Regione Lazio

Regolamenti Regionali

Regolamento regionale 27 aprile 2023, n. 3

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

(*Modifiche all'articolo 438 del regolamento regionale 6 settembre 2002, n. 1 e successive modifiche*)

1. Al comma 1 dell'articolo 438 del r.r. 1/2002 e successive modifiche dopo le parole "di seguito denominato Comitato" sono inserite le seguenti: "o CUG".

Art. 2

(*Modifiche all'articolo 439 del regolamento regionale 6 settembre 2002, n. 1 e successive modifiche*)

1. All'articolo 439 del r.r. 1/2002 e successive modifiche sono apportate le seguenti modificazioni:

a) al comma 1:

1) le parole "I membri del Comitato sono nominati dal Presidente della Regione" sono sostituite dalle seguenti: "Le/I componenti del CUG sono nominate/i con determinazione del Direttore regionale competente in materia di personale";

2) alla lettera a) le parole "dal presidente" sono sostituite dalle seguenti "dalla/dal presidente" e le parole "scelto tra gli appartenenti" sono sostituite dalle seguenti "scelta/o tra le/gli appartenenti";

3) alla lettera b) le parole "dai componenti effettivi designati" sono sostituite dalle parole "dalle/i componenti effettive/i designate/i" e le parole "dei titolari" sono sostituite dalle parole "delle/i titolari". Dopo la parola "generi" è aggiunto il seguente periodo: "Le/i componenti individuate/i dall'Amministrazione sono selezionate/i tramite una procedura comparativa trasparente a cui può partecipare tutto il personale interessato in servizio presso l'amministrazione";

4) la lettera c) è abrogata;

b) il comma 3 è sostituito dal seguente:
"3. La/Il vice presidente del Comitato sostituisce il presidente in caso di assenza o impedimento. Le modalità di designazione della/del vice presidente sono disciplinate dal regolamento che disciplina il funzionamento del Comitato stesso.";
c) al comma 5 le parole "Il componente" sono sostitute dalle seguenti: La/Il componente", la parola "ingiustificato" è sostituta dalla seguente: "ingiustificata/o" e la parola "decaduto" è sostituita dalla parola "decaduta/o".

Art. 3
(*Modifiche all'articolo 440 del regolamento regionale 6 settembre 2002, n. 1*)

1. Al comma 1 dell'articolo 440 del r.r. 1/2002 le parole "I componenti possono essere rinnovati nell'incarico per una sola volta." sono soppresse.

Art. 4
(*Modifiche all'articolo 441 del regolamento regionale 6 settembre 2002, n. 1 e successive modifiche*)

1. All'articolo 441 del r.r. 1/2002 e successive modifiche sono apportate le seguenti modificazioni:
a) al comma 1:
   1) alla lettera a) le parole "di cui alla legge 9 dicembre 1977, n. 903 e alla legge 10 aprile 1991, n. 125" sono sostituite dalle seguenti: "nel rispetto delle disposizioni normative vigenti";
   2) alla lettera b), le parole "del Consigliere" sono sostituite dalle parole "della/del Consigliera/e".
   3) alla lettera d) dopo le parole "molestie sessuali" sono inserite le seguenti: ", le discriminazioni, le violenze morali, psicologiche, il mobbing e lo straining";
   4) la lettera e), è sostituita dalla seguente:
   "e) formula proposte di piani di azioni positive, volti a favorire l'uguaglianza sostanziale sul lavoro tra uomini e donne, le condizioni di benessere lavorativo, nonché a prevenire o rimuovere situazioni di discriminazione o violenze morali, psicologiche, mobbing e disagio organizzativo all'interno dell'amministrazione;";
   5) alla lettera g) le parole "anche attraverso attività di ascolto, orientamento e di prima assistenza nei confronti del personale dipendente regionale" sono sostituite dalle seguenti: "anche inviando alla/al Consigliera/e di fiducia eventuali segnalazioni di comportamenti violenti o molesti affinché non venga consentita o tollerata nei confronti del personale alcuna azione persecutoria o discriminatoria diretta o indiretta";
   6) alla lettera h) le parole "della Presidenza del Consiglio dei Ministri del 23 maggio 2007 recante "Misure per realizzare parità e pari opportunità tra uomini e donne nelle amministrazioni pubbliche" sono sostituite dalle seguenti: "del Ministro per la Pubblica Amministrazione del 16 luglio 2019, n. 2 (Misure per promuovere le pari opportunità e rafforzare il ruolo dei Comitati Unici di Garanzia nelle Amministrazioni Pubbliche)";
b) al comma 3 le parole "pari opportunità" sono sostituite dalla parola "personale".

Art. 5

(*Modifiche all'articolo 442 del regolamento regionale 6 settembre 2002, n. 1*)

1. All'articolo 442 del r.r. 1/2002 ovunque ricorra la parola "C.P.O." è sostituita dalla seguente: "CUG";

Art. 6

(*Modifiche all'articolo 443 del regolamento regionale 6 settembre 2002, n. 1*)

1. All'articolo 443 del r.r. 1/2002 sono apportate le seguenti modifiche:
   a) il comma 2 è sostituito dal seguente:
   "2. Il funzionamento del CUG, ivi comprese le modalità di convocazione ordinaria e straordinaria dello stesso, è disciplinato da un apposito regolamento interno.";
   b) il comma 3 è abrogato;
   c) il comma 4 è abrogato.
   d) ai commi 6, 8 e 9 la parola "C.P.O." è sostituita dalla seguente: "CUG".

Art. 7

(*Modifiche all'articolo 444 del regolamento regionale 6 settembre 2002, n. 1*)

1. All' articolo 444 del r.r. 1/2002 sono apportate le seguenti modifiche:
   a) ovunque ricorra la parola "C.P.O." è sostituita dalla seguente: "CUG";
   b) al comma 2 le parole "del Dipartimento interessato" sono sostituite dalle seguenti: "della struttura interessata";
   c) al comma 3 le parole "per un massimo di due giornate l'anno e" sono soppresse.

Art. 8

(*Modifiche all'articolo 444 bis del regolamento regionale 6 settembre 2002, n. 1 e successive modifiche*)

1. Al comma 1 dell'articolo 444 bis del r.r. 1/2002 e successive modifiche sono apportate le seguenti modificazioni:
   a) alla lettera a), le parole "il Consigliere" sono sostituite dalle seguenti: "la/il Consigliera/e";
   b) dopo la lettera c) sono aggiunte le seguenti:
   "c-bis) la/il Consigliera/e regionale di parità;
   c-ter) la/il Consigliere/a di fiducia regionale;
   c-quater) lo Sportello di ascolto e il servizio di supporto psicologico per il personale regionale;
   c-quinquies) il/i disability manager;
   c-sexies) la struttura competente in materia di promozione del benessere organizzativo in favore del personale;
   c-septies) la/il Responsabile del Servizio Prevenzione e protezione;
   c-octies) altri organismi contrattualmente previsti, quali l'Organismo Paritetico per l'Innovazione (OPI).".

Art. 9

(*Modifiche all'articolo 446 del regolamento regionale 6 settembre 2002, n. 1*)

1. All'articolo 446 del r.r. 1/2002 sono apportate le seguenti modifiche:
   a) la rubrica è sostituita dalla seguente: "Codice di condotta nella lotta contro le molestie sessuali, le discriminazioni, le violenze morali, psicologiche, il mobbing e lo straining nell'ambito dell'attività lavorativa";
   b) al comma 1, le parole "nei luoghi di lavoro" sono sostituite dalle seguenti:", le discriminazioni, le violenze morali, psicologiche, il mobbing e lo straining nell'ambito dell'attività lavorativa".

Art. 10

(*Modifiche all'articolo 446 bis del regolamento regionale 6 settembre 2002, n. 1 e successive modifiche*)

1. All'articolo 446-bis del r.r. 1/2002 e successive modifiche sono apportate le seguenti modificazioni:
   a) alla rubrica la parola Consigliere" è sostituita dalla seguente "Consigliera/e".
   b) al comma 1 le parole "del Consigliere" sono sostituite dalle parole "della/del Consigliera/e"; le parole "Il Consigliere" sono sostituite dalle parole "La/Il Consigliera/e" e la parola "designato" è sostituita dalla seguente "designata/o";
   c) al comma 2 le parole "del Consigliere" sono sostituite dalle parole "della/del Consigliera/e" e le parole "Il Consigliere" sono sostituite dalle parole "La/Il Consigliera/e".
   d) al comma 3 le parole "del Consigliere" sono sostituite dalle parole "della/del Consigliera/e".

Art. 11

(*Inserimento dell'articolo 446- ter al regolamento regionale 6 settembre 2002, n. 1 e successive modifiche*)

1. Dopo l'articolo 446-bis del r.r. 1/2002 e successive modifiche è inserito il seguente:

"**Art. 446-ter**

(*Rete del benessere organizzativo*)

1. La rete del benessere organizzativo è costituita dall'insieme delle figure preposte a favorire e a promuovere il benessere organizzativo e a migliorare il clima e la qualità della convivenza nell'ambito lavorativo.

2. Oltre alle figure istituzionali di cui all'articolo 438 e all'articolo 446- bis, fanno parte della rete del benessere organizzativo:

a) la struttura regionale competente in materia di pari opportunità;

b) la struttura regionale competente in materia di promozione del benessere organizzativo per il personale regionale;

c) la/il Consigliera/e di fiducia che fornisce consulenza ed assistenza alle lavoratrici e ai lavoratori oggetto di discriminazioni, molestie, violenza e mobbing e opera nell'ambito delle procedure informali o formali adeguate alla risoluzione dei singoli casi previste nel Codice di condotta di cui all'allegato "S";

d) lo Sportello di ascolto e il Servizio di supporto psicologico in favore del personale regionale, incardinato nella struttura competente in materia di promozione del benessere organizzativo presso la direzione competente in materia di personale;
e) il/i Disability manager di cui all'allegato "S";
f) il/i medico/i competente/i individuato/i ai sensi del d. lgs. 81/2008 e successive modifiche;
g) la/il Responsabile del Servizio di Prevenzione e Protezione individuata/o ai sensi del d. lgs. 81/2008 e successive modifiche;
h) la/il Mobility manager.".

Art. 12

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

1. Al comma 1 dell'articolo 474-bis del r.r. 1/2002 e successive modificazioni, sono apportate le seguenti modifiche:
a) la lettera h) è sostituita dalla seguente:
"h) la definizione della procedura di gestione della violazione dei dati personali, di cui all'Allegato "OO" concernente la Procedura operativa per la gestione del registro delle possibili violazioni dei dati personali, ivi inclusa la relativa metodologia e valutazione di rischio, ai sensi dell'articolo 33 del RGPD, attraverso la direzione regionale competente in materia di protezione dei dati personali;";
b) dopo la lettera h) è aggiunta la seguente:
"h-bis) l'approvazione, attraverso i soggetti designati di cui all'articolo 474, comma 3, degli accordi di contitolarità, ai sensi dell'articolo 26 del RGPD, redatti sulla base dello schema "I bis" dell'allegato "NN", che prevedano le rispettive responsabilità, con particolare riferimento all'esercizio dei diritti dell'interessato, agli obblighi di rendere l'informativa ai sensi degli articoli 13 e 14 del RGPD e ai ruoli e rapporti dei contitolari con gli interessati.".

Art. 13

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

1. Al comma 1 dell'articolo 474-ter del r.r. 1/2002 e successive modificazioni, sono apportate le seguenti modifiche:
a) alla lettera p):
1) dopo le parole "comunicare al DPO" sono inserite le seguenti: "e alla direzione regionale competente in materia di protezione dei dati personali,";
2) dopo le parole "procedure regionali" sono inserite le seguenti: "di cui all'allegato "OO",";
b) dopo la lettera r) sono aggiunte le seguenti:
"r-bis) predisporre e approvare gli accordi di contitolarità, ai sensi dell'articolo 26 del RGPD, redatti sulla base dello schema "I bis" dell'allegato "NN";
r-ter) collaborare all'analisi e risoluzione dei data breach in coerenza con quanto disposto dall'allegato "OO";
r-quater) sottoscrivere e comunicare al Garante per la protezione dei dati personali, per i trattamenti di propria competenza, gli atti di notifica e di consultazione preventiva, sentito il DPO;
r-quinques) sottoscrivere e comunicare, nell'ambito della procedura regionale di gestione delle violazioni di dati personali di cui all'allegato "OO", le violazioni dei dati personali al

Garante per la protezione dei dati personali ai sensi degli articoli 33 e 34 del RGPD, sentito il DPO, per i trattamenti di propria competenza.”.

Art. 14

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

1. Alla lettera d) del comma 2 dell’articolo 474-quater del r.r. 1/2002 e successive modificazioni, dopo le parole “sistemi informativi” sono aggiunte le seguenti: “e dalla direzione competente in materia di protezione dei dati personali”.

Art. 15

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

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

a) al comma 2, dopo le parole “protezione dei dati personali in essere” sono inserite le seguenti: “, incluse le istruzioni relative alla gestione della violazione dei dati personali,”;

b) al comma 3, le parole “attraverso nome, cognome e codice fiscale,” sono soppresse.

Art. 16

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

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

a) le lettere e) ed f) sono abrogate;

b) dopo la lettera m) sono aggiunte le seguenti:

“m-bis) invia annualmente alla Giunta regionale una relazione sulle attività svolte e le principali tematiche affrontate;

m-ter) supporta il soggetto designato, competente per lo specifico trattamento, in merito agli atti di notifica e di consultazione preventiva al Garante per la protezione dei dati personali;

m-quater) supporta il soggetto designato, competente nell’ambito della procedura regionale di gestione delle violazioni di dati personali, in merito alle comunicazioni delle stesse al Garante per la protezione dei dati personali ai sensi degli articoli 33 e 34 del RGPD.”.

Art. 17

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

1. Alla lettera a), del comma 1, dell'articolo 476 del r.r. 1/2002 e successive modificazioni sono aggiunte, in fine, le seguenti parole: ". Inoltre, se necessario, supporta tecnicamente il processo di gestione delle richieste derivanti dall'esercizio dei diritti degli interessati, di cui all'allegato "MM".".

Art. 18

(Inserimento dell'articolo 476-quater nel regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

1. Dopo l'articolo 476-ter del r.r. 1/2002 e successive modificazioni è inserito il seguente:

"**Art. 476-quater**

(Procedura di gestione della violazione del dato personale "Data Breach)" inserita parentesi

1. Ai sensi degli articoli 33 e 34 del RGPD, ai fini della sicurezza del trattamento e corretta conduzione della procedura operativa per la gestione delle violazioni dei dati personali "Personal Data Breach", nonché ai fini del rispetto degli obblighi di cui al RGPD, è adottata la procedura di cui all'allegato "OO".".

Art. 19

(Modifiche all'Allegato S al regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

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

"ALLEGATO S

(rif. art. 446)

CODICE DI CONDOTTA NELLA LOTTA CONTRO LE MOLESTIE SESSUALI, LE DISCRIMINAZIONI, LE VIOLENZE MORALI, PSICOLOGICHE, IL MOBBING E LO STRAINING NELL'AMBITO DELL'ATTIVITA' LAVORATIVA

1. Ambito di applicazione

1. Il presente Codice si applica a tutto il personale sia a tempo indeterminato che determinato della Regione, nonché al personale che a qualsiasi titolo e livello organizzativo vi presti servizio ed ha ad oggetto la tutela dei lavoratori rispetto ad atti e/o fatti lesivi del proprio benessere, che si manifestino attraverso molestie sessuali, discriminazioni a qualunque titolo inflitte, violenza morale e psichica, mobbing, straining e ogni ulteriore comportamento lesivo della dignità delle lavoratrici e dei lavoratori.

2. Principi e finalità

1. Le lavoratrici ed i lavoratori hanno diritto ad un ambiente di lavoro sicuro, sereno e favorevole alle relazioni interpersonali e ad essere trattati con uguaglianza, correttezza, rispetto e dignità.
A tale fine la Regione Lazio si impegna a:
a) prevenire e/o rimuovere ogni ostacolo all'attuazione di un ambiente di lavoro favorevole alla tutela dell'inviolabilità e della dignità della persona umana;
b) garantire nei luoghi di lavoro opportuna protezione da qualsiasi atto o fatto che produca effetto pregiudizievole nei rapporti interpersonali e che leda le pari opportunità, anche indirettamente, in ragione del genere, della razza e origine etnica, della religione, delle convinzioni personali, della disabilità, dell'età, dell'orientamento sessuale;
c) garantire equità di trattamento e trasparenza delle procedure e dei criteri nell'assegnazione di incarichi e responsabilità e dei relativi livelli di retribuzione, nella promozione del personale e nell'attribuzione dei carichi di lavoro;
d) inibire e perseguire comportamenti prevaricatori o persecutori che provochino disagio e malessere psicofisico alla lavoratrice o al lavoratore;
e) monitorare i fenomeni di discriminazione, attraverso tecniche e strumenti per la rilevazione e analisi qualitative e quantitative (questionari interni, inchieste, relazioni periodiche);
f) prevenire situazioni di rischio psico-sociale legate alla condizione di disabilità, favorendo un sistema di buone pratiche miranti ad accogliere e facilitare l'inserimento nel contesto lavorativo della persona con disabilità;
g) adottare iniziative di informazione/formazione e sensibilizzazione nelle materie di cui al presente Codice, in particolare sulla gestione dei conflitti, anche specificamente dedicati a chi svolge funzioni di coordinamento e gestione del personale.
2. Le lavoratrici ed i lavoratori sono tenuti a cooperare attivamente alla promozione ed allo sviluppo di un ambiente di lavoro sicuro, ispirato a principi di correttezza, lealtà e dignità nei rapporti interpersonali.
3. La Regione contribuisce all'ottimizzazione della produttività del lavoro pubblico, migliorando l'efficienza delle prestazioni, la garanzia di un ambiente di lavoro caratterizzato dal rispetto dei principi di pari opportunità, di benessere organizzativo e dal contrasto di qualsiasi forma di discriminazione e di violenza morale o psichica, garantito dal rispetto del presente Codice.
4. Non è consentito approfittare della propria posizione gerarchica per adottare comportamenti o provvedimenti contrastanti con quanto previsto dal presente Codice.

3. Definizioni e tipologia di molestia

1. La molestia consiste in un comportamento indesiderato che, di per sé o per la sua insistenza sia percepibile, secondo ragionevolezza, come arrecante offesa alla dignità e libertà della persona che lo subisce, ovvero sia suscettibile di creare un ambiente di lavoro intimidatorio, ostile, degradante e umiliante.
2. Le molestie sessuali hanno luogo quando si verifica un atto e/o un comportamento a connotazione sessuale o comunque basato sul sesso, espresso in forma verbale, non verbale o fisica, che sia indesiderato e che arrechi, di per sé o per la sua insistenza, offesa alla dignità e libertà alla persona che lo subisce, che configuri abuso di ufficio ovvero sia suscettibile di creare un ambiente di lavoro intimidatorio, ostile e umiliante. Si intende come tale, inoltre, ogni atto o comportamento ricattatorio, mirante all'ottenimento di prestazioni sessuali in cambio del mantenimento del posto di lavoro, ovvero di vantaggi relativi alla progressione di carriera, agli orari di lavoro, agli emolumenti o altri aspetti della vita lavorativa. Rientrano, in particolare, nella tipologia delle molestie sessuali comportamenti quali:
a) richieste esplicite o implicite di prestazioni sessuali o attenzioni a sfondo sessuale non gradite o ritenute sconvenienti e offensive per chi ne è oggetto;

b) minacce derivanti dal rifiuto di accettare comportamenti ricattatori di natura sessuale, e conseguenti discriminazioni che possano incidere, direttamente o indirettamente, sulla costituzione, lo svolgimento o l'estinzione del rapporto di lavoro, nonché sulla progressione di carriera;
c) contatti fisici indesiderati;
d) apprezzamenti verbali inappropriati ed offensivi;
e) l'utilizzo di un linguaggio ambiguo, ammiccante ed allusivo, con precipuo riferimento alla sfera sessuale;
f) ogni altro atteggiamento e comportamento a sfondo sessuale lesivi della dignità della persona.

4. Definizioni e tipologie di discriminazione

1. Per discriminazione diretta si intende qualsiasi atto o comportamento per effetto dei quali una lavoratrice o un lavoratore riceve un trattamento meno favorevole rispetto a ad un'altra persona in una situazione analoga, e ciò in ragione del genere, della razza, dell'età, dello stato di salute, dell'etnia, degli orientamenti sessuali, religiosi e politici.
2. La discriminazione indiretta si configura quando una disposizione, una prassi, un criterio, un atto, un patto o un comportamento apparentemente neutri determinino, o possano determinare, per le lavoratrici e i lavoratori, una posizione di particolare svantaggio rispetto ad altri soggetti, in ragione del genere, della razza, dell'età, dello stato di salute, dell'etnia, degli orientamenti sessuali, religiosi e politici.
3. Si configura come discriminazione di cui ai punti 1) e 2) ogni trattamento pregiudizievole conseguente all'adozione di criteri che svantaggino in modo proporzionalmente maggiore i lavoratori dell'uno e dell'altro sesso e riguardino i requisiti non essenziali allo svolgimento dell'attività lavorativa, salvo che si tratti di specificazioni giustificate da una finalità legittima e da mezzi necessari ed appropriati.
4. Anche al fine di garantire il rispetto del divieto di discriminazione, sono attuate tutte le azioni positive finalizzate a rimuovere gli ostacoli che di fatto impediscono la realizzazione delle pari opportunità tra lavoratrici e lavoratori.

5. Definizioni e tipologie di violenza

1. Per violenza morale e psicologica si intende l'adozione di atteggiamenti e comportamenti alterati e disfunzionali che tendono a suscitare timore, disistima, senso di inadeguatezza ed insicurezza nella vittima e, seppur non esercitati in riferimento specifico all'attività di lavoro svolta, sono comunque perpetrati nell'ambiente di lavoro. Rientrano in tale categoria anche le condotte intrusive, le minacce e/o le molestie reiterate, finalizzate a cagionare un perdurante e grave stato di ansia o di paura, ovvero ad ingenerare un fondato timore per l'incolumità propria, o di un prossimo congiunto, o di persona al medesimo legata da relazione affettiva, ovvero da costringere il lavoratore o la lavoratrice a modificare le proprie abitudini di vita.
2. A titolo esemplificativo e non esaustivo sono ascrivibili alla violenza morale e psicologica le seguenti fattispecie:
a) minacce verbali e/o scritte, comunicazioni effettuate con toni alterati, atti persecutori;
b) ricerca ossessiva di un contatto non voluto attraverso messaggi ripetuti ed insistenti, contenenti riferimenti a carattere sessuale, sia verbali che scritti;
c) attenzioni morbose ed intrusioni indesiderate, anche con appostamenti presso la sede di lavoro.

6. Definizioni e tipologia di mobbing

1. Il mobbing è una condotta attuata nell'ambito del contesto lavorativo, sistematica e protratta nel tempo, che si sostanzia in comportamenti ostili che assumono forme di prevaricazione e persecuzione psicologica,

isolamento od esclusione dal contesto di lavoro, al fine di emarginare la lavoratrice o il lavoratore, o comunque tali da comportare un'afflizione idonea a compromettere la salute e/o la professionalità e la dignità della persona, intaccandone gravemente l'equilibrio psichico, l'autostima e riducendone la capacità lavorativa.

2. A titolo esemplificativo e non esaustivo sono ascrivibili al mobbing le seguenti condotte:
   a) trasferimenti non motivati da obiettive esigenze organizzative;
   b) ingiustificato ridimensionamento delle mansioni e/o delle competenze, ivi compreso l'impedire deliberatamente l'esecuzione del lavoro affidato;
   c) continue ed immotivate variazioni di compiti e di incarichi;
   d) assegnazione di obiettivi non pertinenti o non perseguibili o mancata assegnazione degli obiettivi con conseguente inattività forzata;
   e) prolungata attribuzione di compiti dequalificanti o di compiti esorbitanti o eccessivi, o comunque non pertinenti con il profilo professionale di appartenenza;
   f) isolamento nella forma dell'esclusione dal circuito informativo interno, della negazione deliberata di informazioni relative al lavoro, della diffusione di informazioni non corrette, incomplete, insufficienti tali da ritardare e/o impedire il normale svolgimento dell'attività di lavoro;
   g) esercizio di atti vessatori consistenti in discriminazioni in ragione del genere, dell'orientamento sessuale, politico, dello stato di disabilità, dell'etnia, della religione;
   h) critiche infondate, inappropriate ed offensive inerenti le modalità di svolgimento dell'attività lavorativa, effettuate sia verbalmente che attraverso i mezzi di comunicazione di norma utilizzati;
   i) minacce, intimidazioni, mortificazioni, insulti e offese, utilizzo di linguaggio volgare o osceno ed atteggiamenti palesemente ostili;
   l) esercizio esasperato e non giustificato di forme di controllo.
3. Lo straining, a differenza del mobbing, è caratterizzato dalla mancanza di frequenza significativa di azioni ostili e ostative, che, pur essendo sporadiche e talvolta circoscritte, comportano un grave disagio in ambito lavorativo e i cui effetti sono duraturi nel tempo.

7. Diritto/dovere di collaborazione

1. Le lavoratrici e i lavoratori hanno il diritto/dovere di contribuire ad assicurare un ambiente di lavoro in cui venga rispettata la dignità delle persone.
2. Il personale con funzione dirigenziale ha il dovere di promuovere le condizioni che consentono a ciascuna lavoratrice e a ciascun lavoratore di operare secondo integrità, onestà, professionalità e, in particolare, di prevenire e contrastare il verificarsi di atti e comportamenti riconducibili a discriminazioni, molestie sessuali, violenza morale o psicologica, stalking, mobbing e straining, lesivi della dignità della persona.

8. Consigliera o consigliere di fiducia

1. La figura del Consigliere o della Consigliera di fiducia, prevista dalla Raccomandazione della Commissione europea 92/131/CEE relativa alla Tutela della dignità delle donne e degli uomini sul lavoro e dalla Risoluzione A3-0043/94 del Parlamento europeo, è incaricata di fornire consulenza ed assistenza alle lavoratrici e ai lavoratori oggetto di discriminazioni, molestie, violenza e mobbing e di avviare le procedure informali o formali adeguate alla risoluzione dei singoli casi.
2. La/il Consigliera/e di fiducia è una figura istituzionale esterna, neutrale ed esercita la sua funzione nella più ampia autonomia e nell'assoluto rispetto della dignità di tutti i soggetti coinvolti, garantendo, in particolare, la totale riservatezza delle notizie e dei fatti di cui viene a conoscenza.

3. La/il Consigliera/e di fiducia è individuata/o tra i soggetti esterni all'amministrazione in possesso di idonee competenze e capacità professionali, attraverso un'apposita procedura di valutazione comparativa per titoli e colloquio. L'incarico è conferito per la durata massima di ventiquattro mesi.
4. Ai fini del conferimento dell'incarico, si tiene conto del percorso professionale-culturale dei candidati con preferenza per l'ambito socio/psicologico e/o giuslavoristico. Si tiene conto, altresì, di ogni esperienza significativa, debitamente attestata, maturata in ambito nazionale o internazionale, sulla tematica delle discriminazioni nell'ambito del rapporto di lavoro e del disagio lavorativo con preferenza per la specifica materia del mobbing e delle molestie sessuali.
5. Il/la Consigliera/e di fiducia gestisce lo "Sportello di ascolto", struttura di accoglienza per le lavoratrici e i lavoratori della Regione Lazio, a cui si può rivolgere il personale interessato dalle fattispecie regolamentate dal presente Codice. Nel caso in cui lo ritenga necessario, e previo consenso della lavoratrice o del lavoratore, il/la Consigliere/a di fiducia può interagire con il medico competente e/o con il Responsabile del Servizio di Prevenzione e Protezione, e/o con il Servizio di Supporto Psicologico per l'eventuale seguito di competenza.
6. Rientra altresì tra i compiti della/del Consigliera/e di fiducia suggerire al CUG ed all'Area della Direzione regionale competente in materia di benessere del personale, azioni opportune volte a promuovere un clima organizzativo idoneo ad assicurare la pari dignità e libertà delle persone all'interno della Regione, nonché partecipare attivamente alle iniziative di informazione e formazione promosse dalla Regione stessa sui temi di cui al presente Codice. La/il Consigliera/e di fiducia ha, inoltre, un ruolo centrale nell'attuazione del Codice di condotta adottato dal datore di lavoro, valuta i diversi casi e fornisce consulenza e assistenza predisponendo idonee strategie di intervento.
7. La/il Consigliera/e di fiducia ha diritto di accesso agli atti relativi al caso trattato e a ricevere tutte le informazioni necessarie per la definizione del medesimo.
8. La Regione fornisce alla/al Consigliera/e di fiducia gli strumenti necessari all'adempimento delle proprie funzioni.
9. La/il Consigliera/e di fiducia relaziona al CUG, con cadenza annuale in merito all'attività svolta, avendo riguardo di omettere i dati identificativi dei soggetti coinvolti per garantirne la riservatezza. Nella relazione devono essere illustrati i casi trattati, i casi risolti, i casi oggetto di rinuncia, i casi ancora in corso, le misure adottate, l'esito, e deve essere fornita ogni ulteriore informazione utile. Copia della relazione presentata dalla/dal Consigliera/e di fiducia viene allegata alla relazione che il CUG elabora annualmente in merito all'attività svolta, da presentare al Direttore della Direzione regionale competente in materia di personale. La/il Consigliera/e di fiducia provvede altresì, con cadenza semestrale, all'aggiornamento della relazione, qualora necessario ai fini dell'esatta quantificazione dei dati relativi alle segnalazioni ricevute. Il nominativo ed i contatti relativi alla/al Consigliera/e di fiducia sono pubblicati sul sito intranet regionale e sul canale tematico del CUG.

9. Sportello d'Ascolto e Servizio di Supporto Psicologico

1. Il "Servizio d'ascolto per la prevenzione del mobbing e delle discriminazioni" della Regione, previsto per la prima volta nell'ambito del Piano Triennale di Azioni Positive 2015-2017, è stato istituito con atto del Direttore regionale competente in materia di personale.
2. Il servizio di cui al punto 1 si pone l'obiettivo di offrire al personale regionale un luogo di riferimento per la prevenzione del mobbing e delle discriminazioni, in cui i casi di violazione del Codice possano essere liberamente trattati, nel rispetto della normativa sulla privacy, al fine di individuare soluzioni idonee al superamento del disagio lavorativo.
3. Le attività dello Sportello di Ascolto sono gestite dalla/dal Consigliera/e di fiducia al fine di favorire il superamento delle situazioni di disagio e di ripristinare il benessere organizzativo negli ambienti di lavoro.

4. Con atto del Direttore regionale competente in materia di personale è strutturata l'attività del "Servizio di supporto psicologico" nell'ambito dello Sportello d'Ascolto, per la tutela della salute psicofisica e personale delle dipendenti e dei dipendenti regionali.
5. Il Servizio di Supporto Psicologico è incardinato presso l'apposita Area della Direzione regionale competente in materia di benessere del personale, struttura competente in ordine alla gestione di tutte le attività e le iniziative connesse alla promozione della salute organizzativa, attraverso la realizzazione di politiche, iniziative e programmi, anche in collaborazione con gli organismi istituzionali interni ed esterni, volti all'accrescimento del benessere organizzativo e della qualità della convivenza lavorativa.
6. Il Servizio di Supporto Psicologico:
   a) offre, consulenza psicologica qualificata al personale della Regione Lazio, per mitigare lo stress dovuto a mutamenti delle proprie condizioni di lavoro e/o familiari, al fine di poter attenuare conseguenti disagi emotivi;
   b) è gestito da un team costituito da personale interno in possesso della laurea in psicologia e di iscrizione all'albo degli psicologi;
   c) svolge un'attività di coordinamento con la/il Consigliera/e di fiducia qualora nel corso dei colloqui, acquisito il consenso del dipendente, dovessero emergere questioni di competenza di quest'ultima/o;
   d) si relaziona con la Direzione regionale competente in materia di personale fornendo periodicamente dati numerici aggregati in ordine al numero di accessi al servizio ed alla tipologia delle problematiche emerse, nonché eventuali ulteriori input rispetto alla generalità delle questioni prospettate, al fine di valutare eventuali iniziative e/o interventi da attuare, quali, a titolo esemplificativo, percorsi formativi, a beneficio di tutto il personale.

10. Strumenti di tutela

1. Il lavoratore o la lavoratrice che ritiene di aver subito comportamenti pregiudizievoli, riconducibili alle fattispecie di cui ai paragrafi 3, 4, 5 e 6 del presente Codice può attivare a propria tutela le seguenti procedure:
   a) la procedura informale di cui al paragrafo 11;
   b) la procedura formale di cui al paragrafo 12.

11. Procedura informale

1. La/il Consigliera/e di fiducia, attraverso lo Sportello di Ascolto, agisce su segnalazione del lavoratore o della lavoratrice che denunci comportamenti pregiudizievoli, secondo modalità e tempistiche idonee a determinare l'interruzione dei comportamenti indesiderati ed a favorire tempestivamente la risoluzione del disagio, previa acquisizione dell'espresso consenso da parte del/la interessato/a.
2. A tutela del/la interessato/a, la/il Consigliera/e di fiducia provvede all'attivazione di una procedura informale, nel corso della quale:
   a) convoca il soggetto individuato/segnalato quale autore/autrice del comportamento lesivo, al fine di reperire informazioni in forma riservata;
   b) acquisisce eventuali testimonianze sui fatti segnalati ed accede agli atti inerenti al caso in esame;
   c) avvia un tentativo di conciliazione tra le parti;
   d) suggerisce l'adozione di opportune azioni idonee a ripristinare il benessere organizzativo ed a favorire un ambiente di lavoro improntato ai principi di cui al presente Codice;
   e) richiede, ove necessario, al/la Dirigente della struttura ove la violazione si è verificata, l'adozione di idonee misure correttive. Nei casi di particolare gravità, la/il Consigliera/e di fiducia può proporre che la parte lesa sia assegnata, anche in via temporanea, ad altro ufficio o ad altra sede, previo l'assenso dell'interessata/o ed il nulla osta al trasferimento;

3. Restano salve le specifiche disposizioni normative vigenti in materia di procedimenti e sanzioni disciplinari e penali, alle quali si rinvia, ivi comprese le disposizioni inerenti le sanzioni a carico di coloro che denuncino il falso nei casi di molestie, violenze, atti discriminatori o episodi di mobbing.
4. Una volta attivata la procedura informale, la stessa può essere interrotta in qualunque momento, qualora la persona lesa ritiri la propria segnalazione.
5. In caso di accertata infondatezza della segnalazione, la procedura viene conclusa.
6. La procedura informale deve concludersi in tempi ragionevolmente brevi e comunque non oltre novanta giorni dall'avvenuta segnalazione del caso.
7. La/il Consigliera/e di fiducia redige una relazione in merito all'attività conciliativa svolta ai sensi del paragrafo 8, punto 8, del Codice, assicurando adeguata tutela della riservatezza dei soggetti coinvolti.
8. Qualora, all'esito dell'esperimento della procedura di cui al presente paragrafo non sia possibile pervenire alla risoluzione della questione, la/il Consigliera/e di fiducia può suggerire l'attivazione della procedura formale di cui al paragrafo 12.

12 Procedura formale

1. La/il Consigliera/e di fiducia avvia la procedura formale su richiesta del/la dipendente, acquisito il suo preventivo ed espresso consenso, previa presentazione di un atto formale di denuncia al/la dirigente o al responsabile della struttura di appartenenza, il/la quale è tenuto/a entro e non oltre trenta giorni a trasmettere gli atti alla struttura regionale competente in materia di procedimenti disciplinari, fatto salvo il ricorso ad ogni altra forma di tutela giurisdizionale.
2. Qualora il/la presunto/a autore/autrice di molestie sessuali sia il/la dirigente della struttura di appartenenza, la denuncia è inoltrata direttamente alla struttura regionale competente in materia di procedimenti disciplinari.
3. Nel corso degli accertamenti è assicurata l'assoluta riservatezza dei soggetti coinvolti.
4. Nel rispetto dei principi che informano il decreto legislativo 11 aprile 2006, n. 198 (Codice delle pari opportunità tra uomo e donna, a norma dell'articolo 6 della legge 28 novembre 2005, n. 246) e successive modifiche, qualora l'amministrazione, nel corso del procedimento disciplinare, ritenga fondati i fatti, adotta, ove lo ritenga opportuno, d'intesa con le organizzazioni sindacali e sentita la consigliera/il consigliere di fiducia, le misure organizzative ritenute, di volta in volta, necessarie ai fini della cessazione immediata dei comportamenti lesivi e del ripristino di un ambiente di lavoro in cui sia assicurata l'inviolabilità della persona.
5. In armonia con i principi che informano il d.lgs. 198/2006 e successive modifiche e nel caso in cui l'amministrazione nel corso del procedimento disciplinare ritenga fondati i fatti, il/la denunciante ha la possibilità di optare tra la richiesta di trasferimento in altra sede di lavoro o il permanere nella propria sede.
6. Nei procedimenti disciplinari attinenti alle materie di cui al presente Codice, la struttura regionale competente per i procedimenti disciplinari può, ove lo ritenga opportuno, ascoltare la/il Consigliera/e di fiducia come persona informata dei fatti.
7. Nel rispetto dei principi che informano il d.lgs. 198/2006 e successive modifiche, qualora l'amministrazione nel corso del procedimento disciplinare non ritenga fondati i fatti, può adottare, su richiesta di uno o di entrambi gli interessati, eventualmente con l'assistenza delle organizzazioni sindacali, provvedimenti di trasferimento in via temporanea, in attesa della conclusione del procedimento disciplinare, al solo fine di agevolare il recupero di un pacifico clima organizzativo.
8. Anche nelle more del procedimento disciplinare, è in ogni caso assicurata adeguata tutela alla persona offesa da forme di ritorsione o penalizzazione e vigilanza attiva al fine di verificare la sussistenza di comportamenti lesivi. A tal fine, può disporsi l'assegnazione di uno dei soggetti coinvolti ad altro ufficio rispetto a quello di appartenenza.

9. Qualora, a seguito di istruttoria esperita in contraddittorio con i soggetti coinvolti e nel rispetto del principio di riservatezza, la denuncia sia ritenuta fondata, si applicano adeguate sanzioni.
10. Restano salve le specifiche disposizioni normative vigenti in materia di procedimenti e sanzioni disciplinari e penali, alle quali si rinvia, ivi comprese le disposizioni inerenti le sanzioni a carico di coloro che denuncino il falso nei casi di molestie, violenze, atti discriminatori o episodi di mobbing.

13. Altre figure a tutela dei lavoratori in caso di discriminazione, malessere organizzativo, molestie, mobbing e straining

1. La Consigliera di Parità, nell'esercizio delle funzioni attribuite, è pubblico ufficiale ed ha l'obbligo di segnalazione all'autorità giudiziaria dei reati di cui viene a conoscenza durante lo svolgimento delle proprie funzioni. È quindi organo promotore di giustizia nei giudizi antidiscriminatori. Si occupa in particolare di discriminazione di genere e di molestie e mobbing, sempre nell'ambito delle discriminazioni di genere. Nelle situazioni disagiate esercita funzioni relative al contenzioso in sede conciliativa e giudiziale;
La Consigliera Regionale di Parità interviene in presenza di squilibrio di genere sul lavoro. Contrasta le discriminazioni di genere, le molestie ed il mobbing sul lavoro, di carattere collettivo.
Su mandato della singola lavoratrice o del singolo lavoratore che lamenti una discriminazione, come primo passo, promuove un tentativo di conciliazione con il datore di lavoro; in caso di mancata conciliazione può ricorrere al Giudice del Lavoro; in ultima istanza può agire in giudizio su delega della lavoratrice o del lavoratore.
2. Il Comitato Unico di Garanzia, per le pari opportunità, la valorizzazione del benessere di chi lavora e contro le discriminazioni, è garante di un ambiente di lavoro rispettoso dei principi di pari opportunità, benessere organizzativo, di contrasto a qualsiasi forma di violenza morale e psichica per i lavoratori e di discriminazione, diretta e indiretta, relativa al genere, all'età, all'orientamento sessuale, alla razza, all'origine etnica, alla disabilità, alla religione e alla lingua. Esercita compiti propositivi, consultivi e di verifica. Il CUG, in virtù della sua più ampia funzione politico/programmatica, non si occupa dei singoli casi specifici; tuttavia, è tenuto a dare riscontro alle richieste ricevute, segnalando le modalità d'inoltro delle segnalazioni agli uffici competenti.
3. Il Disability manager è una figura chiamata ad agevolare il processo di cambiamento nell'organizzazione regionale, orientato alla valorizzazione, all'autodeterminazione e all'autonomia delle persone con disabilità. Il ruolo del Disability manager è esercitato da dipendenti regionali individuati dal Direttore della Direzione regionale competente in materia di personale, in possesso di specifici requisiti professionali e adeguatamente formati.

14. Riservatezza

1. Tutte le persone interessate dalla trattazione dei casi di cui al presente Codice, sono tenute alla riservatezza in merito a persone, fatti e notizie di cui vengano a conoscenza nel corso della trattazione degli stessi.
2. Durante il procedimento di accertamento, e dopo la sua conclusione, le parti coinvolte hanno il diritto all'assoluta riservatezza ed in particolare a che non si dia diffusione delle proprie generalità o di altre informazioni che ne favoriscano una chiara identificazione.
3. La lavoratrice o il lavoratore che abbia subito atti o comportamenti lesivi della propria dignità, ha diritto a richiedere che venga omesso il proprio nome in ogni documento, attinente alle questioni di cui al presente Codice, che sia soggetto a pubblicazione.

15. Azioni positive, formazione e informazione

1. La Regione, nell'ambito della programmazione triennale in materia di formazione del personale dirigente e di comparto, tenuto conto delle proposte contenute nella sezione del Piano integrato di attività e organizzazione (PIAO) dedicata al Piano delle Azioni Positive (PAP) e di eventuali ulteriori iniziative formulate dal/dalla Consigliere/a di fiducia, eroga interventi formativi specifici nelle materie trattate dal presente Codice, al fine di prevenire il verificarsi di comportamenti in violazione dello stesso.
2. I dirigenti promuovono e diffondono la cultura del rispetto della persona, con finalità di prevenzione dei comportamenti lesivi sul posto di lavoro.
3. L'amministrazione promuove, d'intesa con le organizzazioni sindacali, la diffusione del Codice di condotta con tutti i mezzi di informazione disponibili ed i canali in uso, al fine di favorirne la massima conoscenza presso il personale che, a qualsiasi titolo e livello organizzativo, vi presta servizio. Inoltre, favorisce attività di sensibilizzazione dirette ad accrescere la consapevolezza sull'importanza della prevenzione e del contrasto dei comportamenti lesivi della dignità ed integrità delle lavoratrici e dei lavoratori.
4. L'amministrazione regionale monitora l'efficace applicazione del presente Codice di condotta ai fini della prevenzione e della lotta contro le molestie sessuali.

16. Verifiche e pubblicazione

1. La Regione si impegna a verificare periodicamente gli effetti dell'adozione del presente Codice, provvedendo alle eventuali modifiche o integrazioni che si rendano necessarie, anche a seguito dell'emanazione di nuove disposizioni normative nazionali o europee in materia.
2. Il Codice è pubblicato sul sito istituzionale della Regione e sul sito intranet ed è fatto obbligo, a chiunque spetti, di osservarlo e di farlo osservare.".

Art. 20

(Sostituzione dello schema "D" nell'allegato "NN" al r.r.1/2002 e successive modificazioni)

1. Lo schema "D" dell'allegato "NN" del r.r. 1/2002 e successive modificazioni è sostituito dal seguente:

SCHEMA D
INFORMATIVA DATI PERSONALI
PER IL PERSONALE IN SERVIZIO

"**Informativa per il personale in servizio**"
(Regolamento (UE) 2016/679 "RGPD")

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) ed il decreto legislativo 196/2003 e successive modificazioni, stabiliscono che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, al diritto e alla protezione dei dati personali.
Per questi motivi la Giunta Regionale del Lazio (di seguito anche la "giunta regionale", la "Regione" o il "Titolare") in qualità di Titolare del trattamento di dati personali effettuato per finalità di gestione

del personale, nell'ambito delle proprie competenze, è tenuta a fornirLe, ai sensi dell'articolo 13 del RGPD le seguenti informazioni, in relazione ai trattamenti dei dati personali che La riguardano.

1. BASE GIURIDICA E FINALITÀ DEL TRATTAMENTO

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni previste dall'articolo 6, paragrafo 1, lettere da a) ad f) del RGPD:

a) "l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità" (ove applicabile, per le finalità elencate di seguito);

b) "il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso";

c) "il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" (ad esempio adempimenti fiscali, previdenza sociale);

d) "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento";

e) "il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali" (ad esempio per assicurare la sicurezza dei dati e dei sistemi informatici in uso, per la salvaguardia del patrimonio dell'Ente).

Inoltre, eventuale trattamento di dati particolari sarà svolto sulla base dell'articolo 9 paragrafo 2 lettera b): "il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato.".

I dati personali oggetto del trattamento saranno trattati per le sole finalità strettamente connesse e strumentali alla nascita e gestione del rapporto contrattuale di lavoro nei limiti stabiliti da espressa disposizione di legge e regolamenti o da accordi sindacali.

In particolare, i dati da Lei forniti possono riguardare dati anagrafici e fiscali Suoi e dei Suoi eventuali familiari a carico o comunque componenti il Suo nucleo familiare, nonché eventuali diversi beneficiari di programmi assicurativi; gli estremi del suo conto corrente bancario, i dati professionali (competenze acquisite prima o nel corso del rapporto di lavoro con la Giunta di Regione Lazio, ruoli svolti).

Tali dati saranno trattati per le finalità di seguito riportate:

- finalità connesse e strumentali alla gestione ed all'esecuzione del contratto di lavoro, quali l'assunzione, la costituzione e successiva gestione del rapporto di lavoro, la corretta quantificazione della retribuzione, nonché l'eventuale cessazione del rapporto; la base giuridica del trattamento è l'esecuzione del contratto di cui l'interessato è parte;
- assolvere agli obblighi di legge, normativi e regolamentari, CCNL o Accordi collettivi anche aziendali; la base giuridica del trattamento è la gestione del contratto con l'interessato e anche l'obbligo legale al quale è soggetto il Titolare del trattamento;
- comunicazioni a enti regolatori anche non comunitari; la base giuridica del trattamento è l'obbligo legale al quale è soggetto il Titolare del trattamento;
- pubblicazione sul sito Internet ed eventuali riviste aziendali delle Sue immagini (foto o riprese audio-video) in occasione di attività di particolare interesse quali feste, manifestazioni, eventi e riunioni; la base giuridica del trattamento è costituita dal consenso dell'interessato;
- pubblicazione della sua immagine sulla intranet aziendale per la creazione di organigrammi e diagrammi del personale dell'azienda da utilizzare all'interno della Regione o all'esterno per presentazioni a soggetti terzi, consulenti fornitori di servizi, o in occasione di riunioni, incontri

seminari conferenze che hanno attinenza alle attività della Regione o abbiano finalità didattiche o educative anche con eventuale partecipazione del pubblico; su riviste o brochure informative; la base giuridica del trattamento è il consenso dell'interessato;
- verifica del corretto adempimento degli obblighi professionali da parte del lavoratore e del corretto uso degli strumenti aziendali da parte dello stesso (come da normativa interna). I dati raccolti potranno essere utilizzati per fini disciplinari e difensivi nel rispetto di quanto disposto dal Regolamento (UE) 2016/679 e della legge 300/1970; la base giuridica del trattamento è l'adempimento di un compito di interesse pubblico;
- far valere o difendere un diritto del Titolare del trattamento in fase giudiziaria o nelle fasi propedeutiche alla sua eventuale instaurazione, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempreché, qualora i dati siano idonei a rivelare lo stato di salute e la vita sessuale, il diritto da far valere o difendere sia di rango almeno pari a quello dell'interessato; la base giuridica del trattamento è l'adempimento di un compito di interesse pubblico;
- finalità connesse alla gestione di corsi di formazione previsti nel Piano formativo regionale inserito nel PIAO per il personale della Giunta regionale erogati direttamente dalla Regione o da parte di soggetti terzi; attività di formazione/informazione professionale con conseguenti test valutativi anche in osservanza di disposizioni normative (ad esempio in materia di sicurezza sul lavoro, incidenti rilevanti, responsabilità amministrativa degli enti); la base giuridica del trattamento è la gestione del contratto di cui l'interessato è parte;
- finalità connesse all'attivazione dell'assistenza sanitaria integrativa in favore del personale regionale prevista dall'articolo 11 della legge regionale 14/08/2017, n. 9; la base giuridica del trattamento è la gestione del contratto di cui l'interessato è parte;
- finalità connesse alla gestione degli accordi di lavoro agile, ivi compresa la comunicazione dei dati attraverso i portali del Ministero del Lavoro; la base giuridica del trattamento è la gestione del contratto di cui l'interessato è parte;
- finalità di sicurezza delle persone, salvaguardia della vita, sicurezza e tutela dei beni aziendali e controllo degli accessi, compresa la gestione dei sistemi di videosorveglianza installati negli stabilimenti; la base giuridica del trattamento è la gestione del contratto, il legittimo interesse del Titolare, nonché l'obbligo per il Titolare di attuare gli adempimenti previsti dalla normativa vigente per garantire la sicurezza nelle sedi di lavoro;
- per scopi identificativi e relativa realizzazione del badge aziendale; la base giuridica del trattamento è la gestione del contratto con l'interessato o il rispetto di un obbligo normativo;
- finalità volte a garantire la funzionalità e il corretto impiego dei mezzi informatici (ad esempio per rilevare anomalie o per manutenzioni), nonché finalità connesse a ragioni organizzative e di sicurezza e protezione dei dati aziendali. Per il perseguimento di tali finalità, sempre nel pieno rispetto del divieto di controllo a distanza del lavoratore ai sensi dell' articolo 4 della L. n. 300/1970 e successive modifiche, il Titolare potrebbe venire a conoscenza dei Suoi dati personali anche di natura particolare presenti nella posta elettronica e/o tracciati dalla navigazione dei siti internet; la base giuridica del trattamento è l'adempimento di un compito di interesse pubblico;
- trattamento e comunicazione a terzi (professionisti e aziende in funzione del servizio richiesto) dei dati particolari (relativi alla salute o a opinione sindacale) finalizzato alla prestazione di servizi richiesti dall'interessato e società per usufruire di benefit aziendali; la base giuridica del trattamento è il consenso dell'interessato;
- pubblicazione di interviste, interventi che Lei terrà quale relatore in occasione di convegni e attività organizzate dalla Regione Lazio, fotografie o riprese acquisite in occasione di convegni e attività ludiche aziendali saranno pubblicati per promuovere i servizi dell'ente; la base giuridica del trattamento è il consenso dell'interessato;

- per assolvere agli obblighi della Regione (in materia fiscale, di previdenza ed assistenza, di igiene e sicurezza del lavoro, di tutela della salute, ivi comprese le finalità connesse alle procedure per far fronte ad emergenze sanitarie quali la prevenzione da SARS- Covid 19, nonché di sicurezza sociale); la base giuridica del trattamento è la gestione del contratto con l'interessato o il rispetto di un obbligo normativo;
- per la gestione ed esecuzione del contratto di lavoro, anche sotto il profilo economico ed amministrativo, ivi compresi gli adempimenti connessi all'organizzazione di eventuali missioni/trasferte connesse ad attività lavorative; la base giuridica del trattamento è la gestione del contratto con l'interessato o il rispetto di un obbligo normativo;
- finalità connesse alla rilevazione e gestione delle presenze/assenze, ivi compresa la gestione dell'assenza per malattia e per infortunio; la base giuridica del trattamento è l'esecuzione di un contratto di cui l'interessato è parte e il rispetto di un obbligo normativo;
- finalità connesse alla concessione di permessi, congedi (maternità e paternità, per benefici di cui alla Legge 104/1992 e successive modifiche, per studio, ecc.) e aspettative varie (ad esempio per motivi personali, familiari, per cariche politiche, sindacali); la base giuridica del trattamento è la gestione del contratto con l'interessato o il rispetto di un obbligo normativo;
- finalità connesse a procedure selettive interne (progressioni orizzontali) e procedure di mobilità; la base giuridica del trattamento è la gestione del contratto con l'interessato o il rispetto di un obbligo normativo;
- finalità connesse a convenzioni con altri enti locali per l'utilizzo di personale a tempo parziale; trasferimenti, in entrata e in uscita, di personale per mobilità esterna, ovvero per comando; la base giuridica del trattamento è la gestione del contratto con l'interessato o il rispetto di un obbligo normativo;
- per le finalità previste dal d.lgs. 14 marzo 2013, n. 33 e successive modifiche con riferimento agli obblighi di pubblicazione sul Bollettino Ufficiale della Regione Lazio e/o sul sito istituzionale, ivi comprese le finalità di cui all'articolo 18 del citato decreto, con riferimento all'elenco degli incarichi conferiti o autorizzati a ciascuno dei dipendenti, con l'indicazione della durata e del compenso spettante per ogni incarico; la base giuridica del trattamento è il rispetto di un obbligo normativo;
- per le finalità previste dal D.P.R. 28 dicembre 2000, n. 445 e successive modifiche, con riferimento alle verifiche delle dichiarazioni sostitutive, nonché per soddisfare istanze di accesso agli atti ai sensi della L. 241/1990 e successive modifiche, Foia e accesso civico generalizzato; la base giuridica del trattamento è il rispetto di un obbligo normativo e l'adempimento di un compito connesso all'esercizio di pubblici poteri di cui è investito il titolare.

Per l'attivazione e gestione dei rapporti con la Regione è necessario e, in alcuni casi, obbligatorio ai sensi della normativa vigente[1], raccogliere ed utilizzare alcuni dati personali dell'interessato o di persone a lui legate (quali i familiari), senza necessità di acquisire il consenso dell'interessato. In assenza di tali dati la Regione non sarebbe in grado di gestire i rapporti con l'interessato o fornire eventuali servizi richiesti.

Nell'ambito delle predette attività, di regola, la Giunta regionale non tratta categorie particolari di dati personali (dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona). Tuttavia, non è escluso che specifiche operazioni (quali versamenti di quote associative, trattenute dello stipendio), possano determinare un'occasionale conoscenza di informazioni idonee a rivelare tali dati, che saranno necessariamente utilizzati solo per l'esecuzione

[1] Come, ad esempio, gli obblighi di identificazione delle persone fisiche e di registrazione dei relativi dati ai sensi della normativa in materia di sicurezza sul posto di lavoro, ecc.

di quanto richiesto dall'interessato. Per il loro trattamento, inoltre, la normativa sulla protezione dei dati personali richiede comunque una manifestazione di consenso esplicito da parte dell'interessato stesso. Si fa presente che, comunque, in occasione delle operazioni di trattamento dei Suoi dati personali, la Giunta della Regione Lazio potrebbe venire a conoscenza di dati che la normativa definisce "Categorie particolari di dati personali" (articolo 9 del RGPD), o di dati di cui all'articolo 10 del RGPD, in quanto relativi a condanne penali e reati od a connesse misure di sicurezza. Tali dati saranno trattati con la massima riservatezza e per le sole finalità previste dalla legge e dal CCNL vigente.
I dati relativi all'adesione ad un sindacato potranno essere comunicati alle organizzazioni sindacali o di categoria per il controllo delle ritenute solo con riferimento ai propri iscritti. I dati relativi all'adesione ad un partito politico o alle convinzioni religiose saranno trattati esclusivamente per le finalità inerenti alla gestione del rapporto di lavoro, nei limiti previsti dalla normativa vigente.
Sono inoltre presenti eventuali dati personali relativi a Suoi familiari, di natura anche particolare, da Lei trasmessi alla Regione Lazio in loro nome e per conto, necessari per ottemperare ad adempimenti di legge, regolamenti e contrattuali (ad esempio dichiarazione dei redditi, detrazioni fiscali, assegni familiari, permessi per malattia figli, permessi per assistenza a portatori di handicap, certificazioni di matrimonio).
Si precisa, inoltre che la Giunta regionale, in qualità di Titolare degli strumenti informatici e dei dati ivi contenuti e/o trattati dagli utenti, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:
- tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;
- evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo;
- verificare la funzionalità del sistema e degli strumenti informativi.

Per ciò che concerne la conservazione dei dati relativi agli accessi e all'utilizzo degli strumenti messi a disposizione dal datore di lavoro per finalità esclusivamente legate allo svolgimento dei compiti di lavoro si rimanda all'apposito disciplinare allegato al regolamento regionale n.1/2002 e successive modifiche.
Si informa altresì che le persone che svolgono funzioni di Amministratore di Sistema, sia come servizi in outsourcing – svolti principalmente dalla società LazioCrea – che internamente, sono abilitati ad accedere a tutti i dati presenti nel Sistema Informativo in uso presso la Regione (sia nella parte gestita in outsourcing, sia nelle risorse presenti presso la Regione). Considerato che l'attività degli Amministratori di Sistema può riguardare anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, si informa che è possibile conoscere l'identità degli amministratori di sistema nell'ambito regionale, secondo le caratteristiche del servizio, in relazione ai diversi servizi informatici cui questi sono preposti, consultando la sezione dedicata alla protezione dei dati personali della Intranet regionale. Si ricorda il divieto generale di utilizzare le risorse fornite dal Titolare per scopi personali o non attinenti con le attività lavorative affidate.
Infine, la Giunta regionale non effettua apposite registrazioni per il controllo dell'attività lavorativa del personale, ma soltanto registrazioni volte a salvaguardare la sicurezza ed il mantenimento dell'efficienza dei sistemi nonché a garantire la corretta gestione della rendicontazione delle spese. I dati registrati a tale scopo dai sistemi non sono utilizzati in alcun modo per il controllo a distanza dei lavoratori.

2. MODALITÀ DEL TRATTAMENTO

Il trattamento dei Suoi dati, ed eventualmente di quelli dei Suoi familiari, sarà effettuato mediante l'ausilio di strumenti manuali, informatici/elettronici/automatizzati e/o supporti cartacei ad opera di

soggetti a ciò appositamente formati ed incaricati, con logiche strettamente correlate alle suddette finalità e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi. I dati potranno essere trattati esclusivamente dal personale e dai collaboratori della Giunta regionale o dalle imprese espressamente nominate come Responsabili del trattamento.
Alcuni dati, quali, ad esempio, il nominativo, potranno essere resi disponibili sulla intranet aziendale.

3. NATURA OBBLIGATORIA O FACOLTATIVA DEL CONFERIMENTO DEI DATI

Il conferimento dei Suoi dati personali per le suddette finalità è necessario per l'instaurazione, la prosecuzione e corretta gestione del contratto di lavoro; pertanto, l'eventuale rifiuto a fornire tali dati potrà causare la mancata instaurazione del rapporto contrattuale, ovvero in corso di tale rapporto, l'impossibilità di proseguirlo.
Il conferimento dei dati finalizzati ai trattamenti la cui base giuridica è l'esecuzione di un contratto di cui l'interessato è parte è necessario, e un eventuale rifiuto può comportare l'impossibilità di perseguire le summenzionate finalità.
Il conferimento dei dati finalizzati ai trattamenti la cui base giuridica è il consenso non è obbligatorio e un eventuale rifiuto potrà impedire la prestazione di determinati servizi. Lei può in ogni momento revocare il consenso precedentemente conferito. Tale revoca non renderà illecito il trattamento precedentemente effettuato sulla base del consenso prestato.
Il Titolare del trattamento rende noto, inoltre, che l'eventuale non comunicazione, o comunicazione errata, di una delle informazioni obbligatorie, potrebbe avere le seguenti conseguenze:

a) impossibilità del Titolare di garantire la congruità del trattamento stesso rispetto ai patti contrattuali per cui esso è eseguito;
b) possibile mancata corrispondenza dei risultati del trattamento stesso rispetto agli obblighi imposti dalla normativa fiscale, amministrativa o del lavoro cui esso è indirizzato.

4. AMBITO DI COMUNICAZIONE E DIFFUSIONE DEI DATI

I Suoi dati personali saranno comunicati nei limiti previsti dalla vigente normativa, dagli accordi sindacali nonché dalla normativa in materia di protezione dei dati personali. I Suoi dati saranno comunicati agli enti ed alle Autorità competenti in adempimento agli obblighi normativi nella misura strettamente necessaria. In particolare, a titolo esemplificativo e non esaustivo, si evidenzia che i dati potranno essere comunicati alla Corte dei conti (per la gestione dei trattamenti previdenziali), alle Commissioni medico ospedaliere (per la concessione della pensione privilegiata ordinaria e pensione di inabilità, per la concessione del prolungamento del periodo di assenza per malattia, per la risoluzione del rapporto di lavoro per infermità, per nuovo inquadramento per inidoneità fisica), agli Enti preposti alla vigilanza in materia di igiene e sicurezza del lavoro (compresi l'INAIL e l'Autorità locale di pubblica sicurezza per le comunicazioni concernenti gli infortuni sul lavoro), all'INAIL (per la gestione dei trattamenti previdenziali e pensionistici nonché per prestazioni creditizie), alle ASL e strutture sanitarie competenti (per la richiesta di visita fiscale e per gli accertamenti sanitari relativi allo stato di salute del dipendente assente per malattia), ai Centri per l'impiego (per le assunzioni di personale appartenente a categorie protette), alla Presidenza del Consiglio dei Ministri -Dipartimento della Funzione Pubblica (in relazione alla gestione ed alla rilevazione annuale dei permessi per cariche sindacali nonché per l'attivazione di servizi/progettualità riguardanti il personale pubblico a cui la Regione ha aderito).
I dati potranno inoltre essere comunicati:

a) agli Istituti bancari appositamente indicati per il versamento delle somme a qualsiasi titolo spettanti nonché, su espressa e separata richiesta degli interessati, ad enti ed organismi vari per

l'adempimento di specifiche prestazioni aggiuntive facoltative a favore del personale (ad esempio polizze sanitarie, polizze vita ed infortuni, previdenza integrativa);
b) a fornitori, qualora ciò sia necessario per il corretto svolgimento delle Sue attività lavorative;
c) a persone, società, associazioni o studi professionali che prestino servizi o attività di assistenza e/o consulenza al Titolare, con particolare, ma non esclusivo, riferimento ad attività di natura contabile, amministrativa, legale, tributaria retributiva, finanziaria e informatica;
d) a soggetti cui la facoltà di accedere ai dati sia riconosciuta da specifiche disposizioni normative (a titolo esemplificativo il medico competente ai sensi del D.lgs. 81/2008 e successive modifiche).

La Giunta regionale Le garantisce la massima cura affinché la comunicazione dei Suoi dati personali e degli eventuali dati dei Suoi familiari ai predetti destinatari riguardi esclusivamente i dati necessari per il raggiungimento delle specifiche finalità cui i dati stessi o la comunicazione sono destinati.
Si ricorda, infine, l'assunzione da parte Sua delle responsabilità connesse alla trasmissione alla Giunta regionale di eventuali dati personali riguardanti i Suoi familiari per l'ammissione ai benefici cui la raccolta è finalizzata. A tal fine, si prega di curare direttamente ogni adempimento che la renda possibile.
È prevista, con le cautele disposte dalla normativa in materia di protezione dei dati personali, la diffusione dei dati personali nei casi in cui la normativa vigente preveda forme di diffusione dei dati (ad esempio pubblicazione dei ruoli di anzianità del personale, graduatorie di concorsi o procedure selettive).
Si precisa, infine, che non sarà effettuato alcun trasferimento dei Suoi dati all'estero.

5. TITOLARE DEL TRATTAMENTO

Titolare del trattamento è la Giunta della Regione Lazio, con sede in via Rosa Raimondi Garibaldi n. 7– 00147 Roma.

6. RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)

La Giunta della Regione Lazio ha individuato un Responsabile della Protezione dei Dati, che è contattabile via PEC all'indirizzo DPO@regione.lazio.legalmail.it o attraverso la e-mail istituzionale: dpo@regione.lazio.it o presso URP-NUR 06-99500.

7. TEMPI DI CONSERVAZIONE

Il Titolare conserva, di regola, i dati dell'interessato per tutta la durata del rapporto di lavoro e successivamente per un periodo di dieci anni dall'estinzione del rapporto, salvo che sia previsto un periodo di conservazione diverso (ad esempio nel caso di contenzioso o per adempiere ad un obbligo normativo) che potrebbe essere inferiore o superiore a detto termine; in tali casi, i dati saranno conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. Durante tale periodo saranno, comunque, attuate misure tecniche e organizzative adeguate per la tutela dei diritti e delle libertà dell'interessato. Alcuni dati dovranno essere conservati per almeno dieci anni laddove la normativa vigente lo preveda. La durata di conservazione dei dati registrati in diversi log è stabilita in relazione alle disposizioni applicabili (ad esempio il provvedimento del 27 novembre 2007 relativo all'Amministratore di Sistema) o sulla base delle determinazioni della Giunta regionale.

8. DIRITTI DELL'INTERESSATO

Ai sensi degli articoli da 15 a 22 del RGPD, Lei ha il diritto, in qualunque momento, di:

a) 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;
b) esercitare i diritti di cui sopra inviando idonea comunicazione alla casella di posta certificata protocollo@regione.lazio.legalmail.it citando: Rif. Privacy;
c) 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.

L'esercizio dei diritti non è soggetto ad alcun vincolo di forma ed è gratuito, salvi i casi in cui il Titolare può stabilire l'ammontare dell'eventuale contributo spese da richiedere ai sensi della normativa vigente.

9. NATURA DEL CONSENSO

Ai sensi dell'articolo 6 del dal RGPD, il consenso al trattamento dei suddetti dati non è necessario quando i dati sono trattati per adempiere ad obblighi di legge, per l'esecuzione di obblighi derivanti da un contratto di cui l'interessato è parte, per esercitare il legittimo interesse del Titolare del trattamento o per l'adempimento di un compito di interesse pubblico.
Le ricordiamo che, considerando che l'utilizzo delle Sue immagini (foto o riprese audio-video) per le finalità sopra descritte non è vincolante per la prosecuzione dell'incarico da Lei ricoperto, potrà chiedere che le stesse non vengano utilizzate per le finalità sopra descritte. Il suo rifiuto non pregiudicherà la prosecuzione del rapporto di lavoro con la Giunta regionale.

Art. 21

(Sostituzione dello schema "G" nell'allegato "NN" al r.r.1/2002 e successive modificazioni)

1. Lo schema "G" dell'allegato "NN" del r.r. 1/2002 e successive modificazioni è sostituito dal seguente:

SCHEMA G

(art. 474, c. 2)

NOMINA RESPONSABILE DEL TRATTAMENTO

ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI
(*ove necessario* **Allegato al CONTRATTO DEL XX.XX.XXXX)**

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 Società, con sede in ……in persona del legale rappresentante pro tempore Dott. …….;

PREMESSO CHE

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

- svolge attività che comportano il trattamento di dati personali nell'ambito dei servizi istituzionalmente affidati; è consapevole di essere tenuta a mettere in atto misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati e adeguate 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 r.r. 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale) e successive modificazioni, il quale prevede che il titolare del trattamento, con specifico atto negoziale di incarico ai singoli responsabili del trattamento, disciplina i trattamenti affidati al responsabile, i compiti e le istruzioni secondo quanto previsto dall'articolo 28, paragrafo 3, del Regolamento (UE) 2016/679 (di seguito anche "RGPD") e in coerenza con le indicazioni del Responsabile della Protezione dei Dati del Titolare (di seguito anche "DPO"); nell'atto di incarico è, altresì, definita la possibilità di nomina di un sub-responsabile, secondo quanto previsto dall'articolo 28, paragrafi 2 e 4, del RGPD;

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

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

CONSIDERATO che le attività, erogate in esecuzione del Contratto ***<indicare riferimenti del contratto>***, tra 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 prevede che "Titolare del Trattamento" sia "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento

sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri";

PRESO ATTO che l'art. 4, n. 8) del RGPD definisce "Responsabile del Trattamento" "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento";
VISTO il Provvedimento del Garante per la Protezione dei Dati Personali 27/11/2008 (Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema) e successive modificazioni, pubblicato sulla Gazzetta Ufficiale n. 300 del 24/12/2008;
CONSIDERATO che il suddetto Provvedimento richiede che si proceda alla designazione individuale degli Amministratori di Sistema (System Administrator), degli Amministratori di Base Dati (Database Administrator), degli Amministratori di Rete (Network Administrator) e degli Amministratori di Software Complessi, che, nell'esercizio delle proprie funzioni, hanno accesso, anche fortuito, a dati personali (di seguito anche "AdS");
VISTO il provvedimento dell'AgID (Misure minime di sicurezza ICT per le Pubbliche Amministrazioni), adottato in attuazione della Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015 (di seguito "Misure minime AgID"), il quale ha dettato le regole da osservare per garantire un uso appropriato dei privilegi di AdS;
RITENUTO che, ai sensi dell'articolo 28, paragrafo 1 del RGPD, 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 del Lazio è Titolare soddisfi i requisiti e il pieno rispetto delle disposizioni previste dal RGPD;

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

Articolo 1

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

Articolo 2

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

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

– i trattamenti sono svolti per ***<indicare le finalità per cui il fornitore tratta i dati (es. ai fini di assistenza e manutenzione)>***;
– 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"; dati giudiziari di cui all'articolo 10 del RGPD; ***<eliminare le eventuali tipologie di dati non oggetto di trattamento>***
– le categorie di interessati sono ***<indicare le tipologie di interessato cui i dati afferiscono>***.

- La Società è autorizzata a procedere all'organizzazione di ogni operazione di trattamento dei dati nei limiti stabiliti dai contratti in essere tra le parti e dalle vigenti disposizioni contenute nel RGPD.

- La Società si impegna, già in fase contrattuale, al fine di garantire il rispetto del principio della "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" di cui all'articolo 25 del RGPD, a determinare i mezzi del trattamento e a mettere in atto le misure tecniche e organizzative adeguate, ai sensi dell'articolo 32 del RGPD, prima dell'inizio delle attività.
- La Società dovrà eseguire i trattamenti funzionali alle attività ad essa attribuite e comunque non incompatibili con le finalità per cui i dati sono stati raccolti. Qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, la Società dovrà informare il Titolare del trattamento ed il Responsabile della Protezione dei Dati (DPO) della Giunta Regionale del Lazio.

- La Società – per quanto di propria competenza – è tenuta, in forza della 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 e qualità dei dati, nonché l'utilizzo dei predetti dati per le sole finalità specificate nel presente atto e nell'ambito delle attività di sicurezza di specifico interesse del Titolare.

- La Società ha il compito di curare, in relazione alla fornitura del servizio di cui al presente contratto, l'attuazione delle misure prescritte dal Garante per la protezione dei dati personali in merito all'attribuzione delle funzioni di "Amministratore di Sistema" di cui al provvedimento del 27 novembre 2008, e successive modificazioni e, in particolare, di:
  - designare come Amministratore di Sistema, con le modalità previste dal provvedimento del 27 novembre 2008, le persone fisiche autorizzate ad accedere in modo privilegiato (ai sensi dello stesso provvedimento) ai dati personali del cui trattamento la Regione Lazio è titolare;
  - conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte all'interno della vostra Società quali Amministratori di Sistema (in relazione ai dati personali del cui trattamento la Giunta Regionale del Lazio è titolare)
  - porre in essere le attività di verifica periodica, con cadenza almeno annuale, sul loro operato secondo quanto prescritto dallo stesso provvedimento; gli esiti di tali verifiche dovranno essere comunicati al Titolare del trattamento su richiesta dello stesso.

- La Società 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.

- La Società 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. La Società garantirà, inoltre, che le persone autorizzate al trattamento siano vincolate da un obbligo, legalmente assunto, di riservatezza.

- La Società si attiverà per garantire l'adozione delle misure di sicurezza di cui all'articolo 32 del RGPD. In particolare, tenuto conto delle misure di sicurezza in atto, adottate a protezione dei trattamenti dei dati per conto della Giunta Regionale del Lazio come previste dal contratto vigente, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento e, sulla base delle risultanze dell'analisi dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, che derivano in particolare dalla distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati, porrà in essere le opportune azioni organizzative per l'ottimizzazione di tali misure, per garantire un livello di sicurezza adeguato al rischio. Tali misure, qualora necessario, comprendono, altresì, le seguenti:
  a) la pseudonimizzazione e la cifratura dei dati personali;
  b) misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  c) misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
  d) 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, la Società 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.
La Società assicura, inoltre, che le operazioni di trattamento dei dati sono effettuate nel rispetto delle misure di sicurezza tecniche, organizzative e procedurali a tutela dei dati trattati, in conformità alle previsioni di cui ai provvedimenti di volta in volta emanati dalle Autorità nazionali ed europee, qualora le stesse siano applicabili rispetto all'attività effettivamente svolta come Responsabile del trattamento.
Nel caso in cui, considerata la propria competenza e ove applicabile rispetto alle attività svolte, la Società dovesse ritenere che le misure adottate non siano più adeguate e/o idonee a prevenire/mitigare i rischi sopramenzionati, è tenuta a darne tempestiva comunicazione scritta al Titolare e a porre comunque in essere tutti gli interventi temporanei, ritenuti essenziali e improcrastinabili, in attesa delle soluzioni definitive da concordare con il Titolare.
L'adozione e l'adeguamento devono aver luogo prima di iniziare e/o continuare qualsiasi operazione di trattamento di dati.
La Società è tenuta a segnalare prontamente al Titolare l'insorgenza di problemi tecnici attinenti alle operazioni di raccolta e trattamento dei dati ed alle relative misure di sicurezza, che possano comportare rischi di distruzione o perdita, anche accidentale, dei dati stessi, ovvero di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta/dei trattamenti.
Inoltre la Società dovrà adottare le misure minime di sicurezza ICT per le PP.AA. di cui alla circolare AgID del 18 aprile 2017, n. 2/2017 ove applicabile, nonché le eventuali ulteriori misure specifiche stabilite dal Titolare, nel rispetto dei contratti vigenti.
- La Società dovrà predisporre e tenere a disposizione del Titolare la documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito riportate; inoltre renderà disponibili al Titolare tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti normativi previsti dal RGPD, consentendo di effettuare periodicamente attività di verifica, comprese ispezioni da parte del Titolare stesso o di un altro soggetto da questi incaricato.

- La Società 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.

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

- La Società è tenuta ad informare di ogni violazione di dati personali (cosiddetta *personal data breach*) il Titolare ed il Responsabile della Protezione dei Dati (DPO) della Giunta Regionale del Lazio, tempestivamente e senza ingiustificato ritardo, al più presto, comunque non oltre 48 ore dall'avvenuta conoscenza dell'evento. Tale notifica – da effettuarsi tramite PEC da inviare all'indirizzo protocollo@regione.lazio.legalmail.it e dpo@regione.lazio.legalmail.it, deve essere accompagnata da ogni documentazione utile, ai sensi degli articoli 33 e 34 del RGPD, per permettere al Titolare, ove ritenuto necessario, di notificare tale violazione al Garante per la protezione dei dati personali e/o a darne comunicazione agli interessati, entro il termine di 72 ore da quando il Titolare ne è venuto a conoscenza. Nel caso in cui il Titolare debba fornire informazioni aggiuntive alla suddetta Autorità, la Società supporterà il Titolare stesso nella misura in cui le informazioni richieste e/o necessarie per il Garante siano esclusivamente in possesso del Responsabile e/o di suoi sub-Responsabili.

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

- La Società, qualora riceva istanze da parte degli interessati in esercizio dei loro diritti ai sensi degli articoli da 15 a 22 del RGPD, è tenuta a:
  - darne tempestiva comunicazione scritta al Titolare e al Responsabile della Protezione dei Dati (DPO) della Regione Lazio, allegando copia della richiesta;
  - valutare con il Titolare e con il DPO della Regione Lazio la legittimità delle richieste;
  - coordinarsi con il Titolare e con il DPO della Regione Lazio al fine di soddisfare le richieste ritenute legittime.

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

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

- 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.

- La Società 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 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.

- La Società 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.

- La Società è tenuta a comunicare al Titolare ed al DPO della Regione Lazio il nome ed i dati del proprio DPO, laddove la società stessa lo abbia designato conformemente a quanto prescritto dall'articolo 37 del RGPD. Il DPO collaborerà e si terrà in costante contatto con il DPO della Regione Lazio.

- Per "persone autorizzate al trattamento" ai sensi dell'articolo 4, punto 10 secondo quanto previsto dal Regolamento si intendono le persone fisiche che, sotto la diretta autorità del Responsabile, sono autorizzate ad effettuare le operazioni di trattamento dati personali riconducibili alla titolarità della Regione Lazio.

- La Società è tenuta ad autorizzare tali soggetti, ad individuare e verificare almeno annualmente l'ambito dei trattamenti agli stessi consentiti e ad impartire ai medesimi istruzioni dettagliate circa le modalità del trattamento.

- Le "persone autorizzate al trattamento" sono tenute al segreto professionale e alla riservatezza, anche per il periodo successivo all'estinzione del rapporto di lavoro intrattenuto con il Responsabile, in relazione alle operazioni di trattamento da essi eseguite. In particolare la Società garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.
- La Società è tenuta, altresì, a vigilare sulla puntuale osservanza delle proprie istruzioni.

Articolo 3

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

- individuare i soggetti ai quali affidare il ruolo di Amministratori di Sistema (System Administrator), Amministratori di Base Dati (Database Administrator), Amministratori di Rete (Network Administrator) e/o Amministratori di Software Complessi e, sulla base del successivo atto di designazione individuale, impartire le istruzioni a detti soggetti, vigilando sul relativo operato;
- assegnare ai suddetti soggetti una user id che contenga riferimenti agevolmente riconducibili all'identità degli Amministratori e che consenta di garantire il rispetto delle seguenti regole:
  - divieto di assegnazione di user id generiche e già attribuite anche in tempi diversi;

- utilizzo di utenze amministrative anonime, quali “root” di Unix o “Administrator” di Windows, solo per situazioni di emergenza; le relative credenziali devono essere gestite in modo da assicurare l’imputabilità in capo a chi ne fa uso;
- disattivazione delle user id attribuite agli Amministratori che non necessitano più di accedere ai dati;

• associare alle user id assegnate agli Amministratori una password e garantire il rispetto delle seguenti regole:

−utilizzare password con lunghezza minima di almeno 14 caratteri, qualora l’autenticazione a più fattori non sia supportata;

−cambiare la password alla prima connessione e successivamente almeno ogni 30 giorni (password aging).

−le password devono differire dalle ultime 5 utilizzate (password history);

−conservare le password in modo da garantirne disponibilità e riservatezza;

−registrare tutte le immissioni errate di password. Ove tecnicamente possibile, gli account degli Amministratori devono essere bloccati dopo un numero massimo di tentativi falliti di login;

−assicurare che l’archiviazione di password o codici PIN su qualsiasi supporto fisico avvenga solo in forma protetta da sistemi di cifratura;

• assicurare la completa distinzione tra utenze privilegiate e non privilegiate di amministratore, alle quali devono corrispondere credenziali diverse;

• assicurare che i profili di accesso, in particolare per le utenze con privilegi amministrativi, rispettino il principio del need-to-know, ovvero che non siano attribuiti diritti superiori a quelli realmente necessari per eseguire le normali attività di lavoro. Le utenze con privilegi amministrativi devono essere utilizzate per il solo svolgimento delle funzioni assegnate;

• mantenere aggiornato un inventario delle utenze privilegiate (Anagrafica AdS), anche attraverso uno strumento automatico in grado di generare un alert quando è aggiunta un’utenza amministrativa e quando sono aumentati i diritti di un’utenza amministrativa;

• adottare sistemi di registrazione degli accessi logici (log) degli Amministratori ai sistemi e conservare gli stessi per un congruo periodo non inferiore a 6 mesi. Qualora la Società utilizzi sistemi messi a disposizione dalla Regione, comunicare agli Amministratori che la Regione stessa procederà alla registrazione e conservazione dei log;

• impedire l’accesso diretto ai singoli sistemi con le utenze amministrative. In particolare, deve essere imposto l’obbligo per l’Amministratore di accedere con un’utenza normale e solo successivamente dargli la possibilità di eseguire, come utente privilegiato, i singoli comandi;

• utilizzare, per le operazioni che richiedono utenze privilegiate di amministratore, macchine dedicate, collocate in una rete logicamente dedicata, isolata rispetto ad internet. Tali macchine non devono essere utilizzate per altre attività;

• comunicare alla Regione, al momento della sottoscrizione del presente atto, e comunque con cadenza almeno annuale ed ogni qualvolta se ne verifichi la necessità, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema, di Base Dati, di Rete e/o di software Complessi, specificando per ciascuno di tali soggetti:

- il nome e cognome;
- la user id assegnata agli Amministratori;
- il ruolo degli Amministratori (ovvero di Sistema, Base Dati, di Rete e/o di Software Complessi);
- i sistemi che gli stessi gestiscono, specificando per ciascuno il profilo di autorizzazione assegnato;

• eseguire, con cadenza almeno annuale, le attività di verifica dell’operato degli Amministratori e consentire comunque alla Regione ove ne faccia richiesta, di eseguire in proprio dette verifiche;

- nei limiti dell'incarico affidato, mettere a disposizione del Titolare e del DPO della Regione quando formalmente richieste, le seguenti informazioni relative agli Amministratori: log in riusciti, log in falliti, log out. Tali dati dovranno essere resi disponibili per un congruo periodo non inferiore a 6 mesi;
- durante l'esecuzione 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.

La presente nomina ha efficacia fino al termine del suindicato contratto in essere tra Regione Lazio e la Società.

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

Sono consentite ulteriori, eventuali, proroghe contrattuali.

Per il Titolare del Trattamento

_____

Sottoscrivendo il presente atto, ***<indicare ragione e denominazione sociale della Società>***:
□ conferma di conoscere gli obblighi assunti in relazione alle disposizioni del RGPD e di possedere i requisiti di esperienza, capacità ed affidabilità idonei a garantire il rispetto di quanto disposto dal medesimo regolamento e sue eventuali modifiche ed integrazioni;
□ conferma di aver compreso integralmente le istruzioni qui impartite e si dichiara competente e disponibile alla piena esecuzione di quanto affidato;
□ accetta la nomina di Responsabile del trattamento dei dati personali e si impegna ad attenersi rigorosamente a quanto ivi stabilito, nonché alle eventuali successive modifiche ed integrazioni disposte dal Titolare, anche in ottemperanza alle modifiche normative in materia.

Per il Responsabile del Trattamento
Legale Rappresentante

_____

Art. 22
(*Inserimento dello schema "I bis" nell'allegato "NN" al r.r.1/2002 e successive modificazioni)*

1. Dopo lo schema "I" del r.r. 1/2002 e successive modificazioni è aggiunto il seguente:

SCHEMA I bis
(art. 474-bis, c. 1)

Schema tipo - Accordo di contitolarità ai sensi dell'articolo 26 del Reg. (UE) 2016/679.

TRA

La Giunta della Regione Lazio (Soggetto designato:_____) (C.F.:_____ - P. IVA:____) con sede in _____, PEC:_____, all'uopo rappresentato da _____

E

_____ (C.F.:_____ - P. IVA:_____) con sede in _____, PEC:_____, all'uopo rappresentato da _____ (d'ora innanzi, entrambe le parti saranno identificate, congiuntamente, quali "Contitolari" o "Parti")

PREMESSO CHE

1) è in essere tra le Parti un progetto comune consistente in_____, il quale comporta la necessità di determinare congiuntamente le finalità e le modalità del trattamento dei dati personali coinvolti nella realizzazione del medesimo progetto comune;
2) che in data 25 maggio 2018 è divenuto pienamente operativo il Regolamento (CE) del 27 aprile 2016, n. 2016/679/UE (Regolamento del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), di seguito denominato "RGPD";
3) l'articolo 4, paragrafo 1, n. 7) del RGDP definisce quale titolare del trattamento "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali";
4) l'articolo 474, comma 1, del r.r. 1/2002 definisce quale titolare del trattamento dei dati personali, ai sensi dell'articolo 4, n. 7) e dell'articolo 24 del RGPD, la Giunta regionale, cui spettano tutte le attività demandate al titolare dal RGPD e, in particolare, l'adozione di misure tecniche e organizzative idonee a garantire e a consentire di dimostrare, che il trattamento dei dati personali è effettuato conformemente al RGPD;
5) la Giunta regionale, in qualità di titolare del trattamento, può prevedere, ai sensi dell'articolo 2-*quaterdecies* del d.lgs. 196/2003 e successive modificazioni, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano conferiti a persone fisiche, che operano sotto la propria autorità, espressamente designate;
6) a norma dell'articolo 26, paragrafo 1 del RGPD "*Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato,e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a*

meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati";

7) a norma dell'articolo 26, paragrafo 2 del RGPD "*L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato"*;

8) è intenzione delle Parti contraenti regolamentare in modo trasparente i diritti e gli obblighi reciproci quali conseguono alla puntuale osservanza delle norme e dei principi contenuti nel RGPD, con particolare riguardo all'esercizio dei diritti dell'interessato, nonché i rispettivi ruoli nella comunicazione delle informazioni agli interessati, addivenendo alla sottoscrizione del presente accordo;

SI CONVIENE E SI STIPULA QUANTO SEGUE

Articolo 1 – Pattuizioni preliminari

1. Nell'ambito delle rispettive responsabilità come determinate dal presente Accordo, i Contitolari dovranno in ogni momento adempiere ai propri obblighi conformemente ad esso e in modo tale da trattare i dati senza violare le disposizioni normative vigenti e nel pieno rispetto delle linee guida e dei Codici di condotta applicabili, di volta in volta approvati dall'Autorità di controllo.
2. Resta inteso tra le Parti che, ai sensi dell'articolo 26, paragrafo 3, del Regolamento (EU) 2016/679, indipendentemente dalle disposizioni del presente Accordo, l'interessato potrà esercitare i propri diritti nei confronti di e contro ciascun Contitolare del trattamento.
3. In coerenza con la propria missione e i propri valori, i Contitolari si impegnano reciprocamente a proteggere i dati personali di ogni persona fisica che si trovasse ad avere contatto o ad operare con i medesimi ("Interessato"), nel rispetto dell'identità, della dignità di ogni essere umano e delle libertà fondamentali costituzionalmente garantite nel rispetto del RGPD relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione degli stessi.
4. Il presente accordo non determina l'insorgere di alcun diritto alla revisione di prezzi od altre forme di impegno, anche economico, già definiti tra le Parti, trattandosi di obblighi ed adempimenti derivanti da norme di legge già conosciute.
5. Il presente accordo annulla e/o sostituisce qualsivoglia regolazione pattizia esistente tra le Parti in relazione al medesimo oggetto, di talché, a far data dalla sua stipulazione, i loro rapporti saranno regolati esclusivamente dal presente accordo.
6. Qualsiasi modifica od integrazione del presente accordo potrà farsi soltanto per iscritto a pena di nullità.
7. Il contenuto essenziale di questo accordo di Contitolarità è messo a disposizione dell'Interessato nella sezione Trasparenza del Portale di ciascuno dei Contitolari.

Articolo 2 - Oggetto del trattamento

1. I Contitolari dichiarano, in merito al trattamento dei Dati Personali, di condividere le decisioni relative alle finalità e modalità del trattamento di dati e, in particolare:

- le seguenti banche dati: dipendenti e collaboratori,_____;
- le finalità del trattamento di dati personali, ciascuna con le proprie specificità legate alle attività concretamente svolte;
- i mezzi del trattamento e le modalità del trattamento di dati personali;
- la politica di conservazione dei dati;
- lo stile e le modalità di comunicazione delle informative ai sensi dell'articolo 13 del RGPD;
- la procedura di gestione dei consensi (ove necessari);

- la designazione e la formazione dei soggetti autorizzati;
- istruzioni sull'uso degli strumenti informatici per il personale;
- la gestione delle comunicazioni e nomine dei responsabili ai sensi dell'articolo 28 del RGPD;
- la tenuta dei registri del trattamento ai sensi dell'articolo 30 del RGPD;
- le procedure nel caso di trasferimento dei dati fuori dall'UE;
- gli strumenti ed i mezzi utilizzati per l'attuazione delle decisioni e in parte anche per l'operatività dei Contitolari, soprattutto in relazione alle misure di sicurezza fisiche, organizzative e tecniche;
- l'approccio basato sul rischio;
- i profili e la politica di sicurezza dei dati personali, la procedura del *Data Breach* e la procedura di valutazione di impatto sulla protezione dei dati personali (DPIA);
- la gestione della procedura di esercizio dei diritti dell'Interessato;
- una raccolta congiunta delle procedure sulla protezione dei dati personali attraverso la tenuta comune e gestione di un modello organizzativo.

2. La contitolarità è riferita al trattamento dei dati personali ed ha ad oggetto il trattamento di tutti i dati già presenti, in tutti gli archivi sia cartacei che informatizzati, e di tutti quelli che si acquisiranno in futuro. Il flusso dei dati personali sarà così strutturato:_____.
3. Con il presente accordo i Contitolari convengono che i dati personali presenti negli archivi sia cartacei che informatizzati, nonché quelli futuri, verranno trattati per le seguenti finalità:_____.
4. Le attività alla base del presente accordo comportano il trattamento delle seguenti categorie di dati personali:_____.
5. Le categorie di interessati sono: _____

Articolo 3 – Durata ed effetti conseguenti allo scioglimento del Contratto

1. Il presente accordo diviene efficace tra le parti all'atto della sua sottoscrizione e ha durata sino a _____, salvo proroga e fermi restando i casi di cessazione anticipata ai sensi della normativa vigente.
2. Il Trattamento dei dati personali in regime di contitolarità, pertanto, deve avere una durata non superiore a quella necessaria agli scopi per i quali i dati personali sono stati raccolti e tali dati devono essere conservati nei sistemi e nelle banche dati dei Contitolari in una forma che consenta l'identificazione degli Interessati per un periodo di tempo non superiore a quello suddetto, fatto salvo che il trattamento e la conservazione dei dati medesimi ad opera di ciascuno dei Contitolari sia imposta dalla normativa vigente.
3. A seguito della cessazione del trattamento, nonché a seguito della cessazione del rapporto convenzionale sottostante, qualunque ne sia la causa, i Contitolari saranno tenuti a provvedere alla integrale distruzione dei dati personali trattati, salvi i casi in cui la conservazione dei dati sia richiesta dalla normativa vigente o il caso in cui si verifichino circostanze autonome e ulteriori che giustifichino la continuazione del trattamento dei dati da parte dei singoli Contitolari, con modalità limitate e per il periodo di tempo a ciò strettamente necessario.
4. Ciascun Contitolare provvede a rilasciare apposita dichiarazione scritta contenente l'attestazione che, presso di sè, non esiste alcuna copia dei dati personali e delle informazioni trattate nell'ambito del progetto comune. Sul contenuto di tale dichiarazione l'altro Contitolare si riserva il diritto di effettuare controlli e verifiche volte ad accertarne la veridicità.

Articolo 4 – Obblighi tra le parti

1. La tutela dei dati personali è fondata sull'osservanza dei principi illustrati nel presente documento che i

Contitolari si impegnano a diffondere, rispettare e far rispettare ai propri amministratori, ai propri dipendenti e collaboratori ed ai soggetti terzi con cui collaborano nello svolgimento della propria attività istituzionale. In particolare, i Contitolari sono impegnati affinché la politica della protezione dati personali, e quanto ne consegue, sia compresa, attuata e sostenuta da tutti i soggetti, interni ed esterni, coinvolti nelle attività dei Contitolari, tenuto conto della loro realtà concreta, delle loro possibilità anche economiche e dei loro valori.

2. I Contitolari si impegnano a mantenere e garantire la riservatezza e la protezione dei dati personali raccolti, trattati e utilizzati in virtù del rapporto di contitolarità. In particolare, essi, anche disgiuntamente tra loro, si impegnano a:

a) comunicare e diffondere la propria politica in merito alla protezione dei dati personali;

b) prestare ascolto e attenzione a tutte le parti interessate proprie – a mero titolo esemplificativo: amministratori, personale dipendente e collaboratori, cittadini, utenti e beneficiari di prestazioni anche di natura assistenziale, fornitori, consulenti – e tenendo in debito conto le loro istanze in materia di trattamento di dati personali e dando pronto riscontro;

c) trattare i dati personali in modo lecito, corretto e trasparente in linea con i principi costituzionali e con la normativa vigente in materia, in particolare il RGPD, e solo per il tempo strettamente necessario alle finalità previste, comprese quelle per ottemperare agli obblighi di legge;

d) raccogliere i dati personali limitandosi a quelli indispensabili per effettuare le attività costituenti il progetto comune (dati personali pertinenti e limitati);

e) trattare i dati personali secondo i principi di trasparenza per le sole finalità specifiche ed espresse nelle proprie informative;

f) adottare processi di aggiornamento e di rettifica dei dati personali trattati per assicurarsi che i dati personali siano, per quanto possibile, corretti e aggiornati;

g) conservare e tutelare i dati personali di cui è in possesso con le migliori tecniche di preservazione disponibili;

h) garantire il continuo aggiornamento delle misure di protezione dei dati personali. Tale impegno sarà costantemente seguito nell'ambito del principio di responsabilizzazione mettendo in atto, con costanza, misure tecniche e organizzative adeguate e politiche idonee, per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al RGPD, tenuto conto dello stato dell'arte, della natura dei dati personali custoditi e dei rischi ai quali sono esposti. Ciascun Contitolare eseguirà un monitoraggio periodico sul livello di sicurezza raggiunto, al fine di renderlo sempre adeguato al rischio;

i) garantire il tempestivo recupero della disponibilità dei dati personali in caso di incidente fisico o tecnico

l) rendere chiare, trasparenti e pertinenti le modalità di trattamento dei dati personali e la loro conservazione in maniera da garantirne un'adeguata sicurezza;

m) favorire lo sviluppo del senso di responsabilizzazione e la consapevolezza dell'intera organizzazione verso i dati personali, visti come dati di proprietà dei singoli interessati;

n) assicurare il rispetto delle disposizioni legislative e regolamentari applicabili alla tutela dei dati personali aggiornando eventualmente la gestione della protezione dei dati personali;

o) prevenire e minimizzare, compatibilmente con le risorse disponibili, l'impatto di potenziali violazioni o trattamenti illeciti e/o dannosi dei dati personali;

p) promuovere l'inserimento della protezione dati personali nel piano di miglioramento continuo che il Contitolare persegue con i propri sistemi di gestione.

3. I Contitolari si impegnano con particolare riguardo all'esercizio dei diritti dell'Interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, ad uniformare le modalità, lo stile, i modelli e soprattutto le procedure per la protezione dei dati personali a favore dell'Interessato.

4. La comunicazione dei dati personali necessari a garantire il perseguimento del progetto comune avverrà curandone l'esattezza, la veridicità, l'aggiornamento, la pertinenza e la non eccedenza rispetto alle finalità

per le quali sono stati raccolti e saranno successivamente trattati.

Articolo 5 - Incaricati e persone autorizzate

1. Ciascuno dei Contitolari dovrà identificare e designare le persone autorizzate ad effettuare operazioni di trattamento sui dati trattati nel perseguimento del progetto comune, identificando l'ambito autorizzativo consentito ai sensi dell'articolo 29 del RGPD e provvedendo alla relativa formazione, anche in merito ai principi di liceità e correttezza a cui deve conformarsi la politica per la protezione dei dati personali e il trattamento dei dati personali nonché al rispetto delle misure di salvaguardia adottate.
2. Ciascuno dei Contitolari garantisce che i propri dipendenti e collaboratori sono affidabili ed hanno piena conoscenza della normativa primaria e secondaria in materia di protezione dei dati personali.
3. Ciascuno dei Contitolari identifica un referente interno alla propria struttura, con il compito di relazionarsi con analogo soggetto designato dall'altra parte, a presidio del corretto adempimento di quanto previsto dal presente accordo. Il nominativo ed i dati di contatto del referente interno sono tempestivamente comunicati all'altra parte.

Articolo 6 - Responsabili del trattamento

1. Ciascuno dei Contitolari che ravvisasse la necessità di avvalersi di un responsabile del trattamento per l'esecuzione di specifiche attività richieste nell'ambito del progetto comune, è tenuto a comunicarlo all'altra parte con congruo preavviso.
2. Su tale responsabile del trattamento sono imposti, mediante un contratto od un altro atto giuridico previsto ai sensi del diritto dell'Unione o degli Stati membri, specifici obblighi in materia di protezione dei dati, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti previsti dalla vigente.
3. I rapporti tra i Contitolari e gli eventuali responsabili del trattamento restano disciplinati dall'articolo 28 del RGPD.

Articolo 7 – Valutazione d'impatto e Violazioni di dati personali

1. Nei casi previsti dall'articolo 35 del RGPD, la valutazione d'impatto sulla protezione dei dati personali ed il suo eventuale riesame, così come la consultazione preventiva di cui all'articolo 36 del RGPD, sono a carico di _____, il quale informa tempestivamente l'altro Contitolare della relativa necessità e dell'attività compiuta.
2. In eventuali casi di violazione della sicurezza dei dati personali che comportino, accidentalmente od in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati e tali da mettere a rischio i diritti e le libertà degli individui i cui dati personali sono trattati nel contesto del progetto comune, l'attività di coordinamento ai fini dell'adempimento degli obblighi di cui agli articoli 33 e 34 del RGPD è affidata a _____ il quale curerà la predisposizione di un apposito documento (*data breach policy*), ove non già esistente ed adottato.
3. Al verificarsi di una violazione di dati personali, il Contitolare non assegnatario dell'attività di coordinamento provvederà:

a) ad informare l'altro Contitolare tempestivamente ed in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione fornendogli tutti i dettagli della violazione stessa, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sugli Interessati coinvolti e le misure adottate per mitigare i rischi;

b) a fornire assistenza per far fronte alla violazione ed alle sue conseguenze, soprattutto in capo agli Interessati coinvolti. Esso, inoltre, si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive ed attuando tutte le azioni correttive approvate e/o richieste dal Contitolare assegnatario dell'attività di coordinamento. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al Trattamento eseguito.

4. Ciascun Contitolare si impegna a predisporre e a tenere aggiornato un registro interno delle violazioni di dati personali nonché a raccogliere e a conservare tutti i documenti relativi ad ogni violazione, compresi quelli inerenti alle circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Articolo 8 - Decisioni in merito ai trasferimenti internazionali di dati personali

1. Il presente accordo prevede che i dati personali saranno trattati all'interno del territorio dell'Unione Europea.

2. Nell'ipotesi in cui per questioni di natura tecnica e/o operativa si rendesse necessario avvalersi di soggetti ubicati al di fuori dell'Unione Europea, il trasferimento dei dati personali, limitatamente allo svolgimento di specifiche attività di Trattamento, sarà regolato in conformità a quanto previsto dal capo V del RGPD. Saranno quindi adottate tutte le cautele necessarie al fine di garantire la più totale protezione dei dati personali basando tale trasferimento: su decisioni di adeguatezza dei paesi terzi destinatari espresse dalla Commissione Europea; su garanzie adeguate espresse dal soggetto terzo destinatario ai sensi dell'articolo 46 del RGPD; sull'adozione di norme vincolanti d'impresa.

Articolo 9 - Condivisione della procedura per l'esercizio dei diritti dell'Interessato

1. I Contitolari designano congiuntamente un referente unitario quale punto di contatto per gli interessati. Le richieste di esercizio dei diritti e gli eventuali reclami presentati dagli interessati saranno gestiti in via esclusiva dal referente unico, contattabile ai recapiti che saranno resi noti unitamente al suo nominativo, restando in ogni caso inteso che gli interessati potranno esercitare i propri diritti nei confronti di ciascun Contitolare.

2. In particolare, qualora il referente unitario riceva richieste provenienti dall'Interessato, finalizzate all'esercizio dei propri diritti, esso dovrà:

- darne tempestiva comunicazione scritta a ciascun Contitolare a mezzo di posta elettronica certificata, allegando copia delle richieste ricevute;
- coordinarsi, ove necessario e per quanto di propria competenza, con le funzioni interne designate da ciascun Contitolare per gestire le relazioni con l'Interessato;
- verificare la sussistenza dei presupposti e consentirne, differirne o rifiutarne l'esercizio, dandone tempestiva comunicazione scritta a ciascun Contitolare a mezzo di posta elettronica certificata.

3. Il referente unitario fornisce altresì assistenza a ciascuno dei Contitolari nell'ambito dei procedimenti amministrativi e giudiziari instaurati dall'Interessato o dall'Autorità di controllo in conseguenza dell'attività dicui al presente articolo.

Articolo 10 - Verifiche circa il rispetto delle regole di protezione dei dati personali

1. Ciascuno dei Contitolari riconosce all'altro il diritto di effettuare controlli (audit) relativamente alle operazioni aventi ad oggetto il trattamento dei dati personali nell'ambito del progetto comune. A tal fine, ciascuno dei Contitolari ha il diritto di disporre – a proprie cure e spese – verifiche a campione o specifiche attività di audit o di rendicontazione in ambito protezione dei dati personali e sicurezza, avvalendosi di personale espressamente incaricato a tale scopo, presso le sedi dell'altro.

2. Ciascuno dei Contitolari rende disponibile tutta la documentazione necessaria per dimostrare la conformità a tutti i suoi obblighi e per consentire la conduzione di audit, comprese le ispezioni, e per contribuire a tali verifiche.
3. Ciascuno dei Contitolari deve informare e coinvolgere tempestivamente l'altra parte in tutte le questioni riguardanti il trattamento dei dati personali ed in particolare nel caso di richieste di informazioni, controlli, ispezioni ed accessi da parte dell'Autorità di controllo;

Articolo 11 - Responsabilità per violazione delle disposizioni

I Contitolari si obbligano, in solido tra loro, a predisporre, attuare e aggiornare tutti gli adempimenti previsti in materia di protezione dei dati personali.

Articolo 12 - Responsabile della Protezione dei dati personali

1. Ciascuno dei Contitolari rende noto che il Responsabile della Protezione deiDati personali (RPD o DPO) in conformità alla previsione contenuta nell'articolo 37, paragrafo 1, lettera a) del GDPR, è stato individuato quale soggetto idoneo:

_____

Detto nominativo è stato altresì comunicato al Garante per la Protezione dei Dati Personali con procedura telematica.

Articolo 13 – Clausole nulle o inefficaci

Qualora una o più clausole del presente accordo divengano contrarie a norme imperative o di ordine pubblico, esse saranno considerate come non apposte e non incideranno sulla validità dello stesso, fatto salvo il diritto di ciascuna parte di chiedere una modifica dell'accordo.

Articolo 14 – Comunicazioni

Qualsiasi comunicazione relativa al presente accordo dovrà essere data per iscritto ed a mezzo di posta elettronica certificata, con ricevuta di accettazione e conferma di consegna, purché inviati o consegnati all'indirizzo indicato in testa all'accordo. Tale indirizzo potrà essere modificato da ciascuna delle Parti, dandone comunicazione all'altra ai sensi del presente articolo.

Articolo 15 – Disposizioni finali

Per quanto non espressamente indicato nella presente Appendice, si rinvia a quanto previsto dal RGPD, dalle disposizioni normative vigenti, nonché ai provvedimenti dell'Autorità di controllo.

Per il Titolare del trattamento
Il Soggetto designato
<inserire nome e cognome>

Per il Contitolare del trattamento
Il rappresentante legale
<inserire nome e cognome>

Art. 23
(Inserimento dell'allegato "OO" al r.r.1/2002 e successive modificazioni)

1. Dopo l'allegato "NN" del r.r. 1/2002 e successive modificazioni è inserito il seguente:

ALLEGATO OO (art. 474-bis, c.1)

REGIONE LAZIO

Procedura operativa per la gestione delle violazioni dei dati personali "Personal Data Breach"

-versione 1.0-

Sommario

1. Premessa e obiettivi

1.1. Premessa

Il 24 maggio 2016 è entrato in vigore il "Regolamento (UE) 2016/679 (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 tale regolamento è pienamente applicabile in tutti gli Stati membri. Elemento cardine della suddetta normativa è il concetto di "accountability" 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 dei Data Breach, eventi di violazione 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[2] trasmessi, conservati o trattati dalla Giunta della Regione Lazio nel ruolo di Titolare. (di seguito anche "**Data Breach**" o "**Violazione dei dati personali**")[3].

In particolare, secondo quanto previsto dal WP250 *"Guidelines on Personal Data Breach notification under Regulation 2016/679",* gli eventi di possibile violazione dei dati personali possono essere classificati in tre macrocategorie:

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

[2] **«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)

[3] **«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)

Ai sensi 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.

Ai sensi dell'articolo 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 PB[4] 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 "Data Breach".

Il documento contiene le indicazioni operative e le informazioni necessarie per garantire il governo e l'attuazione del processo di gestione dei Data Breach.

Il presente documento si articola in due differenti sezioni:

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

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

A. Definizione della procedura, ruoli e responsabilità

1. Procedura operativa generale

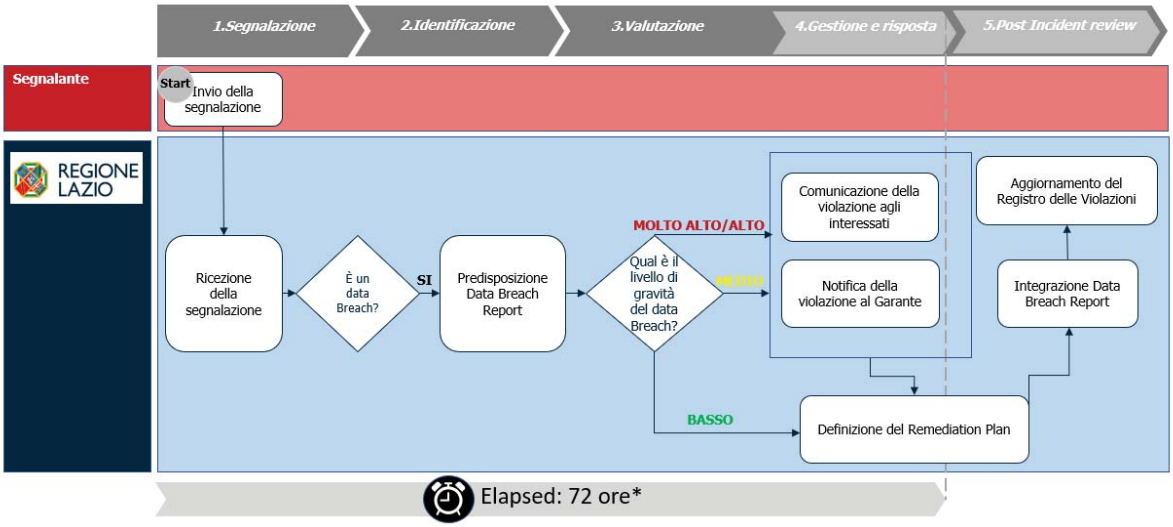
Ogni violazione dei dati personali, occorsa nell'ambito di trattamenti di dati personali trasmessi, conservati o trattati dalla Giunta della Regione Lazio nel ruolo di Titolare, deve essere gestita secondo quanto previsto nelle fasi descritte di seguito:

- **Segnalazione:** fase di segnalazione/ricezione di un potenziale Data Breach;

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

- **Identificazione:** fase in cui la segnalazione ricevuta viene identificata come un Data Breach o come altro incidente di sicurezza (*falso positivo*); se si tratta di 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 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 in seguito, in funzione di nuove informazioni rilevate.
- **Gestione e risposta:** in base al livello di gravità del Data Breach, la Giunta della Regione Lazio dovrà comunicare la violazione agli interessati e/o al Garante; inoltre, in tale fase, viene definito il ***Remediation Plan*** al fine di porre rimedio alla violazione e per attenuarne i possibili effetti negativi;
- **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.*

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 della Regione Lazio, ha la responsabilità ultima della corretta gestione delle violazioni dei dati personali trasmessi, conservati o trattati. Si avvale delle strutture organizzative della Giunta regionale per la segnalazione, l'identificazione, la valutazione e gestione e risposta alle violazioni di dati personali e per il post incident review.
TDB	**Team Data Breach**	Il team Data Breach, formato da alcuni soggetti designati dal Titolare e dal DPO regionale, si attiva a seguito di ogni segnalazione, con la seguente composizione: • DPO regionale • Soggetto designato competente in materia di protezione dei dati personali • Soggetto designato competente in materia di sistemi informativi • Soggetto designato competente per materia Il Team segue tutte le fasi della presente procedura.
DPO	**Data Protection Officer - DPO**	Il DPO supporta il Titolare nell'intero processo di gestione del 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**, con il supporto del Team, stabilisce se la segnalazione costituisca una violazione. Nella fase di **Valutazione**, supporta il Team nella valutazione del livello di gravità. Nella fase di **Gestione e Risposta** supporta il Team nella predisposizione della notifica al Garante e agli interessati, nonché nell'elaborazione del Remediation Plan. Nella fase di Post Incident review, con il supporto del Team, aggiorna il Data Breach Report ed il **Registro delle Violazioni**.
ICT	**Soggetto designato competente in materia di sistemi informativi**	Il soggetto designato competente in materia di sistemi informativi, nella fase di identificazione, supporta il Team per stabilire se la segnalazione costituisca una violazione. Nella fase di valutazione, supporta il Team nella valutazione del livello di gravità. Nella fase di gestione e risposta, in collaborazione con il Team, supporta la predisposizione della notifica al Garante e agli interessati. Nella medesima fase collabora alla stesura del Remediation Plan e, in attuazione

		dello stesso, adotta le conseguenti azioni ricadenti nell'ambito della gestione dei sistemi informativi. Nella fase di Post Incident review fornisce, collaborando con il Team, informazioni per l'aggiornamento del Data Breach Report e del registro delle violazioni.
SDC	**Soggetto designato competente**	Il soggetto designato che ha competenza sul trattamento rispetto al quale è stata segnalata una potenziale violazione, nella fase di Identificazione, supporta il Team per stabilire se la segnalazione costituisca una violazione. Nella fase di valutazione, con il supporto del Team, valuta il livello di gravità della violazione. Nella fase di gestione e risposta, in collaborazione con il Team, predispone e trasmette la notifica al Garante e agli interessati. Nella medesima fase collabora alla stesura del Remediation Plan e, in attuazione dello stesso, adotta le conseguenti azioni ricadenti nell'ambito organizzativo di propria competenza. Nella fase di Post Incident review fornisce, collaborando con il Team, informazioni per l'aggiornamento del Data Breach Report e del registro delle violazioni.
DG	**Direttore Generale**	Il Direttore Generale viene informato dal Team in tutte le fasi del processo, a seguito dell'identificazione di un data breach. Emana eventuali disposizioni di competenza che dovessero rendersi necessarie nelle azioni di remediation.
SS	**Soggetto che effettua la segnalazione**	Soggetto che segnala all'Amministrazione un potenziale 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 step del processo vengono definiti mediante la matrice RACI[5] i ruoli e le responsabilità degli attori coinvolti nella procedura di gestione dei Data Breach.

[5] 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 tre 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	TDB	

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

In qualsiasi momento i dipendenti e/o il personale della Giunta della Regione Lazio o altri possibili soggetti segnalanti, che rilevino un potenziale Data Breach, devono darne tempestivamente comunicazione attraverso l'indirizzo e-mail dedicato databreach@regione.lazio.legalmail.it

E' possibile che le segnalazioni, soprattutto qualora provenienti da terze parti esterne alla Giunta di Regione Lazio (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 incaricato della Giunta della Regione Lazio che ha ricevuto la segnalazione, di un potenziale Data Breach informa tempestivamente e senza ingiustificato ritardo il Soggetto designato (ad esempio il 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 Data Breach (72 ore solari dalla ricezione della segnalazione) **tutti i soggetti incaricati 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 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

A titolo esemplificativo e non esaustivo vengono riportate di seguito alcune tipologie di violazione che potrebbero tradursi in 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 da intervento umano;
- **rivelazione di dati e documenti a soggetti terzi non legittimati**, anche non identificati, conseguenti ad esempio, al fornire 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 alla errata gestione di supporti informatici.

A seguito della segnalazione, il Soggetto designato competente in materia di dati personali convoca, anche per le vie brevi, il Team Data Breach che si occuperà della gestione di tutte le fasi successive del processo.

2.Identificazione

R	A	C	I
SDP	TT	TDB	DG

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

- Dopo aver raccolto tutte le informazioni necessarie e disponibili, il Soggetto designato in materia di protezione dei dati personali valuta la segnalazione ricevuta e:

- se ritiene che non si tratti di un Data Breach, informa il Team Data Breach e, salve obiezioni e/o contestazioni che comportino la necessità di una rivalutazione della segnalazione come violazione dei dati personali, conclude il procedimento, dandone comunicazione al soggetto che ha segnalato il potenziale data breach;
- se ritiene che si tratti di un **Data Breach**, lo notifica al Team e informa il Direttore Generale.

- A seguito della identificazione di un Data Breach, il soggetto designato che ha competenza sul trattamento rispetto al quale è stata identificata una violazione, con la collaborazione del TDB:
    - raccoglie tutte le informazioni disponibili, predisponendo il **Data Breach Report** (**Allegato B**) e coinvolgendo eventualmente anche altri soggetti designati e nominati responsabili del trattamento;

In ogni caso, se la segnalazione riguarda una violazione di natura informatica, il Team Data Breach ed in particolare la Direzione regionale competente in materia di sistemi informativi provvedono ad attivare la specifica procedura adottata dalla Giunta regionale per la gestione 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 soggetto designato che ha competenza sul trattamento rispetto al quale è stata identificata una violazione, con il supporto del Team, valuta la "*gravità*" (severity) del Data Breach 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*" (severity) del Data Breach potrà essere:

Livello	Descrizione
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.).
Molto Alto	Gli interessati possono incontrare conseguenze significative, o addirittura irreversibili, che difficilmente riusciranno a superare (difficoltà finanziarie, debito sostanziale, incapacità lavorativa, disturbi psicologici o fisici a lungo termine, gravi lesioni o morte, 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 Data Breach definito nella fase precedente, il soggetto designato che ha competenza sul trattamento rispetto al quale è stata identificata una violazione procede con:

- la comunicazione agli interessati coinvolti nella violazione dei dati
- la notifica al Garante della violazione dei dati personali

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 molto alto/alto	SI	SI
Rischio medio	SI	NO
Rischio basso	NO	NO

Comunicazione agli interessati

Qualora la valutazione della "*gravità*" (severity) del Data Breach presenti un rischio alto/molto alto per i diritti e le libertà delle persone fisiche, il soggetto designato che ha competenza sul trattamento rispetto al quale è stata identificata una violazione, con il supporto del Team, dà comunicazione agli interessati senza ingiustificato ritardo tramite opportuno strumento di comunicazione.
Possono verificarsi i seguenti casi:

1. sono state adottate preventivamente dal titolare del trattamento, 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;
2. la Giunta della Regione Lazio ha adottato misure successive alla violazione, che garantiscano la riduzione del rischio ad un livello considerato come medio/basso per i diritti e le libertà degli interessati;
3. la comunicazione all'interessato comporta sforzi sproporzionati.

Ai sensi dell'articolo 34, paragrafo 5, del RGPD:
- Nei casi 1 e 2 non dovrà essere effettuata alcuna comunicazione agli interessati.
- Nel caso 3 il soggetto designato che ha competenza sul trattamento rispetto al quale è stata identificata una violazione, con il supporto del Team Data Breach, dovrà valutare una modalità consona per darne comunicazione pubblica in modo tale che gli interessati vengano informati in modo efficace.

Notifica al Garante Privacy

A norma dell'articolo 33 del 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 soggetto designato che ha competenza sul trattamento rispetto al quale è stata identificata una violazione, con il supporto del Team Data Breach, 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 agli interessati, il legislatore europeo ha indicato le seguenti informazioni minime che le stesse devono contenere:

Contenuto notifica diretta all'autorità di controllo[6]	Contenuto comunicazione all'interessato
• **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 della **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

[6] 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.

• 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

Remediation Plan

Il soggetto designato competente in materia di protezione dei dati personali, con il supporto del Team, definisce in questa fase un piano per porre rimedio alla violazione e attenuarne i possibili effetti negativi, con il supporto del Team e, in particolare:

- per la componente del Data Breach di natura tecnico-informatica, del soggetto designato competente in materia di sistemi informativi, tenendo in considerazione e/o integrando il piano con le risultanze dell'attività di gestione degli incidenti di sicurezza informatica ("Identificare e definire le modalità di risoluzione dell'incidente");
- per la componente del Data Breach di natura fisica e organizzativa, del soggetto designato che ha competenza sul trattamento rispetto al quale è stata identificata una violazione.

Ciascun soggetto designato ed eventualmente le altre strutture regionali interessate, per la parte di propria competenza, attuano le azioni definite nel remediation plan.

5. Post Incident Review

R	A	C	I
SDP	SDP	TDB	DG

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

La fase di Post Incident Review è la fase conclusiva di integrazione del Data Breach Report e di analisi *ex post* della violazione al fine di comprendere le cause del Data Breach, apprendere dagli errori e valutare le opportunità di miglioramento.
Il Data Breach Report (**Allegato B**) confluisce 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." (articolo 35, paragrafo 5, del 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 Data Breach	

Allegato A

REGIONE LAZIO

Registro Data Breach

ID	Data	Ora		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
002_2022			☐ ☐	Interna a Regione Lazio: *(specificare)* Esterna a Regione Lazio: *(specificare se fornitore o terzo)*	*Inserire contenuto della segnalazione o link alla struttura*	SI	*Inserire le motivazioni che hanno portato alla decisione di considerare la segnalazione come Data Breach*	*Inserire/Allegare il Data Breach Report*	Medio	SI	NO	*Inserire/Allegare i documenti a supporto della notifica/comunicazione del Data Breach*
003_2022			☐ ☐	Interna a Regione Lazio: *(specificare)* Esterna a Regione Lazio: *(specificare se fornitore o terzo)*	*Inserire contenuto della segnalazione o link alla struttura*	SI	*Inserire le motivazioni che hanno portato alla decisione di considerare la segnalazione come Data Breach*	*Inserire/Allegare il Data Breach Report*	Molto Alto	SI	SI	*Inserire/Allegare i documenti a supporto della notifica/comunicazione del Data Breach*

REGIONE LAZIO

REGIONE LAZIO

in azzurro 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 azzurro, da fornire nella notifica al Garante ai sensi dell'art. 33

Data Breach Report

ID progressivo	001/2022	
Data Breach riportato da:	*Inserire Nome e Cognome dell'Utente che ha segnalato la violazione o del soggetto terzo (es.fornitore)*	
Contatti dell'utente:	*Inserire l'indirizzo email o il numero di telefono dell'utente che ha segnalato la violazione*	
Data e ora:	*Indicare la data della segnalazione (gg/mese/anno) e l'ora (hh:mm)*	
Struttura di appartenenza:	*Inserire la struttura di appartenenza dell'utente*	
Data Protection Officer		
Breve descrizione della violazione	*Hacker entra in possesso delle credenziali, perdita o furto di un laptop, modifica dolosa dei dati di un cliente, etc.*	
Dispositivo oggetto di violazione	*Server, dispositivo mobile, documento cartaeo, file o parte di un file, strumento di bakcup, strumento di rete, etc.*	
Tipologia di violazione	☐	Violazione, intenzionale o accidentale, alla riservatezza dei dati personali (accesso illegittimo)
	☐	Violazione, intenzionale o accidentale, all' integrità dei dati personali (modifica indesiderata)
	☐	Violazione, intenzionale o accidentale, alla disponibilità dei dati personali (scomparsa/distruzione).
Interessati	**numero di interessati coinvolti**	*Indicare, ove possibile, il numero approssimativo dei soggetti impattati dalla violazione*
	☐	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 ordinari
	☐	Dati particolari - sensibili
	☐	Dati particolari - giudiziari
	☐	Dati particolari - patrimoniali
	☐	Dati di videosorveglianza
	☐	Dati biometrici
	☐	Dati CRIF
	☐	Dati CR Banca d'Italia
	☐	Dati di geolocalizzazione
	☐	Dati comportamentali
	☐	Log di sistema
	Volume dei dati coinvoli	*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 sono 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 notificato 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'incident e 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 B

REGIONE LAZIO

Allegato C

Metodologia di valutazione della gravità di un Data Breach

- documento tecnico-metodologico di supporto-

Versione 1.0

1. Premessa e Obiettivi

Il presente documento ha l'obiettivo di declinare la "Metodologia di valutazione delle violazioni dei dati personali" (di seguito anche la *Metodologia*) di cui la Giunta della Regione Lazio, titolare del trattamento, si avvale per valutare la "*gravità*" (severity) potenziale di un eventuale violazione dei dati personali (di seguito anche *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* [7]".

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

- Valutazione del Contesto di elaborazione dei dati (**CED**)[8]
- Determinazione della Facilità di Identificazione (**FI**)[9]
- Valutazione delle Circostanze della violazione (**CV**)[10]
- Calcolo della Gravità (**CG**)

2. Approccio metodologico

La Metodologia adottata dal titolare del trattamento, 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 di un punteggio base 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 Data Breach. Il fattore CV, laddove presente, può solo incrementare la gravità di una specifica violazione.

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

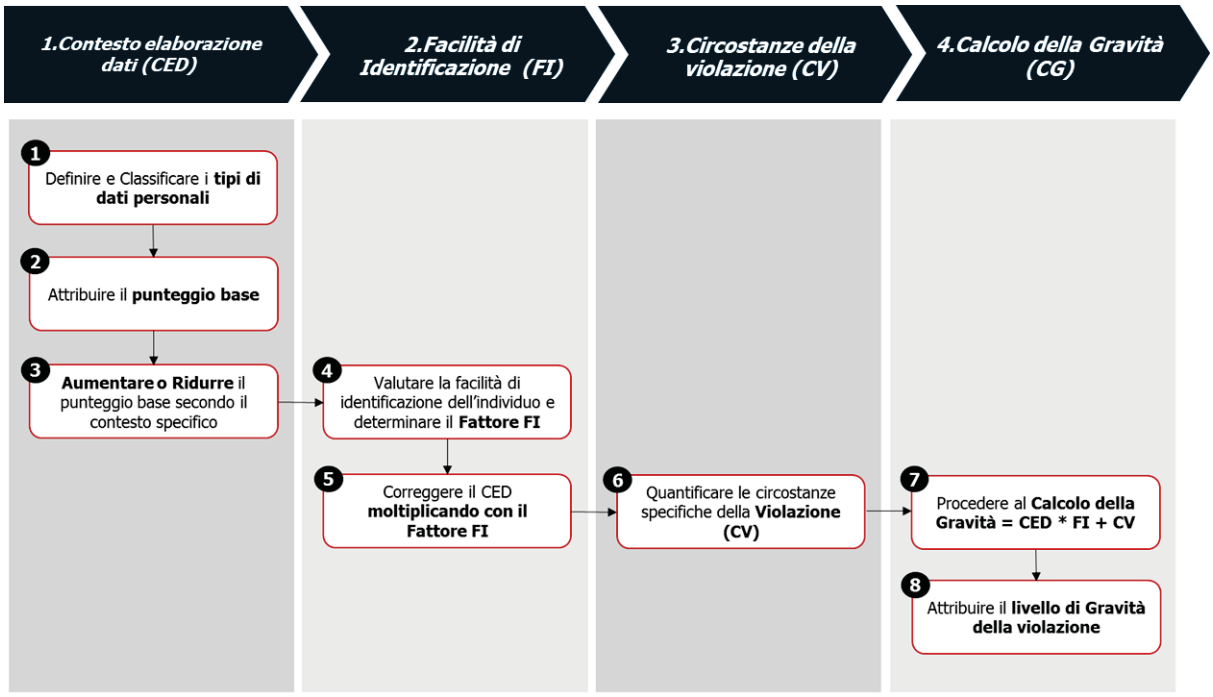
[8] **Data Processing Context (DPC):** Addresses the type of the breached data, together with a number of factors linked to the overall context of processing (cfr. "Recommendations for a methodology of the assessment of severity of personal data breaches")

[9] **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")

[10] **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")

- **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	Definisce e classifica 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)

Attività	Descrizione	Strumenti
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 studio, 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
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**
	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 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 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 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 a 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**

Circostanze della violazione (CV)		Punteggio
	Esempi di dati trasmessi verso un certo numero **di destinatari conosciuti:** - Una 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**
Violazione di integrità	**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.	
	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**
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.	

Circostanze della violazione (CV)		Punteggio
	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 danneggiarli.	**0,5**

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.
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. 24
(Pubblicazione ed entrata in vigore)

1. Il presente regolamento è pubblicato sul Bollettino Ufficiale della Regione Lazio ed entra in vigore il giorno successivo alla data di pubblicazione.

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