbliche amministrazioni muniti del diploma di laurea attinente al posto messo a concorso, che abbiano compiuto almeno cinque anni di servizio in posizioni funzionali per l'accesso alle quali è richiesto il possesso del diploma di laurea;

2) i soggetti che, in possesso del diploma di laurea attinente al posto messo a concorso, abbiano ricoperto incarichi dirigenziali in amministrazioni pubbliche per un periodo non inferiore a cinque anni;

3) i soggetti che, in possesso del diploma di laurea attinente al posto messo a concorso, abbiano ricoperto incarichi dirigenziali in strutture private per almeno cinque anni;

4) i soggetti muniti del diploma di laurea attinente al posto messo a concorso e del diploma di specializzazione in una delle discipline oggetto delle prove scritte previste dal bando ovvero del dottorato di ricerca in una delle discipline oggetto delle prove scritte previste dal bando ovvero di altro titolo post-universitario in una delle discipline oggetto delle prove scritte previste dal bando, conseguito a seguito di corso di studi di durata almeno biennale, con superamento di esame finale, rilasciato da istituti universitari italiani o stranieri, pubblici o privati, già riconosciuti alla data di pubblicazione del bando di concorso;

b) mediante le procedure comparative di cui all'articolo 16, comma 1 bis della legge di organizzazione, riservate al personale in servizio a tempo indeterminato, iscritto al ruolo della Giunta regionale, in possesso dei titoli di studio previsti a legislazione vigente e che abbia maturato almeno cinque anni di servizio nell'amministrazione regionale in posizioni funzionali per il cui accesso sia richiesto il diploma di laurea ovvero al personale in servizio a tempo indeterminato, iscritto al ruolo della Giunta regionale, in possesso dei requisiti di cui all'articolo 16, comma 2, della legge di organizzazione, che abbia ricoperto o ricopra l'incarico di livello dirigenziale di cui all'articolo 19, comma 6, del d. lgs. 165/2001 e successive modifiche presso la Giunta regionale, nel rispetto delle percentuali di riserva previste dal medesimo articolo 16, comma 1 bis.".

Art. 8

(Modifiche all'articolo 334 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. All'articolo 334 del r.r. 1/2002 e successive modificazioni sono apportate le seguenti modifiche:

a) la rubrica è sostituita dalla seguente: "*Indennità di servizio all'estero per il responsabile del servizio Relazioni con l'Unione europea e per il personale che presta servizio presso la sede di Bruxelles*";

b) il comma 1 è sostituito dal seguente:

"1. Al responsabile del servizio "Relazioni con l'Unione europea", al personale che presta servizio presso la sede di Bruxelles ovvero temporaneamente distaccato presso tale sede per un periodo di tempo superiore a venti giorni, viene corrisposta, in aggiunta al trattamento economico in godimento, un'indennità mensile speciale i cui importi sono riportati nell'allegato "U". Tale indennità è determinata con determinazione del direttore regionale competente in materia di personale, previo accordo con le organizzazioni sindacali, con i criteri e nella misura massima di quella spettante per analogo titolo ed analoga

qualifica professionale al personale del ministero degli affari esteri in servizio presso le sedi di rappresentanza all'estero."

Art. 9

(*Modifica all'articolo 335 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni*)

1. All'articolo 335 del r.r. 1/2002 e successive modificazioni sono apportate le seguenti modifiche:

a) la rubrica è sostituita dalla seguente: "*Indennità di sistemazione per il responsabile del servizio Relazioni con l'Unione europea e per il personale che presta servizio presso la sede di Bruxelles*";

b) il comma 1 è sostituito dal seguente:

"1. Per il responsabile del servizio "Relazioni con l'Unione europea" e per il personale che presta servizio presso la sede di Bruxelles, è determinata, previo accordo in sede di contrattazione integrativa, una indennità di sistemazione nella stessa misura di quella spettante, per analogo titolo ed analoga qualifica professionale, al personale del ministero degli affari esteri in servizio presso le sedi di rappresentanza all'estero, i cui importi sono riportati nella tabella dell'allegato "U"."

Art. 10

(Modifiche all'articolo 474 del regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

1. All'articolo 474 del r. r. 1/2002 e successive modificazioni sono apportate le seguenti modifiche:

a) al comma 3:

1) dopo le parole: "in qualità di titolare" sono inserite le seguenti "o di responsabile";

2) dopo le parole: "siano conferiti a persone fisiche," sono inserite le seguenti: ", detti soggetti designati,";

3) dopo la lettera a) è inserita la seguente**:**

"a bis) il Direttore generale per il proprio ambito di competenza;";

4) dopo la lettera e) è aggiunta la seguente:

"e bis) il responsabile della struttura organizzativa autonoma di livello direzionale.";

b) al comma 5 dopo le parole "paragrafo 4, del RGPD," sono inserite le seguenti: "nonché dell'articolo 2-quaterdecies, comma 2, del d.lgs. 196/2003 e successive modificazioni,";

c) al comma 6 dopo le parole "referente privacy," sono inserite le seguenti: "tra i soggetti incaricati ai sensi del comma 5,";

d) dopo il comma 7 è inserito il seguente:

"7 bis) Qualora la Giunta regionale operi per conto di altri titolari del trattamento, in qualità di responsabile del trattamento ai sensi dell'articolo 4, n. 8) del RGPD, la stessa agisce, per mezzo dei soggetti designati, in conformità alle disposizioni del RGPD vigenti in materia, ed in particolare all'articolo 28 del medesimo RGPD.".

Art. 11

(Modifiche all'articolo 474 ter del regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

1. All'articolo 474 ter del r. r. 1/2002 e successive modificazioni, sono apportate le seguenti modifiche:

a) al comma 1:

1) la lettera d) è sostituita dalla seguente:

"d) tenere costantemente aggiornato il registro delle attività di trattamento per la struttura di competenza

qualora la Giunta regionale operi in qualità di titolare del trattamento ai sensi dell'articolo 30, paragrafo 1, del RGPD, nonché tenere aggiornato il registro delle attività relative ai trattamenti svolti per conto di altri titolari nel caso in cui operi in qualità di responsabile del trattamento, ai sensi dall'articolo 30, paragrafo 2, del RGPD;";

2) la lettera e) è sostituita dalla seguente:

"e) predisporre le informative e la modulistica per la raccolta dei consensi, ove previsto dalla normativa vigente, relative al trattamento dei dati personali nel rispetto degli articoli 13 e 14 del RGPD";

3) dopo la lettera r-quinquies) è aggiunta la seguente:

"r sexies) nell'ipotesi in cui, ai sensi dell'articolo 474, comma 7 bis, la Giunta regionale operi in qualità di responsabile del trattamento per conto di altri titolari del trattamento:

1) sottoscrivere il contratto o altro atto giuridico di nomina a responsabile del trattamento, che disciplina i trattamenti svolti per conto del titolare del trattamento, ai sensi dell'articolo 28, paragrafo 3, del RGPD;

2) verificare, prima della sottoscrizione di cui al numero 1), che il contratto o altro atto giuridico di nomina a responsabile contenga le prescritte istruzioni del titolare e l'espressa individuazione del soggetto designato tenuto al trattamento di dati personali;

3) verificare, prima della sottoscrizione di cui al numero 1), che la nomina disciplini gli obblighi previsti dall'articolo 28 del RGPD per il responsabile ed in particolare di:

3.1. non ricorrere ad eventuali sub-responsabili del trattamento in assenza di una previa autorizzazione specifica o generale del titolare;

3.2. imporre agli eventuali sub-responsabili, con contratto o altro atto giuridico, gli stessi obblighi in materia di protezione dei dati personali previsti dall'atto di nomina del numero 1) tra il titolare e il responsabile;

3.3. individuare la materia disciplinata, la durata, natura e finalità del trattamento, il tipo di dati personali e le categorie di interessati;

3.4. garantire che le persone autorizzate al trattamento di dati personali abbiano un obbligo legale di riservatezza;

3.5. adottare le misure richieste dall'articolo 32 del RGPD;

3.6. assistere il titolare, tenendo conto della natura del trattamento, al fine di soddisfare l'obbligo, in capo al titolare stesso, di dar seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del RGPD, nella misura in cui ciò sia possibile;

3.7. assistere il titolare, tenendo conto della natura del trattamento e delle informazioni a disposizione, ai fini del rispetto degli obblighi di cui agli articoli da 32 a 36 del RGPD;

3.8. cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento, su scelta del titolare;

3.9. mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 del RGPD, inclusa la facoltà di effettuare attività di revisione.";

b) dopo il comma 2 è aggiunto il seguente:

"2 bis. Il direttore della direzione regionale competente in materia di personale provvede, con propria determinazione, all'adozione dell'informativa per il personale in servizio e agli aggiornamenti della stessa.".

Art. 12

(Modifiche all'articolo 474 quater del regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

1. Al comma 1 dell'articolo 474 quater del r. r. 1/2002 e successive modificazioni sono apportate le seguenti modifiche:

a) dopo le parole: "nell'ambito della propria struttura," sono inserite le seguenti: "tra i soggetti

incaricati ai sensi dell'articolo 474, comma 5,";

b) dopo la lettera f) è aggiunta la seguente:

"f bis) supportano il soggetto designato nell'assolvimento dei compiti di cui all'articolo 474 ter, comma 1, lettera r sexies)", qualora la Giunta regionale operi in qualità di responsabile per conto di altri titolari del trattamento, ai sensi dell'articolo 474, comma 7 bis.".

Art. 13

(Modifica all'articolo 474 quinquies del regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

1. Al comma 1 dell'articolo 474 quinquies del r. r. 1/2002 e successive modifiche, dopo le parole: "e 32, paragrafo 4, del RGPD" sono inserite le seguenti: "nonché dell'articolo 2-quaterdecies, comma 2, del d.lgs. 196/2003 e successive modificazioni".

Art. 14

(Modifica all'articolo 475 del regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

1. Al comma 1 dell'articolo 475 del r. r. 1/2002 e successive modifiche dopo le parole: "di cui" sono inserite le seguenti: "alla vigente normativa in materia ed in particolare".

Art. 15

(Modifica all'articolo 476 del regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

1. La lettera e), del comma 2, dell'articolo 476 del r. r. 1/2002 e successive modifiche è abrogata.

Art. 16

(Modifica all'articolo 499 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. L'articolo 499 del r.r. 1/2002 e successive modifiche è sostituito dal seguente:

"**Art. 499**

Istituzione dell'autoparco regionale e servizi di mobilità della Giunta Regionale e del Consiglio Regionale

1. È istituito presso la Regione l'autoparco regionale, di seguito denominato autoparco, che comprende tutti gli automezzi destinati ai servizi di mobilità degli uffici centrali e periferici, nonché degli organi della Giunta e del Consiglio regionale, per le rispettive finalità istituzionali.

2. Gli automezzi dell'autoparco sono assegnati, ai fini della gestione, ad una struttura della direzione regionale competente in materia di acquisti di beni e servizi, di seguito denominata direzione regionale competente.

3. Gli automezzi dell'autoparco sono dotati, a cura della struttura di cui al comma 2, di telepass e permesso ZTL.

4. Dipendono dalla struttura di cui al comma 2 le articolazioni organizzative competenti alla gestione degli automezzi dell'autoparco istituite presso sedi regionali centrali e periferiche, nell'ambito delle quali sono nominati dei referenti.

5. Alla conduzione degli automezzi dell'autoparco è destinato:

a) il personale appartenente ai ruoli della Giunta e del Consiglio, in possesso del profilo professionale di autista, assegnato alla struttura di cui all'articolo 4, comma 1, lettera a), n. 11;

b) il personale con mansioni di autista assegnato alla struttura di cui all'articolo 4, comma 1, lettera a), n. 1);

c) il personale autorizzato alla guida autonoma con provvedimento del direttore regionale competente, di cui all'articolo 503, comma 5.

6. L'organizzazione, la gestione e l'assegnazione del personale di cui al comma 5, lettere a) e b) è assicurata dal responsabile della struttura Autoparco dell'Ufficio di gabinetto del Presidente.

7. I servizi di mobilità degli organi della Giunta regionale e del Consiglio regionale possono essere forniti, anche in house, da società o enti regionali, nel rispetto della normativa vigente in materia di acquisti di beni e servizi.".

Art. 17

(Modifica all'articolo 500 del regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

1. L'articolo 500 del r.r. 1/2002 e successive modifiche è sostituito dal seguente:

"**Art. 500**

Determinazione consistenza dell'autoparco

1. La Giunta, su proposta dell'assessore competente in materia di acquisti di beni e servizi, emana le direttive volte a determinare il numero ed il tipo dei mezzi costituenti l'autoparco, in relazione alle effettive esigenze dei servizi, tenendo, altresì, conto di eventuali mezzi sostitutivi necessari in caso di manutenzione e riparazione dei veicoli assegnati.".

Art. 18

*(Modifica all'articolo 501 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni***)**

1. L'articolo 501 del r.r. 1/2002 e successive modifiche è sostituito dal seguente:

"**Art. 501**

Assegnazione degli automezzi dell'autoparco regionale

1. Il direttore della direzione regionale competente in materia di acquisti di beni e servizi, di seguito denominato direttore regionale competente, provvede, con propria determinazione, ad assegnare gli automezzi dell'autoparco, in uso esclusivo, a:

a) il Presidente della Giunta;

b) il Capo di Gabinetto del Presidente;

c) gli Assessori Regionali;

d) il Presidente del Consiglio Regionale;

e) il Direttore Generale.

2. Il direttore regionale competente provvede, con propria determinazione, ad assegnare, ad uso esclusivo, un automezzo dell'autoparco, condotto dal personale di cui all'articolo 499, comma 5, a ciascuna delle seguenti strutture:

a) Direzione Generale;

b) Ufficio di Presidenza;

c) Ufficio di Gabinetto della Giunta;

d) Ufficio di Gabinetto del Consiglio Regionale.

3. È consentita l'assegnazione di automezzi di riserva ai soggetti e alle strutture di cui ai commi 1 e 2.

4. Gli altri automezzi dell'autoparco assegnati alla direzione regionale competente sono destinati, previa formale richiesta, ai servizi di mobilità del personale appartenente alle strutture ed agli uffici centrali e periferici della Giunta regionale per l'espletamento delle rispettive funzioni. La direzione regionale competente comunica settimanalmente al responsabile della struttura di diretta collaborazione di cui all'articolo 4, comma 1, lettera a), n. 11 gli automezzi disponibili per l'espletamento dei servizi di cui al presente comma.

5. Il direttore regionale competente provvede, con propria determinazione, a mettere a disposizione del Consiglio regionale, su richiesta dell'Ufficio di Gabinetto del Consiglio regionale, sette automezzi con autista destinati ai servizi di mobilità inerenti agli organi istituzionali ed ai dirigenti del Consiglio regionale.".

Art. 19

*(Modifica all'articolo 502 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni***)**

1. L'articolo 502 del r.r. 1/2002 e successive modifiche è sostituito dal seguente:

"Art. 502

Utilizzo degli automezzi dell'autoparco

1. Gli automezzi dell'autoparco devono essere utilizzati esclusivamente per l'assolvimento di compiti istituzionali e di servizi di rappresentanza.

2. Gli automezzi assegnati ai sensi dell'articolo 501, comma 1, possono essere utilizzati per il trasporto da e al luogo di residenza degli assegnatari.

3. È vietato trasportare sugli automezzi dell'autoparco persone estranee all'amministrazione regionale, salvo che il trasporto non sia giustificato da motivi istituzionali, di rappresentanza o correlate ai compiti svolti.

4. La struttura di cui all'articolo 4, comma 1, lettera a), n. 11 mette a disposizione della direzione regionale competente il personale necessario alla conduzione degli automezzi in consegna, manutenzione o trasferimento, laddove disponibile.".

Art. 20

(*Modifiche all'articolo 503 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni*)

1. All'articolo 503 del r.r. 1/2002 e successive modificazioni sono apportate le seguenti modifiche:

a) il comma 1 è sostituito dal seguente:

"1. Alla conduzione degli automezzi dell'autoparco è adibito il personale di cui all'articolo 499, comma 5. Le strutture di cui all'articolo 4, comma 1, lettera a), numero 1 e numero 11 individuano, rispettivamente, il personale con mansioni di autista, e il personale con profilo professionale di autista da assegnare in via esclusiva alla conduzione degli automezzi di cui all'articolo 501, comma 1.

b) dopo il comma 2 sono aggiunti i seguenti:

"2 bis. Il profilo professionale di autista è disciplinato dall'articolo 205 del presente regolamento.

2 ter. Il direttore regionale competente stabilisce, con propria determinazione, i criteri e le modalità per l'autorizzazione alla guida autonoma di automezzi dell'autoparco anche da parte di dipendenti che non siano in possesso dello specifico profilo professionale, ferma restando la copertura assicurativa.

2 quater. Le strutture regionali richiedono al direttore regionale competente l'autorizzazione alla guida autonoma per il relativo personale, fornendo apposito elenco da aggiornare semestralmente. Gli autorizzati alla guida autonoma rispettano gli obblighi, le procedure e le modalità di rendicontazione previste per il personale con profilo professionale di autista e, in particolare, devono sottoporsi alle visite mediche di controllo stabilite dal Medico Competente.

2 quinquies. La guida degli automezzi dell'autoparco regionale da parte del personale di cui all'articolo 499, comma 5, lettera c) riveste carattere residuale ove sia accertata la non disponibilità di autisti con specifico profilo professionale o di servizi di mobilità forniti, anche in house, da società o enti regionali.".

Art. 21

(Modifica all'articolo 504 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. L'articolo 504 del r.r. 1/2002 e successive modificazioni è sostituito dal seguente:

"Art. 504

Responsabilità per violazioni del Codice della strada

1. Nel caso di violazioni del Codice della strada, le conseguenti responsabilità e sanzioni amministrative pecuniarie sono di norma addebitabili a chi ha in consegna l'automezzo ossia al soggetto che commette la violazione, salvo che la violazione sia dovuta ad inderogabili esigenze istituzionali ovvero ad eventuali omissioni degli adempimenti di competenza della struttura di cui all'articolo 499, comma 2.

2. L'individuazione del conducente che commette la violazione, per i veicoli in assegnazione esclusiva ai sensi dell'articolo 503, comma 2, è assicurata mediante la tenuta, presso la struttura a cui è assegnato l'automezzo, di un apposito registro nel quale sono giornalmente indicati, per ciascun servizio da svolgere, il nominativo del conducente del mezzo, il modello e la targa dello stesso, la località di svolgimento del servizio, l'orario di partenza e di rientro. Per tutte le altre ipotesi di utilizzo degli automezzi, analogo registro è tenuto a cura della struttura di cui all'articolo 499, comma 2.

3. Tutte le procedure amministrative attinenti alla gestione delle contravvenzioni pervenute all'amministrazione regionale sono di competenza della struttura di cui all'articolo 499, comma 2.".

Art. 22

(Modifiche all'articolo 505 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. All'articolo 505 del r.r. 1/2002 e successive modificazioni sono apportate le seguenti modifiche:

a) al comma 1 dopo le parole: "di categoria D" sono aggiunte le seguenti: "assegnato alla struttura di cui all'articolo 499, comma 2.";

b) al comma 2 dopo le parole: "indicando i chilometri percorsi" sono aggiunte le seguenti: "e la presenta al responsabile della struttura di cui all'articolo 499, comma 2, il quale può impartire le opportune istruzioni per un migliore funzionamento del servizio in rapporto all'economicità della gestione.";

c) il comma 3 è abrogato;

d) al comma 4 le parole da: “La relazione annuale” a: “autoparco regionale” sono sostituite dalle seguenti: “La relazione annuale è presentata al responsabile della struttura di cui all’articolo 499, comma 2 ed è trasmessa anche al responsabile della struttura di cui all’articolo 4, comma 1, lettera a), n. 11.”;

e) al comma 5 le parole da: “preposta” a: ““autoparco regionale”” sono sostituite dalle seguenti: “di cui all’articolo 499, comma 2 ed è trasmessa anche al responsabile della struttura di cui all’articolo 4, comma 1, lettera a), n. 11.”;

f) dopo il comma 6 è aggiunto il seguente:

“6 bis. La struttura di cui all’articolo 499, comma 2 assicura la pianificazione dei corretti interventi di manutenzione periodica sia ordinaria che straordinaria sugli automezzi e la fornitura di un automezzo sostitutivo.”.

Art. 23

(Modifica all’articolo 506 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. Il comma 2 dell’articolo 506 del r.r. 1/2002 e successive modificazioni è sostituito dal seguente:

“2. Il responsabile della struttura di cui all’articolo 4, comma 1, lettera a), n. 11, organizza l’attività del personale in possesso del profilo professionale di autista addetto all’autoparco, utilizzando anche gli istituti della reperibilità e della turnazione con cadenza settimanale, nell’ambito dell’orario di servizio dell’ente definito in sede di contrattazione collettiva.”.

Art. 24

(*Modifiche all’articolo 508 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni*)

1. All’articolo 508 del r.r. 1/2002 e successive modificazioni sono apportate le seguenti modifiche:

a) il comma 1 è sostituito dal seguente:

“1. Il direttore regionale competente disciplina, con propria determinazione, le modalità di consegna e di riconsegna degli automezzi dell’autoparco.”;

b) al comma 3 le parole: “preposta alla gestione dei mezzi costituenti l’autoparco” sono sostituite dalle seguenti: “di cui all’articolo 499, comma 2”.

Art. 25

(*Modifiche all’articolo 511 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni*)

1. All’articolo 511 del r.r. 1/2002 e successive modificazioni sono apportate le seguenti modifiche:

a) al comma 1:

1) le parole: “della “Centrale acquisti” sono sostituite dalla seguente: “competente”;

2) le parole: “dei mezzi” sono sostituite dalle seguenti: “degli automezzi”;

b) al comma 2 le parole da: “i mezzi possono” a “e su richiesta motivata” sono sostituite dalle seguenti: “gli automezzi, previa autorizzazione del direttore regionale competente e sulla base di una richiesta motivata, possono”.

Art. 26

(Modifiche all'articolo 512 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. All'articolo 512 del r.r. 1/2002 e successive modificazioni sono apportate le seguenti modifiche:

a) il comma 1 è sostituito dal seguente:

"1. Il direttore regionale competente individua, con propria determinazione, i dipendenti incaricati della gestione dell'autorimessa qualificati per lo svolgimento di tale mansione.";

b) al comma 5 le parole: "comma 3" sono sostituite dalle seguenti: ", comma 2,".

Art. 27

(Modifiche all'articolo 513 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. All'articolo 513 del r.r. 1/2002 e successive modificazioni sono apportate le seguenti modifiche:

a) dopo la lettera c) del comma 1 è inserita la seguente:

"c bis) eventi sociopolitici e naturali;"

b) il comma 2 è sostituito dal seguente:

"2. Il direttore regionale competente, con propria determinazione, stabilisce i massimali relativi ai rischi di cui al comma 1.".

c) al comma 5:

1) le parole: "preposta alla gestione dei mezzi costituenti l'autoparco" sono sostituite dalle seguenti: "di cui all'articolo 499, comma 2";

2) le parole: "di diretta collaborazione autoparco regionale" sono sostituite dalle seguenti: "di cui all'articolo 4, comma 1, lettera a), n. 11.".

Art. 28

(Modifiche all'articolo 514 del regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. All'articolo 514 del r.r. 1/2002 e successive modificazioni sono apportate le seguenti modifiche:

a) alla rubrica sono aggiunte in fine le seguenti parole: ". Buoni taxi";

b) il comma 1 è sostituito dal seguente:

"1. Il rifornimento di carburante è consentito presso le stazioni di servizio, di norma, a mezzo di carta carburante consegnata al conducente dal responsabile della struttura di cui all'art. 499, comma 2 o da un suo referente presso la competente articolazione organizzativa per la gestione dei mezzi regionali.";

c) al comma 2 le parole: "di diretta collaborazione "autoparco regionale"" sono sostituite dalle seguenti: "di cui all'articolo 4, comma 1, lettera a), n. 11.";

d) dopo il comma 2 è aggiunto il seguente:

"2 bis. Nel caso in cui non sia disponibile un automezzo dell'autoparco il responsabile della struttura di cui all'articolo 499, comma 2 può consegnare uno o più buoni taxi, previa annotazione nell'apposito registro del numero dei buoni taxi consegnati, del nominativo del richiedente e del motivo dello spostamento, da controfirmare da parte dell'interessato. In caso di mancato utilizzo, i buoni taxi devono essere restituiti al consegnatario nel più breve tempo possibile e la restituzione deve essere annotata nel medesimo registro, da controfirmare da parte dell'interessato. Entro il quinto giorno del mese successivo, copia del registro relativo ai buoni taxi rilasciati nel mese precedente deve essere inviata al direttore regionale competente ai fini del controllo con le risultanze delle fatturazioni emesse dalle compagnie dei taxi.".

Art. 29

(Modifica all'allegato D al regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. La lettera A dell'allegato D al r.r. 1/2002 e successive modificazioni è abrogata.

Art. 30

(Modifica all'allegato H al regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. Al numero 19 del paragrafo D dell'allegato H al r.r.1/2002 e successive modificazioni, dopo le parole: "Direttore generale" sono inserite le seguenti: "o da un suo delegato tra i direttori regionali".

Art. 31

(Modifica all'allegato L al regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. Dopo il punto 2 dell'allegato L al r.r. 1/2002 e successive modificazioni è inserito il seguente:

"**Punto 2 bis**

(Procedure comparative riservate)

1. Le procedure comparative previste dall'articolo 16, comma 1 bis, della legge di organizzazione, alle quali possono partecipare i soggetti di cui all'articolo 181, comma 1, lettera b), sono finalizzate alla valutazione delle capacità, attitudini e motivazioni individuali e tengono conto, ai sensi dell'articolo 28, comma 1 ter, del d.lgs. 165/2001 e successive modificazioni, dei titoli professionali, di studio o di specializzazione ulteriori rispetto a quelli previsti per l'accesso alla qualifica dirigenziale, della tipologia degli incarichi rivestiti e dell'esperienza professionale maturata nonché della valutazione conseguita nell'attività svolta, con particolare riguardo a quelli inerenti agli incarichi da conferire.

2. Le procedure di cui al comma 1 consistono, ai sensi dell'articolo 28, comma 1 ter, del d.lgs. 165/2001 e successive modificazioni, in una prova scritta e una prova orale di esclusivo carattere esperienziale, finalizzate alla valutazione comparativa e definite secondo metodologie e standard riconosciuti.

3. I bandi delle procedure comparative riservate, poiché finalizzate alla valorizzazione della professionalità acquisita dal personale di ruolo, riconoscono un punteggio prevalente agli incarichi rivestiti e all'esperienza maturata nonché alla performance conseguita. I bandi prevedono, altresì, i titoli professionali e di studio da valutare e i relativi punteggi.

4. La valutazione degli incarichi, dell'esperienza e dei titoli di cui al comma 3 è effettuata dopo la prova scritta e prima che si proceda alla correzione dei relativi elaborati.

~~3~~5. Il punteggio complessivo è determinato sommando i voti riportati nella prova scritta e nella prova orale e il punteggio conseguito in seguito alla valutazione degli incarichi, dell'esperienza e dei titoli.".

Art. 32

(Modifica all'allegato BB al regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. All'allegato BB del r.r. 1/2002 e successive modificazioni, al paragrafo "Vice capo dell'Ufficio legislativo" le parole "Fino al 35%" sono sostituite dalle seguenti: "Fino al 52%";
2. All'allegato BB del r.r. 1/2002 e successive modificazioni dopo il paragrafo "Vice capo dell'Ufficio legislativo" è inserito il seguente:

Vicecapo dell'Ufficio stampa	Fino al 39% dell'ammontare annuo lordo previsto per il Direttore regionale

Art. 33

(*Modifica all'allegato II al regolamento regionale 6 settembre 2002, n. 1 e successive modifiche*)

1. L'allegato II al r.r. 1/2002 e successive modifiche è sostituito dal seguente:

"ALLEGATO II **(art. 474, c.1)**

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Denominazione delle Attività di Trattamento	Denominazione dell'attività di trattamento
Descrizione delle attività di trattamento	Breve descrizione dei trattamenti effettuati e indicazione se il trattamento è su larga scala.
Finalità dei trattamenti	Per ogni attività di trattamento devono essere indicate le finalità.
Base giuridica e fonte normativa	Per ciascuna finalità deve essere riportata la base giuridica del trattamento ai sensi dell'art. 6 del RGPD e, nei casi di cui alle lettere c) ed e) dell'art. 6 par. 1, deve essere riportata la fonte normativa che disciplina le attività svolte. Inoltre, nei casi in cui si effettui il trattamento di categorie particolari di dati personali e/o di dati relativi a condanne penali e reati, sono esplicitate le condizioni di liceità di cui, rispettivamente, all'art. 9 par. 2 e art. 10 RGPD
Categoria di interessati	Categorie di persone fisiche i cui dati sono oggetto del trattamento.

Categorie di dati	Tipologie di dati trattati, in base alla seguente classificazione: • Dati anagrafici (nome e cognome); • Numeri di identificazione (codice fiscale, indirizzo IP, numero di targa), che permettono l'identificazione diretta dell'interessato; • Dati giudiziari (art. 10 del RGPD); • Dati particolari (dati biometrici, genetici, dati relativi alla salute dell'art. 9 del GDPR).
Trasferimento all'estero	Indica se il trattamento preveda il trasferimento dei dati all'estero. Nel caso in cui si effettui, occorre indicare il paese terzo di destinazione e le eventuali garanzie adeguate di cui al capo V RGPD (es. la decisione di adeguatezza, le clausole contrattuali standard (SCC), ossia clausole standardizzate, approvate dalla Commissione europea, che consentono il trasferimento di dati al di fuori dello Spazio economico europeo (SEE).
Periodo di conservazione	Termine di cancellazione dei dati stabilito dalla normativa vigente, o in mancanza, dal Titolare. Tale termine deve essere adeguato alle finalità del trattamento.
Modalità del trattamento	Nome delle applicazioni software/sistemi utilizzati a supporto del trattamento e indicazione di eventuali archivi cartacei
Destinatari dei dati	Soggetti ai quali i dati possono essere comunicati
Responsabili del Trattamento	Soggetti che effettuano operazioni di trattamento di dati per conto della Giunta Regionale
Contitolari del Trattamento	Eventuali soggetti contitolari
Misure di sicurezza tecniche e organizzative	Descrizione delle misure volte a fornire un quadro complessivo riguardo la sicurezza del trattamento, con la possibilità di effettuare un rinvio, per una valutazione più dettagliata, ad altri documenti quali procedure organizzative interne, security policy, etc.

Art. 34

(Modifica all'allegato MM al regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

1. L'allegato MM del r.r. 1/2002 e successive modifiche è sostituito dal seguente:

"ALLEGATO MM (art. 476 bis)

POLICY PER LA GESTIONE DELLE

ISTANZE DEI SOGGETTI INTERESSATI AI SENSI DEL RGPD

SOMMARIO

1.Premessa

Il Regolamento generale sulla protezione dei dati delle persone fisiche (Regolamento UE 679/2016) - RGPD - ha stabilito nuove ed uniformi norme all'interno dell'Unione Europea con riferimento alla protezione dei dati personali delle persone ivi residenti. Esso garantisce diritti specifici ai soggetti interessati nei confronti del titolare del trattamento con riferimento alla possibilità di accesso, verifica e controllo, cancellazione dei propri dati personali.

1.1 Obiettivo

Finalità del presente documento è definire le attività, i ruoli e le responsabilità che la Regione, in qualità di Titolare dei dati trattati, pone in essere per la gestione delle richieste ricevute da parte dei soggetti interessati per l'esercizio dei propri diritti, così come previsto dall'articolo 12 del RGPD, fermo restando che, per quanto qui non riportato, si applicano le disposizioni previste nel suddetto regolamento.

1.2 Soggetti destinatari

I soggetti ai quali si rivolge il contenuto del presente documento sono:

- il titolare;
- i soggetti designati dal titolare, ovvero:
  - il Capo di Gabinetto;
  - il Direttore generale;
  - i Direttori di direzioni e di strutture di livello direzionale e agenzie regionali;
  - l'Avvocato coordinatore.

2. Ambito di applicazione

Ambito di riferimento del presente documento sono i processi di conformità che devono essere rispettati con riferimento all'evasione delle richieste dei soggetti interessati.

Tali richieste rientrano nell'ambito dell'esercizio dei diritti di quest'ultimi, ai sensi degli articoli da 15 a 22 del RGPD (ferme restando le limitazioni di cui all'articolo 23 del RGPD), ossia diritti di:

a) accesso ai dati (art. 15 del RGPD);

b) rettifica dei dati (art. 16 del RGPD) ed eventuale notifica ai destinatari dei dati (art. 19 del RGPD);

c) cancellazione dei dati (diritto all'oblio, art. 17 del RGPD) ed eventuale notifica ai destinatari dei dati (art. 19 del RGPD);

d) limitazione del trattamento (art. 18 del RGPD) ed eventuale notifica ai destinatari dei dati (art. 19 del RGPD);

e) portabilità dei dati (art. 20 del RGPD);

f) opposizione (art. 21 del RGPD);

g) diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (art. 22 del RGPD).

La possibilità di esercitare tali diritti è prevista all'interno dell'informativa resa al soggetto interessato.

2.1. Diritto di accesso

L'interessato ha il diritto di richiedere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in caso affermativo, di ottenere l'accesso agli stessi e

alle informazioni indicate dall'articolo 15 del RGPD (quali, ad esempio, le finalità del trattamento e le categorie di dati trattati).

Tale accesso non deve ledere i diritti e le libertà altrui; qualora i dati richiesti contengano anche riferimenti a soggetti terzi rispetto all'interessato, il titolare del trattamento deve valutare se la comunicazione di tali dati possa ledere i diritti di libertà dei soggetti terzi. In caso affermativo, occorre applicare una soluzione operativa, quale quella di oscurare i dati relativi a terzi.

In base al Considerando 63 del RGPD, nel caso in cui l'interessato effettui una richiesta di accesso troppo generica, non chiarendo a quali dati si riferisce, si può chiedere un'ulteriore specificazione, in ragione del fatto che la Giunta regionale tratta una notevole quantità di informazioni potenzialmente riferibili all'interessato.

2.2. Diritto di rettifica

L'interessato ha il diritto di richiedere la rettifica dei dati personali inesatti che lo riguardano e/o l'integrazione dei dati personali incompleti. La rettifica e/o l'integrazione devono avvenire senza ingiustificato ritardo.

2.3. Diritto all'oblio

L'interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo. La richiesta del soggetto interessato può essere effettuata solo per uno dei seguenti

motivi che il soggetto designato o il soggetto incaricato hanno l'onere di verificare:
a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a) o all'articolo 9, paragrafo 2, lettera a) del RGPD e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, del RGPD e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere ad un obbligo legale.

Il diritto all'oblio non può essere esercitato se il trattamento è necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo legale che richieda il trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito l'Ente;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, del RGPD, nella misura in cui il diritto di cui all'articolo 17, paragrafo 1, rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
Quando la richiesta dell'interessato, a seguito di valutazione, è ritenuta fondata, occorre altresì verificare se i dati di cui si chiede la cancellazione siano stati indicizzati, nel qual caso

occorre chiedere ai motori di ricerca (ad esempio Google, Bing, Yahoo, etc.) la deindicizzazione dei contenuti relativi ai dati personali riferiti all'interessato.

2.4. Diritto di limitazione del trattamento
L'interessato può richiedere la temporanea esecuzione della sola operazione di conservazione dei dati personali trattati dalla Regione, con conseguente inutilizzabilità e inaccessibilità dei dati per tutto il periodo di limitazione, nei casi di seguito indicati:
a) quando sia contestata l'esattezza dei dati personali che lo riguardano, eventualmente esercitando il diritto di rettifica di cui all'articolo 16 del RGPD; in tali casi la limitazione di trattamento potrà durare per il periodo di tempo necessario a procedere alla verifica dei dati di cui la Regione è in possesso;
b) quando l'interessato sostiene che il trattamento dei dati personali è illecito, ma si oppone alla cancellazione dei propri dati personali e chiede che ne sia limitato l'utilizzo;
c) qualora i dati personali siano necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, seppure non più utili alla Regione;
d) nel caso in cui l'interessato si sia opposto al trattamento dei dati ai sensi dell'articolo 21 del RGPD.
Nonostante sia stata disposta la limitazione di trattamento, i dati personali possono essere eccezionalmente trattati nei seguenti casi:
a) il trattamento sia necessario per l'accertamento, l'esercizio o la difesa di un diritto della Regione in sede giudiziaria;
b) per tutelare i diritti di una persona fisica o giuridica diversa dall'interessato istante;
c) per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
A titolo esemplificativo, si rappresentano le modalità attraverso le quali dare seguito a tale richiesta:

- trasferire temporaneamente i dati personali contrassegnati verso un altro sistema di trattamento;
- contrassegnare i dati personali come inaccessibili agli utenti del sistema di trattamento dei dati;
- rimuovere temporaneamente i dati contrassegnati dal sito web istituzionale.

2.5 Diritto di portabilità dei dati

L'interessato ha il diritto di ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano, forniti a un titolare del trattamento, e di trasmetterli a un altro titolare del trattamento, senza impedimenti da parte del titolare del trattamento cui li ha forniti, qualora siano verificate entrambe le seguenti condizioni:

- il trattamento si basi sul consenso dell'interessato al trattamento dei propri dati personali per una o più finalità specifiche, salvo il caso in cui il diritto dell'Unione o degli Stati membri disponga che l'interessato non possa revocare il divieto di trattare categorie particolari di dati ai sensi dell'articolo 9, paragrafo 1, del RGPD ovvero il trattamento sia necessario per l'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento sia effettuato con mezzi automatizzati.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento ad un altro, laddove risulti essere tecnicamente fattibile.

Il diritto alla portabilità dei dati non pregiudica il diritto di cancellazione. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di autorità pubbliche attribuite al titolare.

Il diritto alla portabilità dei dati non pregiudica i diritti e le libertà altrui.

2.6. Diritto di opposizione al trattamento

Ai sensi dell'articolo 21 del RGPD l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), del RGPD, compresa la profilazione.

Tale opposizione è volta ad inibire unicamente un determinato utilizzo dei dati personali dell'interessato.

I soggetti designati e incaricati possono continuare a trattare, a seguito di propria valutazione, i dati al cui trattamento l'interessato si è opposto, rappresentando allo stesso interessato l'esistenza di motivi legittimi cogenti per procedere al trattamento, che prevalgono sugli interessi o sui diritti e sulle libertà fondamentali che lo riguardano.

2.7 Diritto di non essere sottoposto ad un processo decisionale automatizzato.

Ai sensi dell'articolo 22 del RGPD, l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Quanto sopra a meno che la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
b) sia autorizzata dal diritto dell'Unione Europea o dello Stato membro cui è soggetto il titolare del trattamento;
c) si basi sul consenso dell'interessato.

2.8. Limitazioni ai diritti dell'interessato

È possibile che i diritti dell'interessato di cui ai punti da 2.1 a 2.7 siano limitati da particolari interessi pubblici o di altri privati. In particolare, nell'ambito del bilanciamento tra i diritti riconosciuti all'interessato ai sensi degli articoli da 15 a 22 del RGPD e determinate ipotesi concrete, in cui possa ricorrere l'esercizio degli stessi, il legislatore italiano individua specifici ambiti e materie privilegiate la cui tutela, in certe ipotesi, può determinare una compressione dei diritti dell'interessato.
Con riferimento ai limiti all'esercizio dei diritti previsti dagli articoli da 15 a 22 del RGPD, si applicano, in particolare, gli articoli 2-undecies (limitazioni ai diritti dell'interessato), 2- duodecies (limitazioni per ragioni di giustizia) e 2-terdecies (diritti riguardanti le persone decedute) del d.lgs. 196/2003 e successive modificazioni.
In particolare, ai sensi dell'articolo 2-undecies del suddetto decreto legislativo, i diritti non possono essere esercitati in ragione della possibilità che possa derivare un pregiudizio effettivo e concreto:
a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio;
b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;
c) all'attività di commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad una espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;
f) alla riservatezza dell'identità del dipendente che segnala, ai sensi della normativa vigente, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio;
g) agli interessi tutelati in materia tributaria e allo svolgimento delle attività di prevenzione e contrasto all'evasione fiscale.
3. Esercizio dei diritti degli interessati
Gli interessati che vogliano esercitare uno o più dei diritti ad essi spettanti, devono presentare la relativa domanda all'Ufficio per le Relazioni con il Pubblico (URP), che la inoltra ai soggetti designati dal titolare e tiene traccia delle domande stesse, nonché dei rispettivi riscontri. I soggetti designati dal titolare valutano le domande e provvedono al soddisfacimento delle stesse, tenendo traccia di tutti i passaggi del procedimento relativo a ciascuna di esse.

3.1. Modalità di presentazione delle istanze
Le istanze devono essere formulate in modo che sia possibile una identificazione certa dell'interessato richiedente. In particolare:
a) qualora la richiesta provenga direttamente dall'interessato, dovranno essere richiesti gli estremi del documento di identità in corso di validità;
b) qualora la richiesta provenga da parte di un terzo a ciò delegato, incluso un familiare, dovranno essere richiesti gli estremi del documento di identità in corso di validità di chi presenta la richiesta, gli estremi del documento di identità (fotocopia) in corso di validità dell'interessato, la delega scritta e firmata dell'interessato (non necessaria, invece, in caso di genitore che esercita la potestà genitoriale su un minore; in tal caso è richiesta la documentazione che attesti il legame di parentela);

c) qualora la richiesta provenga da parte di un legale dovranno essere richiesti gli estremi del documento di identità (fotocopia) in corso di validità dell'interessato, la richiesta su carta intestata del legale recante gli estremi necessari per la verifica dell'iscrizione all'albo, il mandato conferito nell'ambito della propria professione o la delega scritta e firmata dell'interessato.

Nei casi di istanze presentate telematicamente, ai fini della verifica dell'identità dell'istante, si richiama quanto disposto dall'articolo 65 del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) e successive modificazioni.
Le istanze per l'esercizio dei diritti sopra citati sono trasmesse dai richiedenti direttamente all'URP con una delle modalità previste dalla normativa vigente.
Per tutte le istanze pervenute l'URP comunica al richiedente, nella stessa forma in cui avviene la richiesta, se le informazioni fornite sono complete, e provvede a dare evidenza dell'avvenuta presa in carico.
L'URP in particolare:

a) inoltra le domande ai soggetti designati dal titolare;
b) invita gli interessati a formulare le richieste a mezzo di apposito modulo messo a disposizione dalla Regione sul proprio sito istituzionale e presso la sede dell'URP;
c) tiene un registro di tutte le richieste e dei riscontri forniti dai soggetti designati dal titolare.

Nel caso in cui, per errore, i soggetti designati dal titolare, il DPO o altro organo regionale riceva direttamente un'istanza, dovrà inoltrare la stessa all'URP per l'avvio della procedura.

3.2 Valutazione e classificazione della richiesta
A seguito della ricezione della richiesta, i Soggetti Designati dal Titolare individuano il trattamento cui la stessa si riferisce e procedono alla verifica della sua legittimità, nonché della veridicità e completezza delle informazioni ricevute. Solo per i casi particolarmente complessi gli stessi possono richiedere il supporto del DPO.
La richiesta viene valutata sulla base dei seguenti aspetti:
a) legittimità: valutazione della presenza di eventuali condizioni ostative all'evasione della richiesta (es. impossibilità di cancellazione dei dati per motivi di ordine superiore, quali salute o sicurezza pubblica, etc.);
b) veridicità: valutazione dell'esistenza dei dati che riguardano l'interessato;
c) completezza: verifica che i dati ricevuti siano completi al fine di evadere la richiesta e valutazione dell'identificabilità del richiedente.

A seconda dell'esito della valutazione, la richiesta viene classificata in:

- Evadibile: la richiesta è legittima, completa e non ci sono elementi ostativi alla richiesta. Le modalità di gestione della richiesta sono descritte nei paragrafi successivi;
- Rigettata: la richiesta non è legittima e sussistono motivazioni per il rigetto da parte dei soggetti designati dal titolare, i quali ne danno informazione all'URP, che provvede al riscontro formale all'interessato;
- Con informazioni mancanti: i soggetti designati dal titolare comunicano all'URP la mancanza di informazioni, e l'URP procede formalmente con la richiesta delle informazioni stesse all'interessato.
-

3.3. Termini per il riscontro
I soggetti designati dal titolare sono tenuti a rispondere, tramite l'URP, alle richieste dell'interessato senza ingiustificato ritardo e al massimo entro un mese.
Il termine decorre dal ricevimento della richiesta che consenta un'identificazione dell'interessato da parte dell'URP. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. L'URP informa l'interessato di tale proroga, nonché dei motivi del ritardo, entro un mese dal ricevimento della richiesta (articolo 12 del RGPD).

3.4. Modalità del riscontro

I soggetti designati dal titolare, eventualmente con il supporto della struttura ICT e del partner tecnologico coinvolto, comunicano all'URP l'esito della richiesta.

L'interessato ha il diritto di ottenere una copia dei dati personali oggetto di trattamento.

I dati e le informazioni richieste sono forniti dall'URP per iscritto o con altri mezzi, anche elettronici, (in particolare se la richiesta è presentata con mezzi elettronici e in un formato elettronico di uso comune), salvo diversa indicazione da parte dell'interessato.

Il riscontro deve essere fornito in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice, chiaro e comprensibile. Se richiesto dall'interessato, le informazioni possono essere anche fornite oralmente.

Qualora la richiesta riguardi la portabilità dei dati, i soggetti designati dal titolare, eventualmente con il supporto della struttura ICT e del partner tecnologico coinvolto, compilano un modulo interoperabile per trasmettere i dati alla parte terza e l'URP comunica all'interessato l'avvenuto trasferimento.

3.5. Mancato accoglimento

Se non ottempera alla richiesta dell'interessato, il titolare del trattamento, per il tramite del soggetto designato informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

Le informazioni fornite ai sensi degli articoli 13 e 14 del RGPD ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, l'URP e i soggetti designati dal titolare possono:

a) addebitare un contributo spese ai sensi dell'allegato V al r.r. 1/2002 e successive modifiche, tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure

b) rifiutare di soddisfare la richiesta.

L'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta è in capo al Titolare e deve essere adeguatamente motivato ai sensi della normativa vigente.

Il mancato accoglimento della richiesta deve essere motivato compiutamente e reso per iscritto, o con altri mezzi, anche elettronici, dall'URP, fornendo l'informazione relativa alla possibilità di proporre reclamo al Garante per la protezione dei dati personali e ricorso giurisdizionale.".

3.6. Tracciamento del processo

I soggetti designati dal titolare hanno l'obbligo di tenere traccia e conservare tutta la documentazione relativa alle richieste raccolte ed evase e di darne comunicazione semestrale al Responsabile Protezione dei Dati (DPO).

La comunicazione deve essere effettuata fornendo almeno le seguenti informazioni:

- numero di protocollo e data di ricezione della richiesta;
- oggetto della richiesta;
- dati identificativi del soggetto interessato richiedente;
- dati identificativi del soggetto eventualmente delegato dall' interessato;
- esito della richiesta;
- data di evasione della richiesta.".

Art. 35

(Modifica allo "schema A" dell'allegato NN al regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

1. Lo schema "A" dell'allegato NN al r.r. 1/2002 e successive modifiche è sostituito dal seguente:

"SCHEMA A
(art. 474, c. 3)

ADDENDUM AL CONTRATTO DI LAVORO

CONFERIMENTO DI COMPITI E FUNZIONI IN QUALITA' DI SOGGETTO DESIGNATO AI SENSI DELL'ARTICOLO 2 *QUATERDECIES* DEL D.LGS. 196/2003 (CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, RECANTE DISPOSIZIONI PER L'ADEGUAMENTO DELL'ORDINAMENTO NAZIONALE AL REGOLAMENTO (UE) N. 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, DEL 27 APRILE 2016, RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI, NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI E CHE ABROGA LA DIRETTIVA 95/46/CE.) E SUCCESSIVE MODIFICAZIONI. ISTRUZIONI PER L'ESERCIZIO DELLE FUNZIONI CONFERITE.

PREMESSO CHE

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

a) stabilisce che la Giunta regionale, in qualità di titolare o di Responsabile del trattamento può prevedere, ai sensi dell'articolo 2 quaterdecies del d.lgs. 196/2003 e successive modificazioni, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano conferiti a persone fisiche che operano sotto la propria autorità, espressamente designate secondo lo schema "A" dell'allegato "NN" al r.r. 1/2002, da allegare quale addendum al contratto di lavoro;

b) individua come soggetti designati di diritto il Capo di Gabinetto, il Direttore Generale, i Direttori regionali, i Direttori delle Agenzie regionali, l'Avvocato coordinatore e il dirigente cui è attribuita la competenza relativamente alle funzioni previste dal decreto legislativo 6 settembre 1989, n. 322 (Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'art. 24 della legge
23 agosto 1988, n. 400) e alle convenzioni con l'ISTAT per l'attuazione del Programma Statistico Nazionale;

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

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

VISTO il decreto legislativo 30 marzo 2001, n. 165 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche) e successive modificazioni;
VISTO il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito RGPD), che garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento al diritto di protezione dei dati personali;
ATTESO che le soluzioni tecniche e organizzative relative al trattamento dei dati personali richiedono alla Regione un costante monitoraggio e che tali misure, periodicamente riesaminate ed aggiornate, qualora necessario, devono tener conto dello stato dell'arte e dei costi di attuazione, oltre che della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso;
ATTESO che il titolare del trattamento è tenuto a mettere in atto misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati, quali la pseudonimizzazione, la minimizzazione e anche ad integrare, nel trattamento, le necessarie garanzie al fine di soddisfare i requisiti del suddetto regolamento e tutelare i diritti degli interessati alla riservatezza ed all'adeguato trattamento dei dati personali e che è tenuto, altresì, a mettere in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
CONSIDERATO che i suddetti obblighi valgono per la quantità dei dati personali raccolti, per la portata del trattamento, per il periodo di conservazione e l'accessibilità e che le misure da adottare devono garantire che, per impostazione predefinita, non siano resi accessibili dati personali ad un numero indefinito di persone fisiche senza l'intervento della persona fisica;
CONSIDERATO che ai fini del RGPD per "trattamento" si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (articolo 4, n. 2) del RGPD);
TENUTO CONTO che, ai sensi dell'articolo 24 del RGPD, il Titolare del trattamento è tenuto a mettere in atto le misure, tecniche ed organizzative, adeguare per garantire ed essere in grado di dimostrare che il trattamento sia effettuato conformemente al RGPD;

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

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

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

Tutto ciò premesso

SI CONVIENE QUANTO SEGUE

Art. 1

(Obblighi del soggetto designato)

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

Art. 2

(Istruzioni per il trattamento dei dati personali)

1. Il **<*indicare nome e cognome*>**, Soggetto designato, nell'ambito delle sue funzioni, presiede ai trattamenti di dati personali di competenza della **<indicare i riferimenti della struttura di afferenza>**, la cui elencazione e descrizione è riportata nel "Registro delle attività di Trattamento" di cui all'articolo 30 del RGPD, attenendosi al rispetto delle seguenti **istruzioni**:

a) i trattamenti devono essere svolti nel pieno rispetto delle previsioni normative vigenti in materia di protezione dei dati personali, nonché tenendo conto dei provvedimenti e dei comunicati ufficiali emessi dall'Autorità Garante per la Protezione dei Dati Personali, di seguito denominata Garante;

b) ciascun trattamento deve avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento; deve pertanto essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi;

c) il soggetto designato dovrà evitare che i dati personali siano soggetti a rischi di perdita o distruzione anche accidentale, che ai dati possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini istituzionali per i quali i dati sono stati raccolti e per i quali vengono trattati;

d) in ogni fase del trattamento non si possono eseguire operazioni per fini non previsti tra i compiti assegnati e si potrà accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere tali compiti;

e) la raccolta dei dati personali e la loro successiva registrazione devono avvenire per il solo perseguimento delle finalità istituzionali della Regione e, comunque, per scopi:
   1) *determinati*, pertanto non è consentita la raccolta come attività fine a sé stessa;
   2) *espliciti*, quindi il soggetto interessato deve essere informato sulle finalità del trattamento;
   3) *legittimi*, pertanto, oltre al trattamento, anche il fine della raccolta dei dati deve essere lecito;

f) i dati personali trattati sono: dati genericamente di natura personale (articolo 4, n. 1), del RGPD); dati sensibili (articolo 9 del RGPD "Categorie particolari di dati personali"); dati giudiziari (articolo 10 del RGPD);

g) le categorie di interessati sono quelle identificate nelle parti di competenza della **<indicare i riferimenti della struttura di afferenza>** del "Registro delle attività di Trattamento" di cui all'articolo 30 del RGPD;

h) le operazioni di trattamento nell'ambito della struttura di competenza, dovranno essere organizzate in conformità con la normativa in materia di protezione dei dati personali applicabile ed in osservanza delle eventuali indicazioni scritte impartite dalla Regione, assicurando l'applicazione del principio della protezione dei dati fin dalla progettazione e protezione predefinita di cui all'articolo 25 del RGPD, determinando i mezzi del trattamento e mettendo in atto le misure tecniche e organizzative adeguate, di cui all'articolo 32 del RGPD, prima dell'inizio delle attività. Inoltre, dovrà essere adottata ogni misura adeguata, fisica e logica, atta a garantire che i dati personali siano trattati in ossequio al principio di necessità e che siano trattati solamente per le finalità previste e per il tempo strettamente necessario al raggiungimento delle stesse (privacy by default);
i) in veste di soggetto designato al trattamento dei dati personali, dovrà collaborare con il Titolare del trattamento affinché siano garantiti tutti i diritti dell'interessato di cui al Capo III del RGPD. In particolare, dovrà attenersi ad ogni istruzione scritta impartita al riguardo dal Titolare;
j) dovranno essere rese disponibili al Titolare del trattamento, tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti previsti dalla normativa in materia di protezione dei dati personali relativamente alla struttura di competenza, consentendo di effettuare periodicamente attività di verifica, comprese ispezioni realizzate dal Titolare stesso, dal Responsabile della Protezione dei Dati o da un altro soggetto incaricato;
k) informare il Titolare del trattamento ed il Responsabile della Protezione dei Dati personali, qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti;
l) i dati devono, inoltre, essere:
    1) esatti, cioè precisi e rispondenti al vero e, se necessario, aggiornati;
    2) pertinenti, ovvero il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
    3) completi: idonei a contemplare specificamente il concreto interesse e diritto del soggetto interessato (da non intendersi nel senso di raccogliere il maggior numero di informazioni possibili);
    4) non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;
    5) conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita;
m) se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dalla normativa vigente in materia di protezione dei dati personali, è necessario provvedere, previa comunicazione al Responsabile della Protezione dei Dati (DPO) della Regione, al blocco dei dati stessi, ossia alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento, fornendo, ad esempio, l'informativa omessa, ovvero provvedendo alla cancellazione dei dati se non è possibile procedere alla regolarizzazione.

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

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

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

Luogo e data:
IL TITOLARE DEL TRATTAMENTO
Per accettazione Luogo e data
Il SOGGETTO DESIGNATO".

Art. 36

(Modifica allo "schema B" dell'allegato NN al regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

1.Lo schema "B" dell'allegato NN al r. r 1/2002 e successive modifiche è sostituito dal seguente:

"SCHEMA B

(art. 474, c. 5)

NOMINA SOGGETTI INCARICATI

(INTESTAZIONE DELLA STRUTTURA)

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

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

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

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

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

Visto il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE) e successive modificazioni;

Considerato che ai fini del RGPD si intende per:

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

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

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

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

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

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

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

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

DISPONE

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

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

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

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

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

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

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

Art. 37
(*Abrogazione dello schema D dell'allegato NN al regolamento regionale 6 settembre 2002, n. 1 e successive modifiche*)

1. Lo schema D dell'allegato NN al r. r. 1/2002 e successive modifiche è abrogato.

Art. 38
(Modifica allo schema F dell'allegato NN al regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

1. Lo schema "F" dell'allegato NN al r.r. 1/2002 e successive modifiche è sostituito dal seguente:

"***SCHEMA F***

INFORMATIVA SUI DATI PERSONALI AI VISITATORI

INFORMATIVA AI VISITATORI

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

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

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

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

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

- i dati potranno essere trattati con la collaborazione di soggetti terzi espressamente nominati Responsabili esterni del trattamento dal Titolare;
- i dati potranno essere comunicati:

  - a tutte le strutture preposte a verifiche e controlli in merito al corretto adempimento delle finalità su indicate;

  - al personale e ai collaboratori in qualità di responsabili e persone autorizzate al trattamento dei dati per le pratiche che La riguardano/interessano; tutti i soggetti sono debitamente informati ed istruiti circa gli adempimenti e le misure da adottare in materia di protezione dei dati personali;

- i dati personali non sono soggetti a diffusione;
- i dati personali saranno conservati per il tempo strettamente necessario al perseguimento delle finalità per cui i dati sono trattati, nei limiti stabiliti dalla normativa vigente e, comunque, non oltre il termine di tre mesi dall'ultimo accesso alle sedi della Giunta regionale.
- i dati raccolti non saranno oggetto di trasferimento verso paesi al di fuori dello Spazio Economico Europeo (SEE).

La informiamo altresì che:

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

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

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

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

Art. 39

(Modifica allo schema G dell'allegato NN al regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

1. Lo schema G dell'allegato NN al r.r. 1/2002 e successive modifiche è sostituito dal seguente:
2.

"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 …. ALLA DETERMINAZIONE REGIONALE N.___DEL ____

TRA

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

E

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

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

PREMESSO CHE

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

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

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

VISTO il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito anche "RGPD" o "Regolamento (UE) 2016/679"), il quale garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento al diritto alla protezione dei dati personali;

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

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

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

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

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

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

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

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

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

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

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

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

SEZIONE I

1. Clausola 1

Scopo e ambito di applicazione

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

2. Clausola 2

Invariabilità delle clausole

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

3. Clausola 3

Interpretazione

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

4. Clausola 4

Gerarchia

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

5. Clausola 5 (facoltativa)

Clausola di adesione successiva

a) qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le parti, aderire alle presenti clausole in qualunque momento, in qualità di titolare del trattamento o di responsabile del trattamento, compilando gli allegati e firmando l'allegato I;

b) una volta compilati e firmati gli allegati di cui alla lettera a), l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un titolare del trattamento o di un responsabile del trattamento, conformemente alla sua designazione nell'allegato I;

c) l'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II OBBLIGHI DELLE PARTI

6. Clausola 6

Descrizione del trattamento

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

7. Clausola 7

Obblighi delle parti

7.1. Istruzioni

a) il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate;

b) il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il Regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. Limitazione delle finalità

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

7.3. Durata del trattamento dei dati personali

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

7.4. Sicurezza del trattamento

a) Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati;

b) Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento al proprio personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. Dati "sensibili" o "particolari"

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

7.6. Documentazione e rispetto

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

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

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

è soggetto a norma delle presenti clausole e del Regolamento (UE) 2016/679;

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

7.8. Trasferimenti internazionali

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

8. Clausola 8

Assistenza al titolare del trattamento

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

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

1) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
2) l'obbligo, prima di procedere al trattamento, di consultare le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;
3) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;
4) gli obblighi di cui all'articolo 32 Regolamento (UE) 2016/679;

d) le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

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

9.2. Violazione riguardante dati trattati dal responsabile del trattamento

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

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

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

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

SEZIONE III
DISPOSIZIONI FINALI

10. Clausola 10

Inosservanza delle clausole e risoluzione

a) fatte salve le disposizioni del Regolamento (UE) 2016/679, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole;

b) il titolare del trattamento ha diritto di risolvere il contratto relativamente al trattamento dei dati personali conformemente alle presenti clausole qualora:

1) il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento ai sensi della lettera a) e il rispetto delle presenti clausole non sia stato adempiuto entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;

2) il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del Regolamento (UE) 2016/679;

3) il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o delle autorità di controllo competenti per quanto riguarda i propri obblighi in conformità alle presenti clausole o al Regolamento (UE) 2016/679;

c) il responsabile del trattamento ha diritto di risolvere il contratto relativamente al trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato, ai sensi della clausola 7.1, lettera b), il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili, il titolare del trattamento insista sul rispetto delle istruzioni stesse;

d) dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

SEZIONE IV

ULTERIORI DISPOSIZIONI

11. Clausola 11

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

a) i trattamenti dovranno essere svolti nel pieno rispetto delle normative vigenti in materia di protezione dei dati personali, nonché tenendo conto dei provvedimenti e dei comunicati ufficiali emessi dal Garante per la protezione dei dati personali. In particolare:

- i trattamenti sono svolti per le ***finalità indicate nell'allegato II***;
- i dati personali trattati in ragione delle attività di cui ai suddetti contratti hanno ad oggetto: dati personali "comuni" (articolo 4, n. 1) del RGPD, eventualmente dati particolari (articolo 9 del RGPD "Categorie particolari di dati personali") ed in casi particolari/eccezionali, previsti dalla normativa vigente, dati giudiziari di cui all'articolo 10 del RGPD (sostanzialmente ex dati giudiziari); **<*eliminare le eventuali tipologie di dati non oggetto di trattamento*>**
- le categorie di interessati sono **<*indicare le tipologie di interessato cui i dati afferiscono*>**;

b) il responsabile è autorizzato a procedere all'organizzazione di ogni operazione di trattamento dei dati nei limiti stabiliti dai contratti in essere tra le parti e dalle vigenti disposizioni contenute nel RGPD;

c) il responsabile si impegna, già in fase contrattuale, al fine di garantire il rispetto del principio della "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" di cui all'articolo 25 del RGPD, a determinare i mezzi "non essenziali" del trattamento e a mettere in atto le misure tecniche e organizzative adeguate, ai sensi dell'articolo 32 del RGPD, prima dell'inizio delle attività, nei limiti della propria autonomia consentita dalle normative vigenti e dal presente atto;

d) il responsabile dovrà eseguire i trattamenti funzionali alle attività ad esso attribuite e comunque non incompatibili con le finalità per cui i dati sono stati raccolti. Qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, il responsabile dovrà informare il titolare del trattamento ed il responsabile della protezione dei dati (DPO) della Giunta regionale del Lazio;

e) il responsabile – per quanto di propria competenza – è tenuto, in forza di normativa cogente e del contratto, a garantire – per sé, per i propri dipendenti e per chiunque collabori a qualunque titolo – il rispetto della riservatezza, integrità, disponibilità dei dati, nonché l'utilizzo dei predetti dati per le sole finalità specificate nel presente documento e nell'ambito delle attività di sicurezza di specifico interesse del titolare;

f) il responsabile ha il compito di curare, in relazione alla fornitura del servizio di cui al contratto in oggetto, l'attuazione delle misure prescritte dal Garante per la protezione dei dati personali (di seguito anche il "Garante") in merito all'attribuzione delle funzioni di "Amministratore di sistema" di cui al provvedimento del 27 novembre 2008, e successive modificazioni ed integrazioni ed, in particolare, di:

1) designare come amministratore di sistema, con le modalità previste dal provvedimento del 27 novembre 2008, le persone fisiche autorizzate ad accedere in modo privilegiato, ai sensi dello stesso provvedimento, ai dati personali del cui trattamento la Giunta regionale del Lazio è titolare;
2) conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte all'interno della società quali amministratori di sistema, in relazione ai dati personali del cui trattamento la Giunta regionale del Lazio è titolare;
3) attuare le attività di verifica periodica, con cadenza almeno annuale, sul loro operato secondo

quanto prescritto dallo stesso provvedimento; gli esiti di tali verifiche dovranno essere comunicati al titolare del trattamento su richiesta dello stesso;

g) il responsabile si impegna a garantire, senza ulteriori oneri per il titolare, l'esecuzione di tutti i trattamenti individuati al momento della stipula del contratto e dei quali dovesse insorgere in seguito la necessità ai fini dell'esecuzione del contratto stesso;

h) il responsabile dovrà attivare le necessarie procedure aziendali per identificare ed istruire le persone autorizzate al trattamento dei dati personali ed organizzarne i compiti in maniera che le singole operazioni di trattamento risultino coerenti con le disposizioni di cui alla presente nomina, facendo in modo, altresì, che, sulla base delle istruzioni operative loro impartite, i trattamenti non si discostino dalle finalità istituzionali per cui i dati sono stati raccolti e trattati. Il responsabile garantirà, inoltre, che le persone autorizzate al trattamento siano vincolate da un obbligo, legalmente assunto, di riservatezza;

i) il responsabile si attiverà per garantire l'adozione delle misure di sicurezza di cui all'articolo 32 del RGPD. In particolare, tenuto conto delle misure di sicurezza in atto, adottate a protezione dei trattamenti dei dati per conto della Giunta regionale del Lazio, come previste dal contratto vigente, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento e, sulla base delle risultanze dell'analisi dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, che derivano in particolare dalla distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati, porrà in essere le opportune azioni organizzative per l'ottimizzazione di tali misure, al fine di garantire un livello di sicurezza adeguato al rischio. Tali misure comprendono, tra le altre:

   1) la pseudonimizzazione e la cifratura dei dati personali;
   2) misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   3) misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
   4) procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

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

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

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

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

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

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

l) il responsabile dovrà predisporre e tenere a disposizione del titolare la documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito riportate; inoltre renderà disponibili al titolare tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti normativi previsti dal RGPD, consentendo di effettuare periodicamente attività di verifica, comprese ispezioni realizzate dal titolare stesso o da un altro soggetto da questi incaricato;

m) il responsabile adotterà le politiche interne e attuerà, ai sensi dell'articolo 25 del RGPD, le misure che soddisfano i principi della protezione dei dati personali fin dalla progettazione di tali misure; adotterà ogni misura adeguata a garantire che i dati personali siano trattati in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il tempo strettamente necessario al raggiungimento delle stesse;

n) il responsabile, ai sensi dell'articolo 30 del RGPD e nei limiti di quanto dallo stesso stabilito, è tenuto a tenere un registro delle attività di trattamento effettuate sotto la propria responsabilità per conto del titolare e a cooperare con il titolare stesso e con il Garante per la protezione dei dati personali, laddove ne venga fatta richiesta ai sensi dell'articolo 30, paragrafo 4, del RGPD;

o) il responsabile è tenuto ad informare di ogni violazione di dati personali (cosiddetta *personal data breach*) il titolare ed il responsabile della protezione dei dati (DPO) della Giunta regionale del Lazio, tempestivamente e senza ingiustificato ritardo, entro 24 ore dall'avvenuta conoscenza dell'evento. Tale notifica, da effettuarsi tramite PEC da inviare all'indirizzo protocollo@regione.lazio.legalmail.it e dpo@regione.lazio.legalmail.it , deve essere accompagnata da ogni documentazione utile, ai sensi degli articoli 33 e 34 del RGPD, per permettere al titolare, ove ritenuto necessario, di notificare questa violazione al Garante per la protezione dei dati personali e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando il titolare stesso ne è venuto a conoscenza. Nel caso in cui il titolare debba fornire informazioni aggiuntive alla suddetta autorità, il responsabile supporterà il titolare nella misura in cui le informazioni richieste e/o necessarie per il Garante siano esclusivamente in possesso del responsabile e/o di suoi sub-responsabili;

p) il responsabile garantisce gli adempimenti e le incombenze anche formali verso il Garante per la protezione dei dati quando richiesto e nei limiti dovuti, adoperandosi per collaborare tempestivamente, per quanto di competenza, sia con il titolare sia con il Garante per la protezione dei dati personali. In particolare:

- fornisce informazioni sulle operazioni di trattamento svolte;
- consente l'accesso alle banche dati oggetto delle operazioni di trattamento;
- consente l'esecuzione di controlli;
- compie quanto necessario per una tempestiva esecuzione dei provvedimenti inibitori, di natura temporanea;

q) il responsabile si impegna ad adottare, su richiesta del Titolare e nel rispetto degli obblighi contrattuali assunti, nel corso dell'esecuzione dei contratti, ulteriori garanzie quali l'applicazione di un codice di condotta applicato o di un meccanismo di certificazione approvato ai sensi degli articoli 40 e 42 del RGPD, laddove adottati. Il titolare potrà in ogni momento verificare l'adozione di tali ulteriori garanzie;

r) il responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del titolare;

s) il responsabile è tenuto a comunicare al titolare ed al DPO della Regione Lazio il nome ed i dati del proprio DPO, laddove il responsabile stesso lo abbia designato, conformemente a quanto prescritto dall'articolo 37 del RGPD. Il DPO collaborerà e si terrà in costante contatto con il DPO della Regione

Lazio;

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

Il Titolare del trattamento ***Il Responsabile del trattamento***

_____ _____

ALLEGATO I

Elenco delle parti

Titolare del trattamento:
Giunta Regionale del Lazio

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

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

……

Data _____ Firma

.....

Responsabile del trattamento Ragione sociale

Sede legale:

via, n.

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

PEC: laziocrea@legalmail.it
Dati di contatto del Responsabile della Protezione dei Dati personali (DPO):
……

Nome, qualifica e dati di contatto del referente:
Inserire nome referente interno

CONTESTO DI RIFERIMENTO

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

ALLEGATO II
Descrizione del trattamento

Categorie di interessati i cui dati personali sono trattati

Categorie di dati personali trattati

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

Natura del trattamento

….

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

Durata del trattamento

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

ALLEGATO III

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

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

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

Le misure applicate al trattamento sono:

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

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

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

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

9	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. 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. 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. 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.

10	Le reti interne al datacenter sono protette da firewall perimetrale. Inoltre è previsto un firewall interno al datacenter per la segregazione delle reti interne.
11	Nella realizzazione dei servizi si provvede a valutare il livello di sicurezza necessario e ad applicare le limitazioni ritenute opportune per garantire la separazione tra domini. Si applicano, in base alle specificità, segregazione di reti, fisiche e/o logiche, gestione degli accessi tramite gateway con specifici firewall e router.
12	Tutte le comunicazioni tramite posta elettronica si basano sulla sicurezza data dal server di posta, le comunicazioni in rete (nei casiritenuti necessari) avvengono in https. Quando necessario scambiare file si usano canali sicuri in STFP
13	Le informazioni coinvolte nelle trasmissioni dei servizi applicativi sono protette mediante l'utilizzo di canali sicuri (firewall, VPN), e mediante certificato o cifratura
14	Gli ambienti di test applicativi, gestiti direttamente dai gruppi di progetti che ne sono responsabili, non contengono mai dati reali, ma solo dati fittizi
15	Le installazioni e configurazioni dei vari asset, quanto possibile, vengono fatte mediante template preventivamente predisposti e verificati. I predetti template sono disponibili esclusivamente al personale autorizzato alle installazioni in sola lettura
16	Le operazioni di amministrazione remota sui server sono eseguite con protocolli sicuri ad esempio SSH ed RDP
17	Eventuali eventi di cambiamento della configurazione e dei permessi di sicurezza del sistema sono inviati al SIEM
18	Le credenziali di amministratore di dominio sono conservate in un wallet protetto da password
19	Per i messaggi di posta è attivo il servizio antispam di Microsoft in Cloud (EOP)
20	Impostazione della scadenza delle password su base trimestrale su tutti gli account con inibizione globale della possibilità di non farscadere le password. 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.
21	Previsione di elevati requisiti di complessità delle password su tutti gli account, quali: requisito di lunghezza minima di 8 caratteri; Invito a non utilizzare password comuni; educazione degli utenti a non utilizzare le password già utilizzate in ambito aziendale per scopi non legati al lavoro.
22	Razionalizzazione degli account di dominio, evitando l'annidamento di gruppi di utenti all'interno di altri gruppi amministrativi. Riduzione degli account amministrativi ad un numero essenziale, secondo i seguenti approcci: - Applicazione di restrizioni agli account locali per l'accesso remoto. - Limitazione dell'accesso di rete a tutti gli account di amministratore locale.
23	Segmentazione delle reti evitando subnet eccessivamente ampie e limitando, di fatto, la possibilità per un potenziale attaccante di eseguire movimenti laterali, favorendo il principio del privilegio minimo
24	Ove necessario, aggiornamento di firmware o SO di tutti i sistemi e i dispositivi di protezione perimetrale (Firewall, IDS/IPS, Proxy /Reverse Proxy) alle ultime release rilasciate dai rispettivi produttori

25	Individuazione di un'unica tipologia di accesso e gestione remota dei sistemi (ad esempio RDP), evitando l'utilizzo esteso di strumenti di terze parti sfruttabili anche da utenti malintenzionati (ad esempio Dameware, AnyDesk, LogMeIn)
26	Aggiornamento, all'occorrenza, dei sistemi operativi risultanti in stato end of life o end of support.
27	In caso di intrusione o minaccia, reinstallazione completa di tutti i sistemi server e contestuale posizionamento in segmenti di rete suddivisi per layer di sicurezza (Tier), ad accesso limitato e amministrabili solo da un numero limitato di workstation, a loro volta isolate dalle altre reti
28	Standardizzazione della configurazione dei Domain Controller, evitando di adibire gli stessi a ruoli secondari come ad esempio Print Server. Limitazione dell'accesso ai sistemi critici solo ad un numero ristretto di utenti, e solo da specifiche postazioni
29	Utilizzo di apparati "Next generation Firewall" periferici, segregazione dei siti, attivazione dei moduli IDS/IPS
30	Utilizzo di politiche restrittive sulla navigazione in internet degli utenti, favorendo il principio del privilegio minimo
31	Dissuasione rispetto all'utilizzo di account di servizio per accedere in modo interattivo. Monitoraggio costante dell'utilizzo degli account di servizio ed indagini circa eventuali accessi interattivi, ad esempio utilizzando il servizio offerto da Active Directory e le Group Policy ai fini della registrazione dettagliata degli eventi
32	Utilizzo di tecnologia SIEM e/o di un servizio di Cyber Detection & Protection, essenziale per la sicurezza dell'infrastruttura e per la raccolta e razionalizzazione centralizzata di log ed eventi di sicurezza provenienti da diverse sorgenti

33	Utilizzo di un servizio di Security Awareness & Training finalizzato all'educazione degli utenti in ambito Cyber Security
34	Esecuzione di assessment periodici sui livelli di maturità dei controlli di sicurezza previsti dai principali standard nazionali ed internazionali. Definizione di diversi domini di intervento analizzando gli obiettivi dell'ente e le informazioni relative ad incidenti pregressi correlati. Valutazione di possibili ulteriori azioni a fronte dei risultati dell'assessment. Consolidamento della propensione al rischio minimo e definizione di soglie di tolleranza del rischio in ciascun dominio individuate.
35	Al fine di prevenire attacchi esterni, esecuzione assessment periodici su sistemi Linux/Unix. Valutazione di possibili ulteriori azioni a fronte dei risultati ottenuti (es. individuazione di account non censiti, creati dall'eventuale attaccante allo scopo di futuri utilizzi; individuazione di possibili tracce di accesso non autorizzato ai sistemi, come autenticazioni fuori dall'orario di servizio o mediante account non noti).
36	Utilizzo di servizi continuativi di Vulnerability Assessment, Penetration Testing & Patch Management. Identificazione continua delle vulnerabilità dei sistemi, al fine di recepire il reale livello di sicurezza dell'infrastruttura e definire un piano di rientro assegnando le giuste priorità sulla base della criticità dei processi di Patching rispetto all'impatto sulla produzione

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

(ove applicabile indicare eventuali subappaltatori del fornitore)
Saranno qui inseriti i sub-responsabili individuati a seguito di specifica esigenza del titolare.

Ragione sociale del sub-responsabile

SUB-TRATTAMENTO DELEGATO: Gestione xxxxxxxxxxxx.

ALLEGATO V
Disciplina dei servizi di Amministratore di Sistema
(laddove le prestazioni contrattuali implichino 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 implichino l'erogazione di servizi di amministrazione di sistema, la società, in qualità di responsabile del trattamento, si impegna a:

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

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

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

ALLEGATO VI
Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

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

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

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

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

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

Art. 40

(Modifica dell'allegato OO al regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

1. L'allegato OO al r.r. 1/2002 e successive modifiche è sostituito dal seguente:

REGIONE LAZIO

"ALLEGATO OO

PROCEDURA OPERATIVA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI "PERSONAL DATA BREACH"

-versione 1.0-

1. PREMESSA E OBIETTIVI

1.1. Premessa

1.2. Ambito di applicazione

1.3. Obiettivi

A. DEFINIZIONE DELLA PROCEDURA, RUOLI E RESPONSABILITÀ

1. Procedura operativa generale

2. Ruoli e Responsabilità

B. PROCEDURA OPERATIVA

1. Segnalazione

2. Identificazione

3. Valutazione

4. Gestione e risposta

5. Analisi post incidente (post incident review)

6. ALLEGATI

Allegato A: Registro Data Breach

Allegato B: Data Breach Report

Allegato C: Metodologia di valutazione della gravità di un Personal Data Breach

1. Premessa e obiettivi

1.1. Premessa

Il 24 maggio 2016 è entrato in vigore il "Regolamento (UE) 2016/679 (di seguito anche "RGDP"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abrogava la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). A partire dal 25 maggio 2018 questo regolamento è pienamente applicabile in tutti gli Stati membri. Elemento cardine di questa normativa è il concetto di "responsabilizzazione totale del Titolare" con il quale viene introdotta la responsabilizzazione dei soggetti convolti nella protezione dei dati personali e la capacità di rendere conto delle proprie azioni.

Una delle novità introdotte dal RGDP è costituita dal processo di gestione delle "Violazioni dei dati personali". Il presente documento descrive la procedura che la Giunta della Regione Lazio adotta per la gestione degli eventi anomali e degli incidenti di violazione dei dati personali.

1.2. Ambito di applicazione

La presente procedura si applica ad ogni evento che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali[1] trattati dalla Giunta della Regione Lazio nel ruolo di Titolare (di seguito anche "***Personal Data Breach***" o "**Violazione dei dati personali**")[2].

In particolare, secondo quanto previsto dalle Linee Guida 9/2022 sulla gestione e la notifica della violazione di dati personali ("*Personal Data Breach*") gli eventi di possibile violazione dei dati personali possono essere classificati in tre macrocategorie:

- "**Violazione di confidenzialità**" o anche detta "**Violazione di riservatezza**": in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;

[1] **«dato personale»**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; (art. 4, n.1, RGPD)

[2] **«violazione dei dati personali»:** violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (Art.4, n.12, RGPD)

- "**Violazione di disponibilità**": in caso di perdita accidentale o non autorizzata dell'accesso ai dati o la distruzione di dati personali;
- "**Violazione di integrità**": in caso di alterazione non autorizzata o accidentale dei dati personali.

Inoltre, una violazione potrebbe comportare contemporaneamente una compromissione della confidenzialità, della disponibilità e dell'integrità dei dati personali.

A norma dell'articolo 33 del RGPD, la **notifica** della violazione **al Garante per la Protezione dei Dati Personali** (nel seguito anche "Garante") deve avvenire senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui si venga a conoscenza della violazione,** a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

A norma dell'art. 34 del RGPD, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento **comunica la violazione all'interessato senza ingiustificato ritardo.**

Si rinvia alle Linee guida EDPB[3] 01/2021 per gli esempi riguardanti la notifica di violazione dei dati.

1.3. Obiettivi

Nel presente documento vengono definite ed individuate le attività, i ruoli e le responsabilità nella gestione dei "*Personal Data Breach*".

Il documento contiene le indicazioni operative e le informazioni necessarie per garantire il governo e l'attuazione del processo di gestione dei *Personal Data Breach*. Il presente documento si articola in due differenti sezioni:

A. DEFINIZIONE DELLA PROCEDURA, RUOLI E RESPONABILITÀ ha l'obiettivo di:

- definire la procedura operativa generale di gestione delle violazioni di dati personali trasmessi, conservati o trattati dalla Giunta della Regione Lazio nel ruolo di Titolare;
- individuare i ruoli e le responsabilità degli attori coinvolti nella procedura;

B. PROCEDURA OPERATIVA DI GESTIONE ha l'obiettivo di:

- declinare analiticamente le fasi di gestione operativa delle potenziali violazioni di dati personali.

A. DEFINIZIONE DELLA PROCEDURA, RUOLI E RESPONSABILITÀ

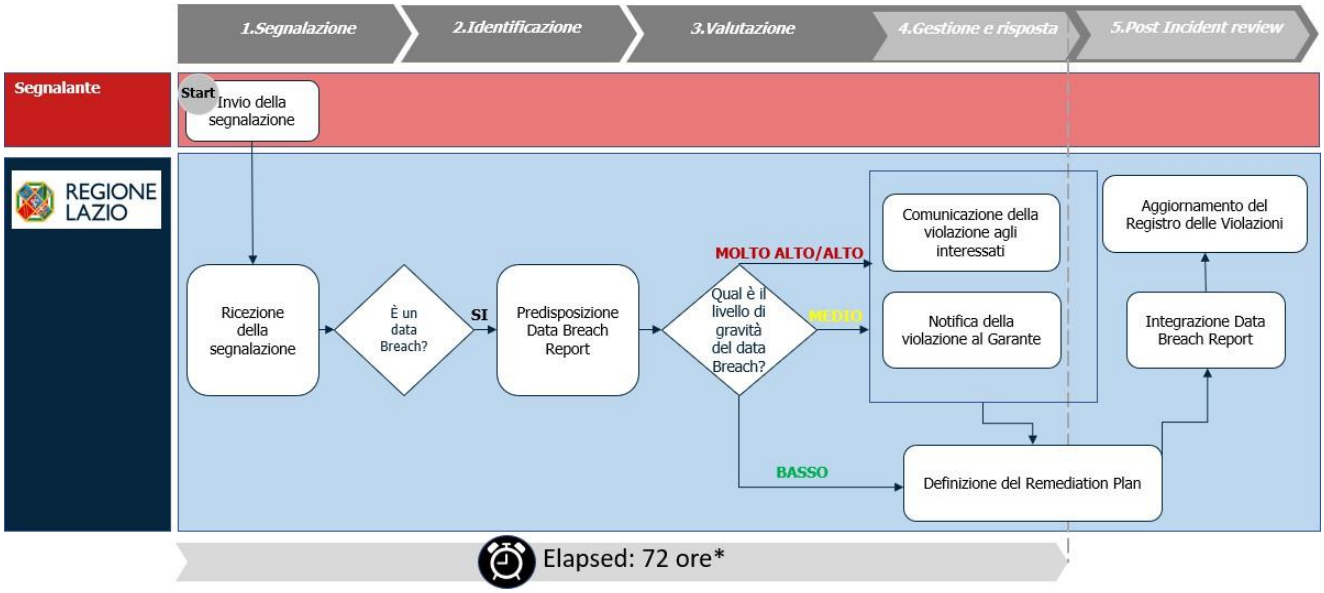
[3] European Data Protection Board (https://edpb.europa.eu/edpb_it)

1. Procedura operativa generale

Ogni violazione dei dati personali, occorsa nell'ambito di trattamenti di dati personali trattati dalla Giunta Regionale nel ruolo di Titolare, deve essere gestita secondo quanto previsto nelle fasi descritte di seguito:

- **Segnalazione**: fase di segnalazione/ricezione di un potenziale *Personal Data Breach*;
- **Identificazione**: fase in cui la segnalazione ricevuta viene identificata come un *Personal Data Breach* o come altro incidente di sicurezza (falso positivo); se si tratta di ***Personal Data Breach***, viene predisposto il *Data Breach Report* sulla base delle informazioni al momento disponibili e si procede alle fasi successive;
- **Valutazione**: fase di analisi e stima della gravità del *Personal Data Breach* con riferimento ai diritti ed alle libertà delle persone fisiche coinvolte, sulla base delle informazioni al momento disponibili.
  Tale fase si protrae anche nel seguito, in funzione di nuove informazioni rilevate.
- **Gestione e risposta**: in base al livello di gravità del Personal Data Breach, la Giunta regionale dovrà comunicare la violazione agli interessati e/o al Garante; inoltre, in tale fase, viene definito il piano di mitigazione (Remediation Plan) al fine di porre rimedio alla violazione e per attenuarne i possibili effetti negativi;
- **Analisi post incidente (*post incident review*)**: fase conclusiva di analisi ex post della violazione al fine di comprendere le cause, apprendere dagli errori e valutare le opportunità di miglioramento; in tale fase viene ulteriormente integrato il *Data Breach Report*.

Nella figura seguente è rappresentato il diagramma di flusso del processo di gestione delle violazioni dei dati personali.



** Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.*

Nel caso in cui la Giunta Regionale agisca in qualità di Responsabile per conto di un altro Titolare, è tenuto a informare tempestivamente il titolare in modo che, qualora la violazione costituisca un *Personal Data Breach*, lo stesso possa attivarsi per le fasi del processo di gestione dello stesso.

2. Ruoli e Responsabilità

La tabella seguente descrive i ruoli e le responsabilità previsti all'interno della presente procedura operativa.

Codice	Attore	Ruolo
TT	**Titolare del Trattamento**	Il Titolare del trattamento, ovvero la Giunta Regionale, ha la responsabilità ultima della corretta gestione delle violazioni dei dati personali trattati. A seguito della ricezione della segnalazione di una possibile violazione, la Giunta regionale, si avvale dei soggetti designati di cui all'art. 474 ter del regolamento regionale 1/2002, per le fasi di **Identificazione**, **Valutazione**, **Gestione e Risposta** alle violazioni di dati personali e per la fase di ***Analisi post incidente (post incident review).***
TDB	**Team Data Breach**	Il team *Data Breach*, formato da alcuni soggetti designati e dal DPO regionale, si attiva nella fase di identificazione, con la seguente composizione: • DPO regionale; • Soggetto designato competente in materia di protezione dei dati personali (SDP); • Soggetto designato competente in materia di sistemi informativi (ICT); • Soggetto designato competente rispetto al trattamento per il quale si è verificata una violazione (SDC); Il *Team Data Breach* segue tutte le fasi della presente procedura.

DPO	**Data Protection Officer - DPO**	Il DPO supporta i Soggetti designati nell'intero processo di gestione del *Personal Data Breach.*
SDP	**Soggetto designato competente in materia di protezione dei dati personali**	Il soggetto designato competente in materia di protezione dei dati personali, nella fase di **Identificazione**, ha la responsabilità di stabilire se la segnalazione costituisca o meno una violazione. Nelle fasi di **Valutazione**, **Gestione e Risposta**, all'interno del Team Data Breach, supporta il SDC nella valutazione del livello di gravità, nonché nell'elaborazione del piano di mitigazione. Nella fase di **Analisi post incidente (post incident review)**, ha la responsabilità di aggiornare il **Registro delle Violazioni**.
ICT	**Soggetto designato competente in materia di sistemi informativi**	Il soggetto designato competente in materia di sistemi informativi, nelle fasi di **Identificazione** e **Valutazione**, supporta, all'interno del Team Data Breach, il SDC nella valutazione del livello di gravità. Nella fase di **Gestione e risposta,** in collaborazione con il *Team Data breach*, supporta il SDC nella redazione della notifica al Garante e agli interessati. Nella medesima fase collabora alla stesura del piano di mitigazione e, in attuazione dello stesso, adotta le conseguenti azioni ricadenti nell'ambito della gestione dei sistemi informativi. Nella fase di **Analisi post incidente (post incident review)** fornisce, collaborando con il *Team data brach*, informazioni per l'aggiornamento del *Data Breach Report*.

SDC	**Soggetto designato competente rispetto al trattamento per il quale si è verificata una violazione**	Il SDC, nella fase di **Identificazione** con il supporto del *Team Data breach* raccoglie tutte le informazioni disponibili, predisponendo il *Data Breach Report*. Nella fase di **Valutazione** ha la responsabilità di valutare il livello di gravità della violazione. Nella fase di **Gestione e Risposta**, con il supporto del *Team Data Breach*, ha la responsabilità di predisporre e trasmettere la notifica al Garante e agli interessati. Inoltre, al termine di tale fase, il SDC compila e trasmette il *Data Breach Report* al SDP. Nella medesima fase collabora alla stesura del **piano di mitigazione (remediation plan)** e, in attuazione dello stesso, adotta le conseguenti azioni ricadenti nell'ambito organizzativo di propria competenza.
DG	**Direttore Generale**	Il Direttore Generale, a seguito dell'identificazione di un *Personal Data Breach*, viene informato dal SDC in tutte le fasi del processo.
SS	**Soggetto che effettua la segnalazione**	Soggetto che segnala un potenziale *Personal Data Breach.*

B. PROCEDURA OPERATIVA

In questa Sezione vengono declinate in modo analitico le fasi del processo di gestione del *Personal Data Breach* adottate dal Titolare.

Per ogni fase del processo vengono definiti mediante la matrice RACI[4] i ruoli e le responsabilità degli attori coinvolti nella procedura di gestione dei *Personal Data Breach*.

[4] La matrice RACI specifica il tipo di relazione fra la risorsa e l'attività: Responsible, Accountable, Consulted, Informed. Responsible (R)= è colui che esegue e assegna l'attività; ***Accountable (A)*** è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato; ***Consulted (C)=*** è la persona che aiuta e collabora con il *Responsible* per l'esecuzione dell'attività; ***Informed (I)=*** è colui che deve essere informato, al momento dell'esecuzione dell'attività o (spesso) al suo completamento.

1. Segnalazione

R	A	C	I
SS	SS	SDP	SDP

R=Esecutore A=Responsabile C=Coinvolto I=Informato

In qualsiasi momento in cui i dipendenti, il personale della Giunta Regionale, il Soggetto Designato anche nell'ambito delle attività di trattamento svolte dalla Giunta Regionale per conto di un altro titolare e altri possibili soggetti, rilevino un potenziale *Personal Data Breach*, devono darne tempestivamente comunicazione al SDP attraverso l'indirizzo e-mail dedicato databreach@regione.lazio.legalmail.it.

È possibile che le segnalazioni, soprattutto qualora provenienti da terze parti esterne alla Giunta regionale (es. utenti, fornitori), vengano ricevute attraverso un canale di comunicazione diverso da quello sopra indicato, quale ad esempio:

- Posta ordinaria;
- Posta elettronica;
- Indirizzo PEC diverso da quello sopra indicato;
- Comunicazione allo sportello - URP della Giunta della Regione Lazio.

In questi casi, il soggetto che ha ricevuto la segnalazione di un potenziale *Personal Data Breach*, informa tempestivamente e senza ingiustificato ritardo il Soggetto Designato (es. Direttore regionale) e contestualmente trasmette la segnalazione all'indirizzo databreach@regione.lazio.legalmail.it.

Stante il limitato arco temporale a disposizione del Titolare, per comunicare all'Autorità l'eventuale Personal Data Breach (72 ore solari dalla ricezione della segnalazione) **tutti i soggetti riceventi le segnalazioni sono tenuti a trasmetterle tempestivamente all'indirizzo** databreach@regione.lazio.legalmail.it e **a fornire prontamente il proprio supporto in caso di qualsivoglia dubbio sulla natura della richiesta.**

Si riportano di seguito alcune caratteristiche che possano aiutare a rilevare un evento anomalo che possa rappresentare un potenziale *Personal Data Breach*:

- Qualsiasi evento di un sistema o servizio che tratti dati personali o di rete che sia indicativo di una possibile violazione della politica di sicurezza delle informazioni;
- Un fallimento di una misura di sicurezza;
- Un malfunzionamento del pc o dei programmi utilizzati (ad esempio antivirus, firewall, sistemi di rilevamento delle intrusioni);

- Una situazione anomala o precedentemente sconosciuta che potrebbe essere rilevante per la sicurezza;
- La rilevazione di dati personali diffusi pubblicamente in Internet.

Inoltre, a titolo esemplificativo e non esaustivo vengono riportate di seguito alcune tipologie di violazione che potrebbero tradursi in *Personal Data Breach* qualora dovessero coinvolgere i dati personali:

- **distruzione di dati informatici o documenti cartacei** (intesa come indisponibilità irreversibile di dati con accertata impossibilità di ripristino degli stessi), conseguente ad eliminazione logica (es. errata cancellazione dei dati nel corso di un intervento manuale o automatizzato) o fisica (es. rottura di dispositivi di memorizzazione informatica, incendio/allagamento locali dove sono archiviati i contratti ed altri documenti dei clienti);
- **perdita di dati, conseguente a smarrimento/furto di supporti** informatici (es. laptop, HD, memory card) o di documentazione contrattuale o altri documenti cartacei (in originale o in copia);
- **accesso non autorizzato o intrusione a sistemi informatici**, lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione oppure attraverso la compromissione o rilevazione abusiva di credenziali di autenticazione (es. userid e password) per l'accesso ai sistemi;
- **modifica non autorizzata di dati**, derivante ad esempio da un'erronea esecuzione di interventi sui sistemi informatici o intervento umano;
- **rivelazione di dati e documenti a soggetti terzi non legittimati**, anche non identificati, conseguenti ad esempio, alla fornitura di informazioni, anche verbali, a persone diverse dal soggetto legittimato (in assenza di delega formale di quest'ultimo), all'invio di fatture o altri documenti di valore contrattuale a soggetti diversi dall'effettivo destinatario o errata gestione di supporti informatici.

2. Identificazione

R	A	C	I
SDP	SDP	TDB	DG

R=Esecutore A=Responsabile C=Coinvolto I=Informato

Dopo aver raccolto tutte le informazioni necessarie e disponibili, il SDP valuta la segnalazione ricevuta e:

- se ritiene che **non** si tratti di un *Personal Data Breach*, conclude il procedimento, dandone comunicazione al SS.

- se ritiene che si tratti di un *Personal Data Breach*, convoca, anche per le vie brevi, *il team data*

breach (TDB) che si occuperà di tutte le fasi successive e informa il Direttore Generale.

A seguito dell'identificazione di un *Personal Data Breach*, il SDC con il supporto del *Team Data breach*:

- raccoglie tutte le informazioni disponibili, predisponendo il ***Data Breach Report*** (**Allegato B**), coinvolgendo eventualmente anche altri soggetti designati ed eventuali responsabili del trattamento.

In ogni caso, se la segnalazione riguarda una violazione di natura informatica, il Team Data Breach e, in particolare, il Soggetto designato competente in materia di sistemi informativi (ICT), provvedono ad attivare la specifica procedura adottata dalla Giunta Regionale per la gestione degli incidenti di sicurezza informatica.

3. Valutazione

R	A	C	I
SDC	SDC	TDB	DG

R=Esecutore A=Responsabile C=Coinvolto I=Informato

In base alle informazioni raccolte nel *Data Breach Report* (**Allegato B**), il SDC, coadiuvato dal TDB, ha la responsabilità di valutare la *gravità* della violazione dei dati personali mediante la "**Metodologia di valutazione della gravità di un Data Breach**" (**Allegato C**), stimando il potenziale rischio per i diritti e le libertà delle persone fisiche.

In alternativa, è utilizzabile lo strumento di auto-assesment di valutazione per la notifica di una violazione dei dati personali (Data Breach) presente sul sito web del Garante al seguente link https://servizi.gpdp.it/databreach/s/self-assessment.
Ai fini del calcolo del punteggio di gravità dei Data Breach vengono utilizzati i criteri fondamentali stabiliti dalla metodologia e dalle raccomandazioni stilate da ENISA (European Union Agency for Network and Information Security), "*Recommendations for a methodology of the assesment of severity of personal data breaches* " (by Enisa – European Union Agency for Network and Information Security).

All'esito di questa fase, il livello di "*gravità*" del *Personal Data Breach*, che deve essere comunicato al Direttore Generale (DG), potrà essere:

Livello	Descrizione

Trascurabile	Il rischio non comporta conseguenze significative o danni considerevoli per gli individui interessati.
Basso	Gli interessati non sono stati impattati o potrebbero incontrare alcuni inconvenienti superabili senza particolari difficoltà (tempo trascorso a reinserire informazioni, disagi minori, etc.).
Medio	Gli interessati possono incontrare taluni disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, discriminazione lieve, incomprensione, stress, etc.).
Alto	Gli interessati possono subire conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in black-list, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento delle condizioni di salute, etc.).

4. Gestione e risposta

R	A	C	I
SDC	SDC	TDB	DG

R=Esecutore A=Responsabile C=Coinvolto I=Informato

In base al livello di gravità del *Personal Data Breach* definito nella fase precedente, il SDC, coadiuvato dal TDB, ha la responsabilità di procedere con:

- la redazione del modulo per la notifica preliminare, integrativa e definitiva;
- l'invio al Garante della notifica della violazione dei dati personali;
- la comunicazione agli interessati coinvolti nella violazione dei dati.

Il SDC procede secondo le regole sintetizzate in tabella:

Livello di rischio	Ove possibile entro le 72 ore	Senza ingiustificato ritardo
	Notifica al Garante	*Comunicazione all'interessato*
Rischio alto	SI	SI

Rischio medio	SI	NO
Rischio basso	NO	NO
Rischio trascurabile	NO	NO

Comunicazione agli interessati

Qualora il *Personal Data Breach* presenti un rischio alto per i diritti e le libertà delle persone fisiche, il SDC ha la responsabilità di dare comunicazione agli interessati senza ingiustificato ritardo tramite opportuno strumento di comunicazione.
Tuttavia, qualora sussista una delle seguenti condizioni, non è necessaria la comunicazione agli interessati:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Notifica al Garante per la protezione dei Dati Personali

A norma dell'articolo 33 RGPD è prevista la notifica della violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il Titolare ne sia 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.
La notifica viene effettuata dal SDC, attraverso l'apposita procedura telematica resa disponibile dal Garante nel portale dei servizi online dell'Autorità, raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ (*Provvedimento del 27 maggio 2021*).
Al fine di garantire uniformità delle notifiche/comunicazioni dirette rispettivamente all'Autorità di controllo e all'interessato/i, il legislatore europeo ha indicato le informazioni minime che le stesse devono contenere, così come di seguito indicato:

Contenuto notifica diretta all'autorità	Contenuto comunicazione all'interessato

di controllo[55]	
• **Natura della violazione** dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione	• **Descrizione** con linguaggio semplice e chiaro circa la **natura della violazione** dei dati personali
• **Nome e i dati di contatto del DPO** o di altro punto di contatto presso cui ottenere più informazioni	• **Nome e i dati di contatto del DPO** o di altro punto di contatto presso cui ottenere più informazioni
• **Probabili conseguenze della violazione** dei dati personali	• **Probabili conseguenze della violazione** dei dati personali
• Descrizione delle **misure adottate o di cui si propone l'adozione** per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi	• Descrizione delle **misure adottate o di cui si propone l'adozione** per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi

Piano di mitigazione

Il SDC definisce in questa fase un piano per porre rimedio alla violazione e attenuarne i possibili effetti negativi. Inoltre, per la componente del *Personal Data Breach* di natura fisica e organizzativa, assume gli atti di propria competenza.
Inoltre, si avvale del supporto del ICT per la componente del *Personal Data Breach* di natura tecnico-informatica, tenendo in considerazione e/o integrando il piano con le risultanze dell'attività di gestione degli incidenti di sicurezza informatica.
Ciascun soggetto designato ed eventualmente le altre strutture regionali interessate, per la parte di propria competenza, attuano le azioni definite nel remediation plan.

Al termine di questa fase il SDC invia al SDP il **Data Breach Report** aggiornato.

5. Analisi post incidente (post incident review)

R	A	C	I

[5] Qualora e nella misura in cui **non sia possibile fornire le informazioni contestualmente**, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

SDP	SDP	TDB	DG

R=Esecutore A=Responsabile C=Coinvolto I=Informato

La fase di Post Incident Review è la fase conclusiva e di analisi *ex post* della violazione al fine di comprendere le cause del *Personal Data Breach*, apprendere dagli errori e valutare le opportunità di miglioramento.
Il SDP ha la responsabilità di far confluire il *Data Breach Report* nel ***Registro Data Breach*** (**Allegato A**) che consentirà al Titolare di documentare "qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio." (art. 35, paragrafo 5, RGPD).
Tale Registro consentirà al Garante di verificare, in caso di ispezione o richiesta di specifica, il rispetto degli adempimenti in capo al Titolare nella gestione delle violazioni dei dati personali.

6. Allegati

ID	Allegato	
A	**Registro Data Breach**	
B	**Data Breach Report**	
C	**Metodologia di valutazione della gravità di un *Personal Data Breach***	

Allegato A

Registro Data Breach

REGIONE LAZIO

Struttura segnalante	Descrizione della segnalazione	E' un Data Breach?	Motivazioni della scelta	Data Breach Report	Valutazione del livello di gravità del Data Breach	Notifica al Garante	Comunicazione agli interessati	Documenti a supporto
☐ Interna a Regione Lazio: *[specificare]* ☐ Esterna a Regione Lazio: *[specificare se fornitore o terzo]*	*Inserire contenuto della segnalazione o link alla stessa*	**NO**	*inserire le motivazioni che hanno portato alla decisione di non considerare la segnalazione come Data Breach*	/		/	/	/
☐ Interna a Regione Lazio: *[specificare]* ☐ Esterna a Regione Lazio: *[specificare se fornitore o terzo]*	*Inserire contenuto della segnalazione o link alla stessa*	**SI**	*inserire le motivazioni che hanno portato alla decisione di considerare la segnalazione come Data Breach*	*Inserire / linkare il Data Breach Report*	Medio	SI	NO	*Inserire/ linkare i documenti a supporto della notifica /comunicazione del Data Breach*
☐ Interna a Regione Lazio: *[specificare]* ☐ Esterna a Regione Lazio: *[specificare se fornitore*	*Inserire contenuto della segnalazione o link alla stessa*	**SI**	*inserire le motivazioni che hanno portato alla decisione di considerare la segnalazione come Data Breach*	*Inserire/ linkare il Data Breach Report*	Molto Alto	SI	SI	*Inserire/ linkare i documenti a supporto della notifica/ comunicazione del Data Breach*

	o terzo]							

Allegato B

Data Breach Report

REGIONE LAZIO

in celeste sono indicate le informazioni da fornire in caso di comunicazione agli interessati ai sensi dell'art. 34

in grigio sono indicate le informazioni, in aggiunta alle informazioni in celeste, da fornire nella notifica al Garante ai sensi dell'art. 33

ID progressivo	**001/ 2022**	
Data Breach riportato da: **Contatti dell' utente:** **Data e ora:** **Struttura di appartenenza:**	*Inserire Nome e Cognome dell'Utente che ha segnalato la violazione o del soggetto terzo (es.fornitore) Inserire l'indirizzo email o il numero di telefono dell'utente che ha segnalato la violazione* *Indicare la data della segnalazione (gg/mese/anno) e l'ora (hh:mm)* *Inserire la struttura di appartenenza dell'utente*	
Data Protection Officer		
Breve descrizione della violazione	*Es. Hacker entra in possesso delle credenziali, perdita o furto di un laptop, modifica dolosa dei dati di un cliente, etc.*	
Dispositivo oggetto di violazione	*Es. Server, dispositivo mobile, documento cartaceo, file o parte di un file, strumento di bakcup, strumento di rete, etc.*	
Tipologia di violazione	☐	Violazione, intenzionale o accidentale, alla riservatezza dei dati perso nali (accesso illegittimo)
	☐	Violazione, intenzionale o accidentale, all' integrità dei dati personali (modifica indesiderata)
	☐	Violazione, intenzionale o accidentale, alla disponibilità dei dati personali (scomparsa/distruzio ne).
	numero di interessati coinvolti	*Indicare, ove possibile, il numero approssimativo dei soggetti impattati dalla violazione*

Interessati	☐	Dipendenti
	☐	Familiari dei dipendenti
	☐	Collaboratori e professionisti esterni
	☐	Fornitori
	☐	Soci
	☐	Visitatori
	☐	Clienti
	☐	Clienti potenziali
	☐	Amministratori/Sindaci
	☐	Familiari Amministratori/sindaci
	☐	Candidati all'assunzione
	☐	Stagisti/interinali
	☐	Minori
	☐	Soggetti terzi
Tipologie di Dati personali	☐	Dati ordinary
	☐	Dati particolari - sensibili
	☐	Dati particolari - giudiziari
	☐	Dati particolari - patrimoniali
	☐	Dati di video sorveglianza
	☐	Dati biometrici
	☐	Dati CRIF
	☐	Dati CR Banca d'Italia
	☐	Dati di geo localizzazione
	☐	Dati comportamentali
	☐	Log di Sistema
	Volume dei dati coinvolti	*Indicare, ove possibile, il numero approssimativo di registrazioni di dati personali oggetto di data breach*
Misure di sicurezza tecnico - organizzative (ex ante)	*Indicare se i dati oggetto di data breach so no protetti da tecniche di cifratura/crittografia o protetti da altre misure tecnico /organizzative che limitano ex ante gli effetti negativi per i diritti e le libertà degli interessati.*	
Misure di sicurezza tecnico - organizzative (ex post)	*Descrivere le misure tecnico /organizzative di cui si propone l'adozione, o già adottate subito, per porre rimedio alla violazione e per attenuare i possibili effetti negativi*	
Conseguenze della violazione	*Indicare le probabili conseguenze della violazione dei dati personali*	

Valutazioni del Comitato Privacy	
Valutazione del livello di gravità del Data Breach	*CG = CED * FI +CV (ref. Metodologia di valutazione della gravità di un Data Breach)*
Deve essere notificato al Garante?	*Se SI allegare il documento con il quale si è no tificato il Data Breach al Garante Privacy*
Deve essere comunicato agli interessati?	*Se SI, allegare il documento con il quale si è comunicato il Data Breach agli interessati*
Piano di Remedation	*Descrizione del piano e delle azioni puntuali di remediation che il Team Data Breach ha valutato di intraprendere per porre rimedio alla violazione e attenuarne i possibili effetti negativi*

Post incident review	
Descrizione completa della violazione	*Inserire la descrizione completa dell'incidente delle attività intraprese per gestirlo*
Cause della violazione	*Inserire il risultato della root cause analysis:* • *cosa è successo ?* • *come è successo ?* • *perché è successo ?*
Lezioni apprese	*Indicare le "lesson learned" apprese durante la gestione dell'incidente.*
Opportunità di miglioramento	*Inserire le misure da porre in essere per rendere più efficiente ed efficace la gestione dell'incidente*

Allegato C

REGIONE LAZIO

Metodologia di valutazione

della gravità di un Personal Data Breach

- documento tecnico-metodologico di supporto-

Versione 1.0

1. Premessa, Obiettivi e Definizioni

Il presente documento ha l'obiettivo di declinare la "Metodologia di valutazione delle violazioni dei dati personali" (di seguito anche la *Metodologia*) di cui il titolare del trattamento, Giunta della Regione Lazio, si avvale per valutare la "*gravità*" potenziale di un eventuale violazione dei dati personali (di seguito anche *Personal Data Breach*), ovvero la gravità della violazione per i diritti e le libertà delle persone fisiche. Tale metodologia è stata definita sulla base delle indicazioni fornite dall'**ENISA** (*European Union Agency for Network and Information Security*) all'interno del documento "*Recommendations for a methodology of the assesment of severity of personal data breaches*[6]*"*.

All'interno del documento vengono pertanto descritte le fasi della Metodologia che consentono di identificare la gravità potenziale di un determinato Personal Data Breach. Nell'ordine:

- Valutazione del Contesto di elaborazione dei dati (**CED**)[7]
- Determinazione della Facilità di Identificazione (**FI**)[8]8
- Valutazione delle Circostanze della violazione (**CV**)[9]
- Calcolo della Gravità (**CG**)

Definizioni

[6] https://www.enisa.europa.eu/publications/dbn-severity

[7] Data Processing Context (DPC): Addresses the type of the breached data, together with a number of factors linked to the overall context of processing (cfr. "Recommendations for a methodology of the assessment of severity of personal data breaches")

[8] Ease of Identification (EI): Determines how easily the identity of the individuals can be deduced from the data involved in the breach (cfr. "Recommendations for a methodology of the assessment of severity of personal data breaches")

[9] Circumstances of breach (CB): Addresses the specific circumstances of the breach, which are related to the type of the breach, including mainly the loss of security of the breached data, as well as any involved malicious intent (cfr. "Recommendations for a methodology of the assessment of severity of personal data breaches")

a) "rischio": uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità (WP 248). È la potenzialità che uno scenario, un'azione o un'attività scelta (includendo la scelta di non agire) porti a una perdita o ad un evento indesiderabile. La nozione implica che una scelta influenzi il risultato. Le stesse perdite potenziali possono anche essere chiamate "rischi";
b) "gestione dei rischi": l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi;
c) "rischio potenziale": il rischio che si potrebbe manifestare in assenza di ogni contromisura volta a mitigare il rischio stesso;
d) "rischio residuo": il rischio esistente (effettivo) dopo l'applicazione delle contromisure/delle misure volte ad attenuare il rischio;
e) rischio effettivo: il rischio effettivamente esistente, misurato in un determinato istante temporale;
f) "processo di gestione dei rischi": l'insieme delle regole, delle procedure, delle risorse (umane, tecnologiche e organizzative) e delle attività di controllo volte a identificare, misurare o valutare, monitorare, prevenire o attenuare nonché comunicare ai livelli gerarchici competenti tutti i rischi assunti o assumibili nelle diverse attività, in una logica integrata, nonchè le interrelazioni reciproche anche con l'evoluzione del contesto esterno;
g) "controllo" qualsiasi azione o insieme di azioni, (attività, procedura, blocco, limite) in grado di abbassare il livello del rischio (per raggiungere un livello che sia accettabile).

2. Approccio metodologico

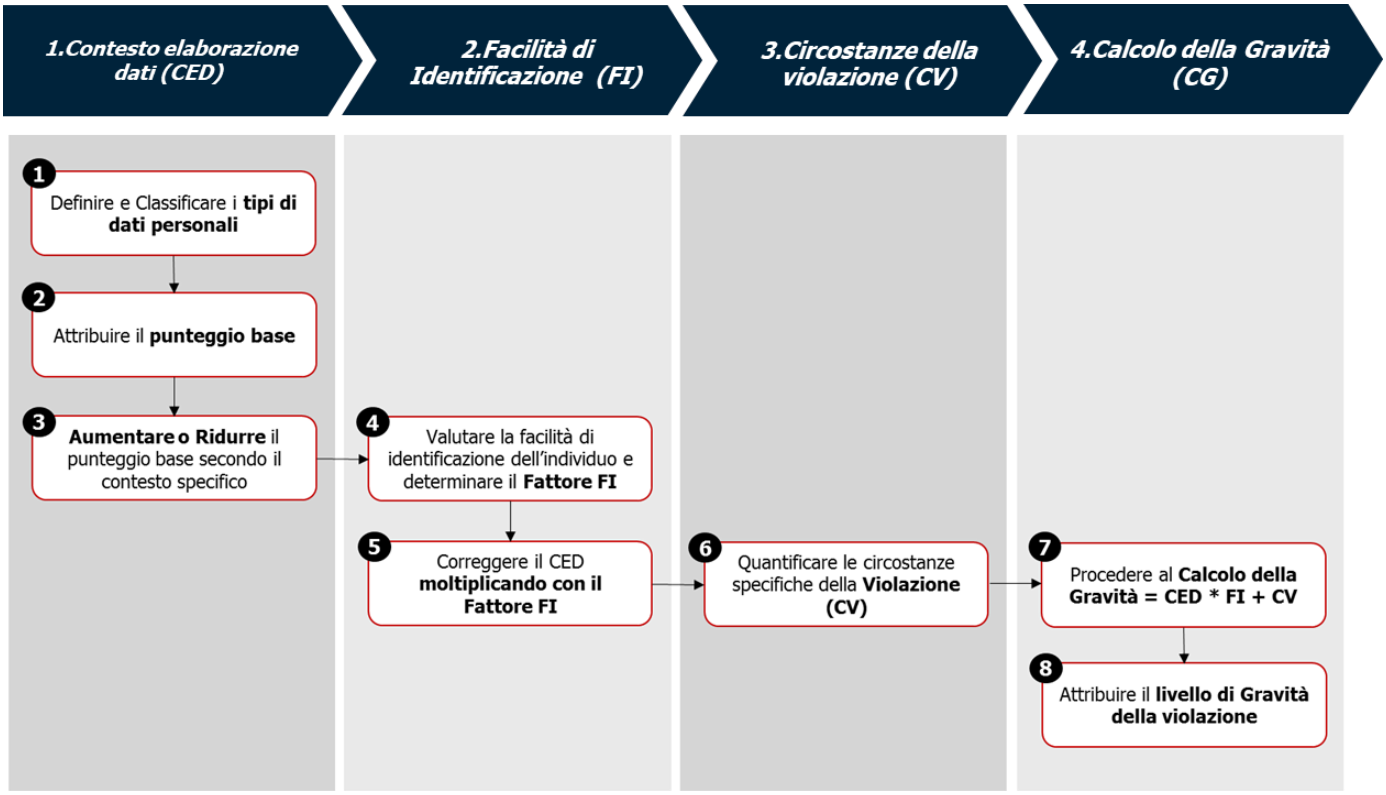
La Metodologia adottata dal titolare del trattamento, Giunta della Regione Lazio, volta a consentire di valutare/individuare il livello di rischio esistente (effettivo) in relazione ai dati personali oggetto della violazione dei dati, si basa su un approccio articolato secondo le seguenti fasi:

- **Fase 1: Valutazione del CED**: in questa fase si definisce il perimetro dei dati personali oggetto della violazione e si classificano gli stessi sulla base dell'appartenenza ad una delle categorie di dati previste dall'ENISA (Dati Ordinari, Dati Comportamentali, Dati Patrimoniali, Dati Sensibili). La classificazione comporta l'attribuzione al rischio residuo/esistente di un punteggio base (tenuto conto delle misure di sicurezza in essere/effettive) che può essere aumentato o diminuito in funzione della presenza di fattori contestuali relativi all'elaborazione dei dati;
- **Fase 2: Determinazione della FI**: si tratta della determinazione del fattore di correzione del CED. La criticità complessiva di una violazione dei dati può essere ridotta in base al valore di FI, ovvero in relazione alla facilità con cui il soggetto che entra in possesso dei dati può ricondurli o meno all'individuo a cui appartengono;
- **Fase 3: Valutazione delle CV:** in questa fase si valutano le eventuali minacce (violazione di riservatezza, violazione di integrità, violazione di disponibilità, o eventuali intenzioni malevole) causate o meno in seguito al Personal Data Breach. Il

fattore CV, laddove presente, può solo incrementare la gravità di una specifica violazione.

- **Fase 4: Calcolo della gravità:** si giunge al valore finale della gravità della violazione sulla base dei 3 precedenti elementi CED, FI, CV.

Viene riportata di seguito una rappresentazione del processo di valutazione della gravità della violazione sotto forma di diagramma di flusso:



2.1. Valutazione del contesto dell'elaborazione dei dati (CED)

Il punteggio attribuito al CED è al centro della Metodologia in quanto consente di valutare la criticità dell'insieme di dati violati in un contesto di elaborazione specifico.

Nella tabella seguente sono riassunte le attività svolte in questa fase:

Attività	Descrizione	Strumenti
1- Definire e Classificare i tipi di dati personali	Definire e classificare la tipologia di dato trattato che ha subito una violazione sulla base delle seguenti quattro macrocategorie: • Dati Ordinari; • Dati Comportamentali; • Dati Patrimoniali; • Dati Particolari.	Data Breach Report

2- Attribuire il punteggio base	Attribuisce il punteggio base secondo la **Tabella 1 – CED**	TABELLA 1 – CONTESTO ELABORAZIONE DATI (CED)
3- Aumentare o Ridurre il punteggio base secondo il contesto specifico	Aumenta o riduce il punteggio base in funzione della presenza di fattori contestuali relativi all'elaborazione dei dati (ad es. volume di dati, caratteristiche speciali dei Titolari o degli individui, inesattezza dei dati, disponibilità del dato al pubblico prima della violazione, natura del dato). Il punteggio del CED può variare da 1 a 4.	TABELLA 1 – CONTESTO ELABORAZIONE DATI (CED)

Di seguito si riporta la Tabella da utilizzare **per la valutazione del CED:**

Contesto Elaborazione Dati (CED)		**Punteggio**
Dati Ordinari	**Esempi di dati ordinari: Nome, Cognome Numero di Telefono, Indirizzo, E-mail, NDG, Fotografia, Data di nascita, Stato di famiglia, Titolo di Studi, Lavoro, Inquadramento lavorativo, etc.**	
	Punteggio Base: quando la violazione riguarda "Dati Ordinari" e il Titolare non è a conoscenza di alcun fattore aggravante.	**1**
	Il punteggio CED potrebbe essere **aumentato di 1**, ad esempio quando il volume di "Dati Ordinari" e/o le caratteristiche del Titolare sono tali da consentire l'abilitazione di determinati profili o possono essere formulate assunzioni sullo stato sociale/patrimoniale dell'individuo.	**2**
	Il punteggio CED potrebbe essere **aumentato di 2**, ad esempio quando i "Dati Ordinari" e/o le caratteristiche del Titolare possono portare a supposizioni sullo stato di salute dell'individuo, sulle preferenze sessuali, sulle convinzioni politiche o religiose.	**3**
	Il punteggio CED potrebbe essere **aumentato di 3**, ad esempio quando a causa di determinate caratteristiche dell'individuo (ad es. gruppi vulnerabili, minori), l'informazione può essere critica per la sicurezza personale o per le condizioni fisiche / psicologiche.	**4**

Contesto Elaborazione Dati (CED)	**Punteggio**

Dati Comportamentali	**Esempio di Dati Comportamentali: Abitudini, preferenze personali, interessi, vita sociale, affidabilità, spostamenti, ubicazione, etc.**	
	Punteggio Base: quando la violazione comporta "Dati Comportamentali" e il Titolare non è a conoscenza di fattori aggravanti o di diminuzione.	**2**
	Il punteggio CED potrebbe essere **diminuito di 1**, ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili pubblicamente (ad esempio la combinazione di informazioni da ricerche web).	**1**
	Il punteggio CED può essere **aumentato di 1**, ad esempio quando il volume di "Dati Comportamentali" e / o le caratteristiche del Titolare sono tali da consentire la creazione di un profilo dell'individuo, esponendo informazioni dettagliate sulla sua vita quotidiana e sulle sue abitudini.	**3**
	Il punteggio CED può essere **aumentato di 2**, ad esempio se è possibile creare un profilo basato sui dati particolari di una persona.	**4**
Dati Patrimoniali	**Esempio di Dati Patrimoniali: IBAN, Numero di conto, Saldo conto, Transaction History, Informazioni su carta di credito/debito (con o senza CVC), Dati sui mutui/prestiti, Dati Crif, Dati CR Banca d'Italia, etc.**	
	Punteggio Base: quando la violazione riguarda "Dati Patrimoniali" e il Titolare non è a conoscenza di fattori aggravanti o di diminuzione.	**3**
	Il punteggio CED potrebbe essere **diminuito di 2**, ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni patrimoniali dell'individuo (ad esempio, il fatto che una persona sia il cliente di una determinata banca senza ulteriori dettagli).	**1**
	Il punteggio CED potrebbe essere **diminuito di 1**, ad esempio quando il set di dati specifici include alcune informazioni patrimoniali ma non fornisce ancora informazioni significative sullo stato/sulla situazione patrimoniale dell'individuo (ad esempio: i numeri di conti bancari semplici senza ulteriori dettagli).	**2**

Contesto Elaborazione Dati (CED)		Punteggio
	Il punteggio CED potrebbe essere **aumentato di 1**, ad esempio quando a causa della natura e / o del volume dell'insieme di dati specifici, vengono divulgate informazioni complete patrimoniali (ad esempio: informazioni complete sulla carta di credito con il codice CVC)	4
Dati Sensibili	**Esempio di Dati Particolari/Sensibili: Dati sanitari o relativi alla salute, origine razziale/etnica, Orientamento politico e religioso, convinzioni religiose o filosofiche, appartenenza a sindacati, orientamenti sessuali, procedimento penale /condanna, dati biometrici, dati genetici.**	
	Punteggio Base: quando la violazione riguarda "Dati particolari/Sensibili" e il Titolare non è a conoscenza di alcun fattore di diminuzione.	4
	Il punteggio CED potrebbe essere **diminuito di 3**, ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni sui Dati particolari o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili pubblicamente (ad esempio la combinazione di informazioni da ricerche web).	1
	Il punteggio CED potrebbe essere **diminuito di 2**, ad esempio quando la natura dei dati può portare a ipotesi generali.	2
	Il punteggio CED potrebbe essere **diminuito di 1**, ad esempio quando la natura dei dati può portare a supposizioni su informazioni particolari.	3

TABELLA 1 – CONTESTO ELABORAZIONE DATI (CED)

Se i dati corrispondono a più di una categoria, è necessario seguire i passaggi sopra indicati per ogni categoria applicabile. In questi casi il valore CED da utilizzare corrisponde al valore più elevato di gravità tra tutte le categorie di dati trattati.

2.2. Determinazione del punteggio per la facilità di identificazione (FI)

Il punteggio del FI è il fattore di correzione del CED e consente di valutare la facilità di identificazione dell'individuo in base ai dati violati.

Nella tabella seguente sono riassunte le attività svolte in questa fase:

Attività	Descrizione	Strumenti
4- Valutare la facilità di identificazione dell'individuo e determinare il fattore FI	Valuta la **facilità di identificazione** dell'individuo ed attribuisce un punteggio secondo la **Tabella 2 - FI** definita dalla Metodologia secondo i seguenti quattro livelli: • trascurabile (0,25); • limitato (0,5); • significativo (0,75); • massimo (1). Il fattore di correzione FI può variare da 0,25 a 1. Il **punteggio più basso** viene attribuito quando la possibilità di identificare l'individuo è trascurabile, il che significa che è estremamente difficile abbinare i dati a una determinata persona, ma comunque potrebbe essere possibile con determinate condizioni. Al contrario, il **punteggio più alto** viene attribuito quando l'identificazione è possibile direttamente dai dati violati, senza alcuna ricerca specifica per determinare l'identità dell'individuo.	TABELLA 2 – FACILITÀ DI IDENTIFICAZIONE (FI)
5- Correggere il CED moltiplicando con il fattore FI	Una volta individuato il fattore di correzione, esso viene moltiplicato per il CED, al fine di determinare il punteggio iniziale della gravità della violazione dei dati.	***CED * FI***

Di seguito si riporta la Tabella da utilizzare **per la valutazione del secondo criterio (FI):**

Facilità di identificazione (FI)	Punteggio	Livello
La violazione riguarda dati identificativi o dati personali **non direttamente identificabili (ad esempio: nome/cognome molto diffuso in un paese)**	**0,25**	Trascurabile
La violazione riguarda i dati identificativi **di un individuo ma non facilmente identificabile (ad esempio: nome/cognome condiviso da poche persone in un intero paese)**	**0,5**	Limitata
La violazione riguarda dati identificativi e **rivela ulteriori informazioni di identificazione dell'individuazione (ad esempio: nome completo con l'indicazione dell'indirizzo e-mail di questa persona)**	**0,75**	Significativo
La violazione riguarda dati identificativi o dati personali **direttamente identificativi (ad esempio: nome completo con l'indicazione della data di nascita e l'indirizzo e-mail di questa persona)**	**1**	Massimo

TABELLA 2 – FACILITÀ DI IDENTIFICAZIONE (FI)

2.3. Valutazione delle Circostanze della violazione (CV)

Il punteggio del CV quantifica le **circostanze specifiche della violazione** che possono essere presenti o meno in una particolare situazione.

Nella tabella seguente sono riassunte le attività svolte in questa fase:

Attività	Descrizione	Strumenti

6- Quantificare le circostanze specifiche della violazione (CV)	Attribuisce il punteggio relativo **alle circostanze della violazione** classificate secondo le seguenti macrocategorie: • violazione di riservatezza; • violazione di disponibilità; • violazione di integrità dei dati; • eventuali intenzioni malevole. Le circostanze possono avere solo un'influenza aggiuntiva sulla gravità di una violazione. Il punteggio del CV può incrementare il punteggio precedentemente ottenuto delle gravità di 0,25 o 0,5 a seconda dei casi.	TABELLA 3 – CIRCOSTANZE DELLA VIOLAZIONE (CV)

Di seguito si riporta la tabella da utilizzare **per la valutazione del terzo indicatore (CV):**

Circostanze della violazione (CV)		Punteggio
Violazione di riservatezza	**Definizione:** La perdita di riservatezza si verifica quando le informazioni **sono accessibili da parti che non sono autorizzate o che non hanno uno scopo legittimo** di accedervi. L'entità della perdita di riservatezza varia a seconda della portata della divulgazione, ovvero il numero potenziale e il tipo di parti che possono avere accesso illecito all'informazione.	
	Esempi di dati esposti a rischi di riservatezza **senza prove che l'elaborazione illegale si è verificata:** - Un file cartaceo o un laptop si perde durante il transito; - L'attrezzatura è stata smaltita senza distruzione dei dati personali.	**0**
	Esempi di dati trasmessi verso un certo numero **di destinatari conosciuti:** - Un'e-mail con dati personali è stata inviata erroneamente a un certo numero di destinatari conosciuti; - Alcuni clienti possono accedere agli account di altri clienti in un servizio online.	**0,25**
	Esempi di dati trasmessi verso un certo numero **di destinatari sconosciuti:** - I dati sono pubblicati su una bacheca internet; - I dati vengono caricati su un sito P2P; - Un dipendente vende un CD ROM con i dati del cliente; - Un sito Web configurato in modo errato rende accessibili pubblicamente i dati Internet dagli utenti interni.	**0,5**
	Definizione: La perdita di integrità si verifica **quando le informazioni originali vengono alterate** e la sostituzione dei dati può essere pregiudizievole per l'individuo. La situazione più grave si verifica quando esistono gravi possibilità che i dati modificati siano stati utilizzati in un modo che potrebbe danneggiare l'individuo.	

Violazione di integrità	Esempi di **dati modificati** ma **senza alcun uso errato o illegale** identificato: - Le registrazioni di un database con dati personali sono state erroneamente aggiornate ma è stata effettuata una copia dell'originale prima del verificarsi della modifica.	**0**
	Esempi di dati modificati ed **eventualmente usati in modo errato o illegale ma con possibilità di recupero**: - Un dato necessario per la fornitura di un servizio online è stato modificato e l'individuo deve richiedere il servizio in modalità offline. - È stato modificato un dato importante per l'accuratezza del file di un individuo in un servizio medico online.	**0,25**
	Esempi di dati modificati ed **eventualmente usati in modo errato o illegale senza possibilità di recupero**: - Valgono gli esempi precedenti con l'aggravante che i dati originali non possono essere recuperati.	**0,5**

Circostanze della violazione (CV)		**Punteggio**
Violazione di disponibilità	**Definizione:** La **perdita di disponibilità** si verifica quando non è possibile accedere ai dati originali quando ce n'è bisogno. Può essere temporaneo (i dati sono recuperabili ma richiederà un periodo di tempo e questo può essere dannoso per l'individuo) o permanente (i dati non possono essere recuperati).	
	Esempi di dati che **possono essere recuperati senza difficoltà**: - Una copia del file è persa ma sono disponibili altre copie. - Un database è danneggiato ma può essere facilmente ricostruito da altri database.	**0**
	Esempi di **indisponibilità temporale**: - Un database è corrotto ma può essere ricostruito da altri database, sebbene sia richiesta qualche elaborazione. - Un file è perso ma l'informazione può essere fornita di nuovo dall'individuo	**0,25**
	Esempi di **indisponibilità totale** (i dati non possono essere recuperati dal controllore o dai singoli): - Un file è perso / database danneggiato, non c'è il backup di queste informazioni e non può essere fornito dall'individuo.	**0,5**
Intenzioni malevole	**Definizione:** La violazione è **dovuta a un'azione intenzionale malevola**, ad esempio al fine di causare problemi al Titolare o danneggiare gli interessati.	
	Esempi di violazione dovuta a un'azione intenzionale: - Un dipendente di un'azienda condivide intenzionalmente dati privati dai clienti in un sito pubblico di social media. - Un dipendente di un'azienda vende dati privati dei clienti a un'altra società. - Un membro di un social network invia intenzionalmente delle informazioni sugli altri membri ai propri familiari al fine di	**0,5**

	danneggiarli.	

TABELLA 3 – CIRCOSTANZE DELLA VIOLAZIONE (CV)

2.4. Calcolo della Gravità

Il punteggio finale mostra il livello di gravità di una determinata violazione, tenendo conto dell'impatto sui diritti e libertà delle persone fisiche in correlazione con le contromisure/misure di sicurezza in essere.
Nella tabella seguente sono riassunte le attività inerenti la **fase di Calcolo della gravità (CG):**

Attività	Descrizione	Strumenti
7- Procedere al Calcolo della Gravità	Calcola la gravità della violazione applicando la formula definita dalla Metodologia	Formula: ***Gravità = CED * FI + CV***
8- Definire il livello di gravità della violazione	Definisce il livello di gravità (basso, medio, alto e molto alto) secondo il risultato finale della valutazione. Il risultato viene classificato secondo quattro livelli di gravità: • Basso (punteggio finale è **inferiore a 2**) • Medio (punteggio finale è **tra 2 e 3**) • Alto (punteggio finale è **tra 3 e 4)** • Molto alto (punteggio finale è **superiore a 4**)	TABELLA 4 – LIVELLO DI GRAVITÀ

Di seguito si riporta la tabella da utilizzare **per la valutazione del livello di gravità:**

Punteggio	Livello	Descrizione
Gravità < 2	**Basso**	Gli individui non saranno interessati dalla violazione o potrebbero incontrare alcuni inconvenienti, che supereranno senza alcun problema (tempo trascorso a reinserire informazioni, fastidi, etc.).
2 ≤ Gravità < 3	**Medio**	Gli individui possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, etc.).
3 ≤ Gravità < 4	**Alto**	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in black-list, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, etc.).
4 ≤ Gravità	**Molto Alto**	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (difficoltà finanziarie, incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, etc.).

TABELLA 4 – LIVELLO DI GRAVITÀ”

Art. 41
(Disposizione di coordinamento)

1. Nel r.r. 1/2002 e successive modificazioni, ovunque ricorra l'espressione “direttore regionale competente in materia di bilancio” questa è sostituita con “Ragioniere generale”.

Art. 42
(*Entrata in vigore*)

1. Il presente regolamento entra in vigore il giorno successivo a quello della sua pubblicazione sul Bollettino Ufficiale della Regione.

Il presente regolamento regionale sarà pubblicato sul Bollettino Ufficiale della Regione. E’ fatto obbligo a chiunque spetti di osservarlo e di farlo osservare come regolamento della Regione Lazio.

Il Presidente
Francesco Rocca