“Consiglio regionale della Campania”

Segreteria Generale

Determina N. 1543 del 12/12/2024

Oggetto: presa d'atto di documentazione e procedure relative al trattamento dei dati personali presso il Consiglio regionale, in conformità al Regolamento UE 2019/679 (RGPD)

Elenco firmatari

Antonio Virtuoso - Segreteria Generale

Mario Vasco - Segreteria Generale

Consiglio regionale della Campania

Il Segretario generale

Determinazione

Oggetto: presa d'atto di documentazione e procedure relative al trattamento dei dati personali presso il Consiglio regionale, in conformità al Regolamento UE 2019/679 (RGPD).

Su proposta del Responsabile per la protezione dei dati, dirigente del Settore Risorse finanziarie e strumentali e del Servizio Sistemi Informativi, del dirigente del Settore Risorse umane e del Direttore della Direzione generale Risorse umane finanziarie e strumentali;

vista l'istruttoria compiuta dai rispettivi Uffici, le cui risultanze sono richiamate con il presente atto;

PREMESSO che

- il Regolamento (UE) 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 « *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)*» (di seguito RGPD), pubblicato nella Gazzetta ufficiale dell' U.E. il 4 maggio 2016, è applicabile con efficacia diretta in tutti i Paesi dell' U.E. a partire dal 25 maggio 2018, senza che sia ndo richiesta alcuna norma di ricezione o esecutiva da parte degli Stati membri;
- il Garante per la protezione dei dati personali ha emanato una Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali che intende offrire un panorama delle principali problematiche che i soggetti pubblici, oltre alle imprese, devono tenere presenti per la piena applicazione del Regolamento;
- le norme introdotte dal Regolamento UE 2016/679 si traducono in obblighi organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono considerare ai fini della piena e consapevole applicazione del nuovo quadro normativo in materia di privacy;

CONSIDERATA

- la necessità di aggiornare ed uniformare la documentazione informativa, ai sensi degli artt. 13 e 14 del RGPD, contenente le informazioni da fornire all'interessato qualora i dati personali che lo riguardano siano raccolti presso il medesimo ovvero nel momento in cui sono altrimenti ottenuti, e precisamente:
  a. "Informativa sul Trattamento dei dati personali", in forma estesa, da utilizzare da parte degli Uffici, secondo le particolari esigenze del caso, quando i dati siano consensualmente forniti dall'interessato ovvero quando il trattamento debba essere effettuato, senza il consenso di questo, in presenza di una lecita base giuridica;
  b. "Privacy Policy", con riferimento ai dati eventualmente acquisiti o forniti dall'utente tramite l'interazione con il sito istituzionale del Consiglio regionale;
  c. "Cookies Policy", con riferimento alla operatività di identificatori, idonei a raccogliere dati sull'utente nel corso della consultazione del sito;
- la necessità di definire una procedura volta alla tempestiva e adeguata gestione degli eventi di violazione dei dati personali, sia al fine di valutare le condizioni in base alle quali occorre effettuare la notifica all' Autorità di controllo ovvero la comunicazione agli interessati, ai sensi degli artt. 33 e 34 del RGPD, sia al fine di tenere ed aggiornare il Registro delle violazioni rilevate;
- l'opportunità di predisporre schema e contenuti degli atti da utilizzare al momento della individuazione, per il conferimento dell'incarico, delle principali figure che affiancano il Titolare del trattamento nel sistema di gestione e tutela della riservatezza;

RITENUTO

- di adeguare ovvero integrare la documentazione relativa al trattamento dei dati personali e di prendere atto, pertanto, della documentazione elaborata all'esito dell'attività progettuale svolta dagli Uffici coinvolti, in attuazione di specifico obiettivo del corrente anno, attesa la necessità di aggiornamento a seguito dell'entrata a regime del nuovo assetto ordinamentale dell'Amministrazione consiliare;

VISTI
lo Statuto regionale;
il Regolamento recante "*Ordinamento amministrativo del Consiglio regionale*" (b.u.r.c. n. 53 del 12/7/2023);
il Regolamento Generale sulla Protezione dei Dati personali;
il Decreto P.C.R. n. 86 del 7/8/2023 di nomina del Responsabile della protezione dei dati;

DETERMINA

per le ragioni espresse in premessa che formano parte sostanziale del presente atto,

- di adottare i seguenti documenti informativi, ai sensi dell' art. 13 del RGPD:
  a. "Informativa sul Trattamento dei dati personali" (Allegato 1), da utilizzare da parte delle strutture amministrative ai fini del trattamento di dati personali connesso a procedimenti, attività, servizi di rispettiva competenza;
  b. "Privacy Policy" (Allegato 2), relativa ai dati acquisiti o forniti tramite il sito istituzionale del Consiglio o durante la consultazione dello stesso;
  c. "Cookies Policy" (Allegato 3), relativa all'utilizzo di identificatori in fase di accesso al sito istituzionale;
- di inserire entrambi i documenti delle precedenti lett. b) e c) sul sito istituzionale, tramite collegamento ipertestuale in fondo-pagina;
- di adottare, ai fini della gestione delle violazioni dei dati personali, la procedura definita con il documento recante "Procedura per la segnalazione di violazioni dei dati personali (*data breach policy*)" (Allegato 4);
- di adottare gli schemi degli atti di nomina dei seguenti soggetti:
  "Nomina Responsabile della protezione dei dati" (Allegato 5)
  "Nomina Responsabile del trattamento" (Allegato 6)
  "Nomina Autorizzato al trattamento" (Allegato 7)
  "Nomina Amministratore di sistema" (Allegato 8);
- di dare divulgazione e rendere disponibile la detta documentazione tramite circolare informativa, indirizzata alle strutture ammnistrative dell'Ente, Direzioni Settori e Servizi;
- di trasmettere il presente provvedimento alla Direzione Risorse umane, finanziarie e strumentali, al Settore Risorse umane, al Servizio Sistemi informativi, per gli adempimenti conseguenziali.

IL SEGRETARIO
dott. M.Vasco

Consiglio regionale della Campania

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

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

(versione estesa)

La presente Informativa è redatta ed adottata ai sensi degli artt. 13 e 14 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)*», entrato in vigore il 24 maggio 2016 ed applicabile a partire dal 25 maggio 2018.

Il Regolamento generale sulla protezione dei dati personali (RGPD) dà attuazione all' art. 8 della Carta dei diritti fondamentali dell' Unione Europea, che enuncia il principio secondo cui "*ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano*" e all' art. 16 del Trattato sul funzionamento dell' Unione Europea, che demanda al Parlamento e al Consiglio di stabilire "*le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell' Unione nonché da parte degli Stati membri nell' esercizio di attività che rientrano nel campo di applicazione del diritto dell' Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti a prescindere dalla nazionalità o residenza*".

I dati personali devono essere trattati secondo i principi dell' art. 5 del RGPD, ossia devono essere:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Titolare del trattamento dei dati (e responsabile del trattamento)

Art. 13, par. 1, lett. a) del Regolamento 2016/679/UE

Il Titolare del trattamento è la persona fisica o giuridica o l'autorità pubblica, che ha la facoltà di determinare quali informazioni trattare, per quali finalità e con quali modalità e garanzie.

Il Titolare del trattamento è il Consiglio regionale della Campania (CRC).
Indirizzo: Centro Direzionale, Isola F13 - 84013 Napoli.
p.e.o.: presidente@cr.campania.it; p.e.c.: protocollo.generale@pec.cr.campania.it

Tutti i dirigenti in servizio presso il Consiglio regionale sono delegati, ognuno per gli affari ed atti di propria competenza, al trattamento dei dati effettuato nello svolgimento dell'incarico ricevuto, secondo quanto previsto dal rispettivo contratto individuale di lavoro.

[le singole Direzioni, Settori o Servizi del Consiglio regionale specificano e comunicano all'/agli interessato/i i dati di contatto della struttura e del soggetto (dirigente o incaricato) responsabile del/i trattamento/i connesso/i ad attività, procedimenti o servizi di rispettiva competenza.]

Responsabile della protezione dei dati

Art. 13, par. 1, lett. b) del RGPD

Il Responsabile per la protezione dei dati è la figura che tutti gli interessati possono contattare per le questioni relative al trattamento dei loro dati personali nonché all'esercizio dei diritti derivanti dal Regolamento.

Il Consiglio Regionale della Campania, ai sensi dell' art. 37, par. 1, lett. a) del RGPD, ha nominato quale Responsabile della protezione dei dati il dirigente:
ing. Francesco Crisci
Indirizzo: Centro Direzionale, Isola F13 - 84013 Napoli.
p.e.o.: dpo@cr.campania.it; p.e.c.: protocollo.generale@pec.cr.campania.it

Finalità del trattamento dei dati personali

Art. 13, par. 1, lett. c) del RGPD

Il Consiglio regionale può effettuare trattamenti di dati personali acquisiti per lo svolgimento delle funzioni istituzionali e, dunque, per l'esecuzione di compiti di interesse pubblico o connessi all' esercizio dei pubblici poteri di cui è investito.

I dati saranno trattati secondo i principi di liceità, correttezza, trasparenza, sicurezza e riservatezza, nel rispetto di quanto previsto dall'art. 32 del Regolamento (UE) 2016/679, ad opera di soggetti appositamente incaricati ed istruiti ai sensi dell'art. 29 del Regolamento. Il trattamento avviene

prevalentemente in maniera non automatizzata (UE) 2016/679 e, quando le finalità perseguite possono essere parimenti realizzate, in maniera anonima o con modalità che permettono di identificare l'interessato solo in caso di necessità.

Specifiche finalità, relative a determinati trattamenti, potranno essere segnalate in maniera dettagliata, unitamente ad eventuali informazioni integrative sul trattamento stesso, nell'ambito delle procedure di contatto e di accesso degli interessati alle attività e servizi del CRC.

[le singole Direzioni, Settori o Servizi del Consiglio regionale specificano e comunicano all'/agli interessato/i le finalità dei trattamenti connessi ad attività, procedimenti o servizi di rispettiva competenza.]

Base giuridica del trattamento

Art. 13, par. 1, lett. c) del RGPD e artt. 2-ter e 2-sexies del d.lgs. 30 giugno 2003 n. 196

Il trattamento dei dati personali per le finalità di cui al paragrafo precedente si fonda, in specie, sulle condizioni di liceità previste dal RGPD all' 6, par. 1, lett. c) «*il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento*» e all' art. 6, par. 1, lett. e) «*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*». In tali casi, la base giuridica legittimante è costituita da una norma del diritto euro-unitario ovvero da una norma nazionale di legge o di regolamento o da un atto amministrativo a carattere generale, ai sensi dell' art. 2-ter del d.lgs. 30 giugno 2003 n. 196.

Il trattamento dei dati rientranti nelle particolari categorie di cui all' art. 9 del Regolamento, necessario per motivi di interesse pubblico rilevante, è effettuato, ai sensi dell' art. 2-sexies del d.lgs. 30 giugno 2003 n. 196, sulla base di disposizioni di diritto euro-unitario o di diritto interno previste da legge o regolamento o da atti amministrativi generali, le quali specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi della persona cui i dati si riferiscono.

[le singole Direzioni, Settori o Servizi del Consiglio regionale specificano e comunicano all'/agli interessato/i la base giuridica dei trattamenti connessi ad attività, procedimenti o servizi di rispettiva competenza.]

Destinatari (o categorie di destinatari) di dati personali

Art. 13, par. 1, lett. e) ed f) del RGPD

I dati personali potranno essere comunicati o trattati esclusivamente a/da responsabili del trattamento o personale interno previamente autorizzato o collaboratori cui siano state impartite specifiche ed adeguate istruzioni sulla base di apposite autorizzazioni.

I dati personali non saranno soggetti a diffusione, salvo che ne sia prevista per legge la pubblicazione obbligatoria, ad esempio sul sito informatico istituzionale del Consiglio regionale, anche all' interno

della sezione “Amministrazione trasparente”. In forza di obblighi normativi, i dati personali potranno essere comunicati alle seguenti categorie di soggetti pubblici:

- Autorità pubbliche, legittimate ad accedere ai dati personali in forza di norme di legge o, sulla base di queste, di provvedimenti amministrativi;
- Amministrazioni pubbliche, legittimate ad accedere ai dati personali in ragione delle potestà di cui sono investite, per l’espletamento dell’ attività di controllo.

In nessun caso, i dati personali dell’ interessato saranno trasferiti a soggetti terzi, ovunque stabiliti al di fuori del territorio nazionale, né saranno utilizzati per finalità non dichiarate nella presente Informativa.

Periodo di conservazione e durata del trattamento

Art. 13, par. 2, lett. a) del RGPD

I dati personali vengono acquisiti e conservati nei supporti di memorizzazione del sistema informatico del Consiglio Regionale della Campania e sono protetti dalle misure di sicurezza adottate a protezione del sistema stesso. L’accesso ai sistemi informatici è strettamente personale e avviene mediante l’utilizzo di credenziali di autenticazione in possesso unicamente dei singoli utenti. Ove conservati su supporti cartacei, i dati personali sono adeguatamente custoditi e protetti da accessi indebiti, da parte di soggetti non autorizzati.

Nel rispetto dei principi di liceità, limitazione delle finalità e minimizzazione dei dati, ai sensi dell’ art. 5 del RGPD, i dati personali saranno conservati per tutta la durata delle attività finalizzate alla realizzazione dei compiti istituzionali. I dati personali potranno essere conservati per periodi più lunghi per essere trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all’ art. 89, par. 1 del RGPD.

Indipendentemente dalla determinazione dell’interessato alla loro rimozione, i dati personali potranno essere tuttavia conservati, secondo i termini previsti dalla vigente normativa, ove sia necessario per garantire adempimenti specifici propri delle attività di competenza del Titolare del trattamento ed esclusivamente per tali finalità; ad esempio, nel caso in cui si dovessero far valere in giudizio questioni afferenti alle attività di competenza del Titolare. Nel caso di contenzioso giudiziale, i dati personali saranno conservati per tutta la durata dello stesso, fino all’ esaurimento dei termini di esperibilità delle azioni di impugnazione.

I dati personali che siano soggetti a pubblicazione obbligatoria nella sezione “Amministrazione trasparente” del sito istituzionale saranno conservati per 5 anni, decorrenti dal 1° gennaio successivo all’ anno di pubblicazione.

Diritti dell’ interessato

Art. 13, par. 2, lett. b), d) del RGPD

L’interessato potrà esercitare in ogni momento, mediante richiesta al Titolare del trattamento ovvero al Responsabile della protezione dei dati, indirizzata ai rispettivi recapiti, i diritti previsti dagli articoli

da 15 a 22 del RGPD, di seguito analiticamente descritti:

- **diritto di accesso, art. 15**
  L'interessato ha diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati e alle altre informazioni elencate nell' art. 15 RGPD. In ogni caso ha diritto di ricevere una copia dei dati personali oggetto di trattamento.

- **diritto di rettifica, art. 16**

  L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo nonché di ottenere l'integrazione dei dati personali incompleti.

- **diritto alla cancellazione, art. 17**
  L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano, senza ingiustificato ritardo. Il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali nei casi determinati dalla norma (dati non più necessari rispetto alle finalità, revoca del consenso o insussistenza di altro fondamento giuridico, opposizione dell' interessato, illiceità del trattamento).

- **diritto di limitazione del trattamento, art. 18**
  L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle ipotesi previste: l'interessato contesta l'esattezza dei dati; il trattamento è illecito e si chiede che ne sia limitato l'utilizzo; i dati sono necessari per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; l'interessato si è opposto al trattamento per motivi legittimi. Se il trattamento è limitato, i dati personali saranno trattati solo con l'esplicito consenso dell' interessato. Il titolare è tenuto ad informare quest'ultimo prima che la limitazione sia revocata.

- **obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento, art. 19**
  L'interessato ha diritto ad ottenere che il titolare del trattamento comunichi a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell' art. 16, dell' art. 17, par. 1, e dell' art. 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento ha l'obbligo di comunicare all' interessato tali destinatari qualora lo richieda.

- **diritto alla portabilità dei dati, art. 20**
  L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto ad ottenere che i dati siano trasmessi, da parte del titolare cui siano stati forniti ad un altro titolare del trattamento senza impedimenti, qualora il trattamento si basi sul consenso o su un contratto e qualora il trattamento sia effettuato con mezzi automatizzati.

- **diritto di opposizione, art. 21**
  L'interessato ha diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento di dati personali che lo riguardano. Il titolare del trattamento si astiene

dal trattare ulteriormente i dati personali, salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell' interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

- **diritto di non essere sottoposto a processi decisionali automatizzati, art. 22**
  L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
  Il Consiglio regionale non adotta alcun processo di trattamento automatizzato di dati personali, sulla base del quale siano assunte decisioni che comportino effetti giuridici o che incidano in maniera equivalente nei confronti di potenziali interessati.

Ai sensi dell' art. 13, par. 2, lett. d) del RGPD, si informa che l'interessato può proporre reclamo motivato al Garante per la Protezione dei Dati Personali, se ritiene che il trattamento dei dati che lo riguardano non è conforme alle disposizioni vigenti ovvero se la risposta ad un' istanza per l'esercizio dei diritti menzionati non è tempestiva o soddisfacente. Le informazioni sulle modalità di presentazione possono essere consultate sito istituzionale dell' Autorità, www.garanteprivacy.it

Modalità di revoca del consenso

Art. 13, par. 2, lett. c) del RGPD

L'interessato ha il diritto di revocare in qualsiasi momento il consenso prestato al fine di autorizzare, sulla base dell' art. 6, par. 1, lett. a) o sulla base dell' art. 9, par 2, lett. a) del RGPD, il trattamento dei propri dati per una o più finalità specifiche.

La revoca può essere comunicata al Titolare del trattamento ovvero al Responsabile della protezione dei dati, ai rispettivi recapiti, nonché al Responsabile del determinato trattamento individuato nell' Informativa rilasciata al momento dell' acquisizione del consenso, all' indirizzo di contatto ivi indicato.

La revoca avrà effetto con riguardo al periodo successivo alla sua comunicazione, senza pregiudicare la liceità del trattamento già effettuato in base al consenso prestato prima della revoca.

[le singole Direzioni, Settori o Servizi del Consiglio regionale specificano e comunicano all'/agli interessato/i le modalità di acquisizione del consenso e di revoca dello stesso nell'ambito dei trattamenti connessi ad attività, procedimenti o servizi di rispettiva competenza.]

Consiglio regionale della Campania

PROCEDURA PER LA SEGNALAZIONE DI VIOLAZIONI DEI DATI PERSONALI

Data Breach Policy

1. Finalità

Il Consiglio Regionale della Campania, ai sensi del Regolamento UE 2016/679 (RGPD), è tenuto a trattare e conservare in sicurezza i dati personali acquisiti nell'ambito delle proprie attività e ad agire senza ingiustificato ritardo in caso di violazione degli stessi.

Con il presente documento, dunque, si intende predisporre le azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, tanto al fine di prevenire rischi per i diritti e le libertà degli interessati ed eventuali danni, anche economici, all'Amministrazione quanto al fine di ottemperare tempestivamente all'onere di segnalazione all'Autorità di controllo (ossia il Garante per la Protezione dei Dati personali, GPD) ovvero di comunicazione agli interessati.

L'omissione della notifica o della comunicazione, quando ne ricorrano le condizioni rispettivamente ai sensi dell'art. 33 e dell'art. 34 del RGPD, può comportare l'applicazione da parte dell'Autorità di controllo di una sanzione amministrativa pecuniaria nella misura di cui all'art. 83, par. 4, del RGPD, anche in aggiunta o in luogo di una misura correttiva ai sensi dell'art. 58, par. 2, del RGPD.

Pertanto, la seguente procedura ha lo scopo di definire il flusso operativo ed informativo per la gestione delle violazioni dei dati personali trattati dal Consiglio regionale in qualità di Titolare del trattamento; ad integrazione delle altre misure adottate per la salvaguardia dei dati personali, ai sensi della legislazione vigente.

2. La violazione dei dati personali (data breach)

La violazione di dati personali consiste in una infrazione alla loro sicurezza, la quale comporti la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non consentito ai dati personali trasmessi, conservati o comunque trattati dal Titolare del trattamento.

L'infrazione può essere determinata in maniera accidentale o illecita, sia dall'esterno che all'interno dell' Amministrazione, e può manifestarsi in svariate situazioni pratiche:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- accesso non autorizzato da parte del personale interno, con successiva divulgazione in ambiente pubblico

(infedeltà del dipendente);

- accesso abusivo ai sistemi informatici da parte di terzi, con successiva divulgazione delle informazioni (casi di pirateria informatica);
- alterazione o distruzione di banche-dati, senza autorizzazione rilasciata dal legittimo responsabile;
- virus o altri attacchi al sistema informatico o alla rete;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di dispositivi o attrezzature informatiche in cui siano memorizzati dati personali o tramite cui sia possibile accedere agli stessi;
- invio di documenti informatici o messaggi di posta elettronica contenenti dati personali ad un destinatario errato.

In linea di massima, le situazioni di infrazione di dati personali sono classificabili in tre macro-categorie:

1) **violazione della riservatezza**, quando vi è un accesso accidentale o abusivo a dati personali;

2) **violazione della disponibilità**, quando vi è una perdita o distruzione accidentale o non autorizzata del dato personale;

3) **violazione dell'integrità**, quando vi è un'alterazione accidentale o non autorizzata del dato personale.

3. Soggetti coinvolti nella procedura

Sono obbligati ad attenersi alla presente procedura tutti i soggetti che a qualsiasi titolo svolgono operazioni relative a dati personali di competenza del Titolare del trattamento, e precisamente:

- il personale interno dell'Amministrazione, incluso quello a tempo determinato o in comando nonché coloro che collaborano presso l'Amministrazione a qualsiasi titolo – e, quindi, a prescindere dal tipo di rapporto intercorrente –, i quali nello svolgimento dei loro impieghi abbiano accesso ai dati personali trattati per conto del Titolare del trattamento;
- qualsiasi altro soggetto (persona fisica o persona giuridica) che, in ragione di un rapporto contrattuale in essere con il Titolare del trattamento, abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 GDPR o di autonomo Titolare.

I menzionati destinatari devono essere debitamente informati dell'esistenza e del carattere obbligatorio della presente procedura, tramite idonei mezzi di divulgazione e/o comunicazione individuale.

Il mancato rispetto delle regole di comportamento previste potrà comportare responsabilità disciplinare a carico dei dipendenti ovvero potrà essere causa di risoluzione per inadempimento dei contratti in essere con soggetti terzi, secondo la normativa vigente.

4. Tipi di dati cui si riferisce la procedura

I dati in presenza dei quali deve attivarsi la procedura di segnalazione in caso di violazione sono essenzialmente i seguenti:

- dati personali trattati "da" o "per conto" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;
- dati personali conservati o trattati con qualsiasi mezzo o sistema in uso presso l'Amministrazione.

Ai sensi dell'art. 4 del RGPD, per «dato personale» si intende: "*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 oppure a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

In pratica, sono dati personali tutte quelle informazioni relative a caratteristiche individuali le quali permettono di identificare una persona distinguendola dalle altre, come ad esempio i dati anagrafici (nome, cognome, data di nascita, luogo di nascita), i dati di contatto (indirizzo postale, indirizzo di posta elettronica, numero di telefono fisso o mobile), i dati di accesso e identificazione (username, password), i dati di finanziari e/o di pagamento, etc.

4. Comunicazione dell'evento di violazione dei dati

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un suo delegato, sotto la supervisione del Responsabile della protezione dei dati (RPD).

È necessario che l'eventuale violazione sia affrontata, da parte dei diversi soggetti coinvolti, con immediatezza al fine di prevenire o minimizzare l'impatto sui diritti e le libertà degli interessati e di evitare che il medesimo evento possa ripetersi, anche nel breve periodo.

In primo luogo, nel caso in cui uno dei soggetti indicati al *Punto 3* abbia contezza o fondatamente presuma la possibilità del verificarsi di una concreta o potenziale violazione dei dati personali, dovrà immediatamente **segnalare** la circostanza al responsabile dirigenziale della struttura di riferimento, il quale con il supporto del segnalante si occuperà di **informare** il Titolare del trattamento o un suo delegato ed il Responsabile della protezione dei dati, mediante l'allegato A) "Modulo di comunicazione interna".

5. Gestione della violazione dei dati

La procedura di gestione da svolgere in base alla comunicazione si articola nelle seguenti fasi:

fase 1: identificazione e indagine preliminare

Il Titolare del trattamento o un suo delegato compie una valutazione preliminare della notizia dell' evento segnalato, al fine di stabilire se si sia effettivamente verificata un'ipotesi di infrazione alla sicurezza di dati personali (data breach) e se sia necessaria un'indagine più approfondita dell'accaduto con il coinvolgimento del RPD.

Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Titolare del trattamento o un suo delegato dovrà coinvolgere nella procedura anche l'Amministratore di sistema.

La valutazione preliminare sarà effettuata attraverso l'esame delle informazioni riportate nella comunicazione, riguardanti in particolare:

- la data di scoperta della violazione (tempestività);
- il soggetto che è venuto a conoscenza della violazione;
- la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
- la descrizione di eventuali azioni già adottate.

fase 2: azioni di contenimento e valutazione del rischio (risk assessment)

Accertata la possibilità o il verificarsi della violazione, di comune intesa, il Titolare del trattamento o un suo delegato ed il RPD dovranno stabilire:

- se esistono azioni che possano limitare i danni potenzialmente causati dalla violazione (ad esempio, riparazione fisica di strumentazione, utilizzo delle risorse di salvataggio per recuperare dati persi o danneggiati, isolamento o chiusura di un settore compromesso della rete, cambio dei codici di accesso, ecc.) e quali siano i soggetti che devono attuare le azioni di contenimento identificate;
- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Il Titolare del trattamento e il RPD valutano la gravità della violazione e motivatamente individuano il livello di rischio connesso all'evento verificatosi o potenziale, secondo una graduazione da semplice (il rischio per i diritti e le libertà delle persone fisiche è improbabile), a medio (il rischio è probabile), ad elevato (la probabilità di verificazione del rischio è elevata). Il superamento della soglia di rischio semplice comporta l'obbligo di notificazione all'Autorità Garante, mentre l'obbligo di comunicazione agli interessati è connesso al livello di rischio elevato.

I principali parametri da tenere in considerazione durante la valutazione dell'impatto dell'infrazione di sicurezza sulla sfera personale degli interessati sono i seguenti:

- tipologia dei dati oggetto della violazione nel contesto generale del trattamento;
- grado di identificabilità degli interessati a partire dai dati violati;
- circostanze specifiche della violazione, in relazione alle cause e modalità della perdita di sicurezza dei dati e alla eventuale natura dolosa o non della stessa.

Ai fini della valutazione, potrà essere impiegata la metodologia illustrata dalla European Union Agency for Cybersecurity nel documento denominato "*Recommendations for a methodology of the assessment of severity of personal data breaches*" del dicembre 2013; in applicazione della quale, secondo le istruzioni di dettaglio dell'Allegato B, la gravità dell'incidente (**GI**) può essere determinata tramite la seguente equazione:

GI = **CT** (contesto del trattamento) × **FI** (facilità di identificazione) + **CV** (circostanze della violazione)

Nel caso in cui il valore calcolato corrisponda ad un livello di rischio semplice, il Titolare del trattamento ed il RPD prendono atto della non necessità di procedere a notifica ovvero a comunicazione, al contempo disponendo le misure di recupero ovvero di sicurezza da ripristinare o da adottare per evitare il ripetersi dell'evento in futuro.

Nel caso in cui il valore corrisponda ad un livello di rischio medio, il Titolare del trattamento ed il RPD ne prendono atto ed attivano immediatamente la procedura di cui alla *fase 3*.

Infine, nel caso in cui il calcolo restituisca un valore corrispondente ad un rischio elevato, il Titolare del trattamento ed il RPD ne prendono atto e contemporaneamente attivano la procedura di cui alla *fase* 3 ed effettuano la comunicazione di cui alla *fase 4*.

fase 3: eventuale notifica all'Autorità Garante

Qualora sia necessario effettuare la notifica all'Autorità Garante, secondo quanto prescritto dall'art. 33

del RGPD, il Titolare o un suo delegato provvede senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è stato accertato l'evento di rischio.

L'inoltro della segnalazione deve avvenire avvalendosi del servizio telematico dedicato, disponibile sul sito istituzionale del Garante, al seguente indirizzo: https://servizi.gpdp.it/databreach/s/

Nella medesima sezione del sito (https://www.garanteprivacy.it/), è possibile reperire le istruzioni e la documentazione di supporto, fra cui un fac-simile dimostrativo delle informazioni o dati che è necessario inserire durante la procedura di notifica.

fase 4: eventuale comunicazione agli interessati

Qualora sia necessario effettuare anche la comunicazione agli interessati, ossia le persone fisiche cui si riferiscono i dati violati, secondo quanto prescritto dall'art. 34 del RGPD, il Titolare o un suo delegato provvede senza ingiustificato ritardo.

La comunicazione deve contenere:

- la descrizione chiara ed esaustiva del tipo di violazione occorsa;
- il nome e i dati di contatto del Responsabile della protezione dei dati;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

La comunicazione non è richiesta quando il Titolare del trattamento abbia adottato, in precedenza ovvero anche dopo il verificarsi della violazione, misure tecniche ed organizzative adeguate, che consentano di escludere il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.

Quanto alle modalità di inoltro della comunicazione, questa dev'essere effettuata direttamente e in maniera riservata al singolo interessato, utilizzando un linguaggio chiaro e semplice, in modo da rendere comprensibile e trasparente il messaggio ed il suo contenuto. Soltanto nel caso in cui, per l'elevato numero dei potenziali destinatari ovvero per la difficoltà di identificazione degli stessi, la comunicazione a carattere individuale non è possibile o richiederebbe sforzi spropositati, allora sarà possibile procedere ad una comunicazione pubblica o similare, idonea ad informare gli interessati con analoga efficacia.

fase 5: documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione o comunicazione, in presenza di una informativa interna, redatta alla stregua del *Punto 4*, il Responsabile della protezione dei dati, eventualmente con l'ausilio dell'Amministratore di sistema, qualora la violazione riguardi dati contenuti in sistemi informatici, è tenuto a conservarne documentazione, mediante l'istituzione di un apposito Registro delle Violazioni, in cui confluiscono la detta informativa e le schede sintetiche, anche in formato tabellare, con i seguenti dati: i. n. d'ordine; ii. data violazione; iii. natura della violazione; iv. categoria di interessati; v. categoria di dati personali coinvolti; vi. numero approssimativo di registrazioni dei dati personali; vii. conseguenze della violazione; viii. contromisure adottate; ix. se sia stata effettuata notifica all'Autorità Garante; x. se sia stata effettuata comunicazione agli interessati.

Il Registro è tempestivamente aggiornato ed è messo a disposizione del Garante qualora questo, in funzione di controllo, chieda di accedervi.

Allegato A)

Informativa interna

Informativa sulla Violazione dei dati *da inoltrare al Titolare del trattamento e al Responsabile della protezione dei dati*	
nominativo e dati di contatto del soggetto segnalante	
struttura organizzativa afferente, nominativo e dati di contatto del responsabile	*Direzione, Settore, Servizio* *dirigente p.t.*
momento di verificazione della violazione	*a) data:* gg/mm/aaaa *(eventuale orario)* *b) dal* gg/mm/aaaa*, la violazione è ancora in corso* *c) dal* gg/mm/aaaa *al* gg/mm/aaaa *d) non è possibile determinare il momento*
data della constatazione o accertamento	gg/mm/aaaa *(eventuale orario)*
descrizione del tipo di violazione e delle modalità di verificazione	*ad esempio, se trattasi di:* *furto o smarrimento di dispositivi* *accesso abusivo ai sistemi* *perdita o cancellazione di dati, etc.;* *e secondo quali circostanze modali:* *luogo dell'evento, tipo di dispositivo, utilizzo di credenziali, software pericoloso, etc.*
tipologia di dati personali violati	*ad esempio, se trattasi di:* *dati anagrafici o codice fiscale,* *credenziali di accesso e di identificazione,* *dati finanziari o giudiziari,* *dati sensibili di cui all'art.9 del RGPD,* *dati relativi a condanne, reati o misure di sicurezza* *altri dati personali identificativi, etc.*
categoria di interessati coinvolti	*ad esempio, se trattasi di:* *dipendenti o collaboratori,* *terzi quali utenti o fornitori,* *soggetti che ricoprono cariche istituzionali, etc.*
numero di interessati coinvolti	*indicare:* *il numero preciso di interessati, se noto* *una stima determinata per approssimazione*

	nessuna indicazione è possibile
descrizione delle misure di sicurezza in uso e delle eventuali azioni adottate a seguito della violazione	*ad esempio:* *cifratura dei dati personali,* *utilizzo di password, antivirus e simili,* *sostituzione di credenziali,* *denuncia di furto o smarrimento* *salvataggio di copie protette*
informazioni ulteriori	

Allegato B)

Sistema di misurazione della gravità del *data breach*

La metodologia raccomandata dalla European Network and Information Security Agency (ENISA) definisce dei criteri quantitativi di valutazione dell'impatto della violazione rispetto ai diritti e alle libertà dei soggetti interessati.

La valutazione è effettuata sulla base delle informazioni raccolte nella *fase 1* di identificazione ed indagine preliminare dell'evento di rischio; è opportuno che la valutazione sia reiterata nel corso della "gestione delle violazioni", in base alle ulteriori informazioni acquisite nelle fasi successive.

I principali parametri del Sistema di misurazione sono i seguenti:

- il Contesto del Trattamento dei dati (**CT**), ossia la tipologia dei dati oggetto della violazione nel contesto generale del trattamento;
- la Facilità di Identificazione (**FI**), ossia la stima del grado di identificabilità degli interessati a partire dai dati violati;
- le Circostanze della Violazione (**CV**), ossia le circostanze specifiche della violazione, in relazione alle cause e modalità della perdita di sicurezza dei dati e alla eventuale natura dolosa o non della stessa.

Il **CT** valuta la criticità di un certo insieme di dati in uno specifico contesto di trattamento. Per calcolare tale parametro è necessario individuare la tipologia di dati personali oggetto della violazione, classificandole in almeno una delle seguenti quattro categorie:

- **semplici** (1 punto), a titolo esemplificativo possono essere dati anagrafici, dati di contatto, dati relativi ai titoli di studio e alla formazione, informazioni relative alla vita familiare, alle esperienze professionali;
- **comportamentali** (2 punti), può trattarsi di dati relativi alle preferenze e abitudini personali, dati di geolocalizzazione o dati di traffico;

- **finanziari** (3 punti), ossia qualunque tipo di dato finanziario (ad esempio: reddito, transazioni finanziarie, estratti conto, investimenti, carte di credito, ricevute, etc.), incluse le informazioni finanziarie relative alla previdenza sociale;
- **particolari** (4 punti), ossia qualunque tipo di dato particolare (ad esempio, salute, affiliazione politica, vita sessuale, etc., attinenti alle categorie di cui agli artt. 9 e 10 del RGPD).

Indicazioni più dettagliate per il calcolo del punteggio in base a circostanze specifiche sono contenute nell'Allegato l del documento di ENISA. Si precisa, in questa sede, che le credenziali di autenticazione non sono di per sé ascrivibili ad una categoria specifica, ma devono essere considerate in base alla tipologia di dati trattati nei sistemi cui danno accesso.

Dopo aver classificato il dato e assegnato un punteggio è necessario incrementarlo o diminuirlo in base al valore di fattori contestuali al trattamento dei dati.

I fattori aggravanti sono: la quantità dei dati, le speciali caratteristiche del Titolare o dei soggetti interessati.

I fattori attenuanti sono: la non validità o inaccuratezza dei dati, la disponibilità pubblica dei dati prima della violazione e la natura dei dati.

Il parametro **FI** ha effetto correttivo del **CT**. La criticità complessiva del trattamento può essere ridotta in base al valore di **FI**: minore è la facilità di identificazione e minore sarà il valore associato alla criticità complessiva.

Ai fini della presente metodologia vengono definiti quattro livelli di **FI**, con un incremento lineare nel punteggio:

- Trascurabile (0,25 punti).

- Limitato (0,50 punti).

- Significativo (0,75 punti).

- Massimo (1 punti).

Il punteggio più basso è assegnato quando la possibilità di identificare gli interessati è trascurabile, mentre il punteggio più alto è selezionato quando l'identificazione è possibile direttamente in base ai dati violati, senza che siano necessarie particolari ricerche o elaborazioni per scoprire l'identità dei soggetti interessati. Durante la definizione del valore di **FI**, devono essere tenuti in considerazione tutti i mezzi che ragionevolmente è probabile possano essere utilizzati da qualunque persona per identificare i soggetti interessati, tra cui, ad esempio, le informazioni disponibili pubblicamente, detenute o ottenute in qualunque modo, incluse quelle reperibili tramite Internet, ovvero anche incrociando dati presenti in altre fonti accessibili dal Titolare o da terze parti.

La moltiplicazione dei valori di **FI** e **CT** fornisce il ***valore inziale*** della gravità dell'incidente (**GI**).

Il parametro **CV** definisce specifiche circostanze della violazione che possono essere o non essere presenti. Nello specifico, i fattori da prendere in considerazione sono:

- **perdita di riservatezza**, che si verifica allorquando le informazioni entrano in possesso di soggetti non autorizzati o privi di un legittimo motivo per accedervi. L'entità della perdita di riservatezza può variare in base all'ambito della divulgazione (ad esempio, il numero potenziale di soggetti che possono aver avuto accesso abusivamente alle informazioni). Valore: da 0 a 0,5 punti;
- **perdita di integrità**, che avviene quando le informazioni originali sono state alterate e la sostituzione dei dati può pregiudicare i soggetti interessati. La situazione più grave si verifica quando ci sono serie

possibilità che i dati modificati siano stati usati in modo da arrecare danno ai soggetti interessati. Valore: da 0 a 0,5 punti;

- **perdita di disponibilità**, che avviene quando i dati originali non sono disponibili per l'accesso nel momento in cui se ne abbia la necessità. Può essere sia temporanea (i dati possono essere recuperati, ma dopo un periodo di tempo che può risultare dannoso per i soggetti interessati) o permanente (i dati non possono essere in alcun modo recuperati). Valore: da 0 a 0,5 punti;
- **comportamento doloso**, che ricorre allorquando la violazione non possa essere ascritta ad un errore, umano o tecnico, ma è stata causata da un'azione volontaria di tipo intenzionale. Il comportamento doloso è un fattore che può incrementare la probabilità che i dati vengano utilizzati con un intento dannoso per i soggetti interessati, potendo essere questo lo scopo originale della violazione. Valore: da 0 a 0,5 punti.

A differenza dei primi due parametri, **CT** e **FI**, ove il valore associabile è univoco, il valore complessivo del terzo parametro **CV** è determinato dalla sommatoria dei valori attribuiti a ciascuno dei fattori enunciati, atteso che in presenza della stessa violazione possono ricorrere circostanze diverse.

Il valore di **CV** deve essere sommato al ***valore iniziale*** di **GI**, in modo da definirne il ***valore finale***, secondo la seguente formula di calcolo:

$$GI = CT \bullet FI + CV$$

Il risultato ricadrà in predeterminati intervalli di valori, ciascuno corrispondente ad uno dei possibili livelli di gravità, come riportato in tabella:

valore finale GI	livello GI
inferiore o uguale a 2	basso
inferiore o uguale a 3	medio
superiore a 3	elevato

Determinato in tal modo il livello di gravità della violazione, il Titolare del trattamento ed il RPD assumono le iniziative descritte in *fase 2* della procedura di gestione del *data breach*.