CITTÁ DI PINEROLO

Città Metropolitana di Torino

ORIGINALE

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

N° 57 del 28/02/2024

OGGETTO:	**GDPR REGOLAMENTO (UE) 2016/679 – DISPOSIZIONI OPERATIVE IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONI DEI DATI PERSONALI (DATA BREACH). APPROVAZIONE AGGIORNAMENTO.**

Provv. In.	Cat. cls.	F.A.	Int.	I.	L.
57 GC 2024	01.10.02	2/2024			

L'anno **2024**, addi **ventotto**, del mese di **Febbraio**, alle ore **15:10,** presso questa sede comunale, nella solita sala delle adunanze, regolarmente convocata, si è riunita la Giunta Comunale:
Assume la presidenza Il Sindaco **Luca SALVAI**.
Assiste alla seduta Il Segretario Generale **Dott.ssa Annamaria LORENZINO.**

Intervengono i signori:

Cognome e Nome	Qualifica	Presente	Assente
SALVAI LUCA	SINDACO	X	
COSTARELLI FRANCESCA	VICESINDACO - ASSESSORE ALLO SVILUPPO ECONOMICO	X	
MILANESI FRANCO	ASSESSORE ALL'ISTRUZIONE E CULTURA	X	
DESTEFANIS BRUNA	ASSESSORE ALLO SPORT	X	
PEZZANO LARA	ASSESSORE ALLE POLITICHE SOCIALI E SANITARIE E AL LAVORO	X	
CARIGNANO LUIGI	ASSESSORE ALL'INNOVAZIONE E DIGITALIZZAZIONE	X	
VODINI FABIANO	ASSESSORE ALL'URBANISTICA E AL PATRIMONIO	X	
PROIETTI GIULIA	ASSESSORE ALL'AMBIENTE E MOBILITA' SOSTENIBILE		X

Totale Presenti: 7 Totale Assenti: 1

Il Presidente, riconosciuta legale l'adunanza, dichiara aperta la seduta ed invita la Giunta Comunale a trattare il seguente argomento:

N. 57 /GC del 28/02/2024

OGGETTO:	**GDPR REGOLAMENTO (UE) 2016/679 – DISPOSIZIONI OPERATIVE IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONI DEI DATI PERSONALI (DATA BREACH). APPROVAZIONE AGGIORNAMENTO.**

Relaziona il SINDACO

Premesso che:

- la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale e che l'articolo 8, paragrafo 1, della Carta dei Diritti Fondamentali dell'Unione Europea e l'articolo 16, paragrafo 1, del Trattato sul funzionamento dell'Unione Europea stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;
- il Comune di Pinerolo, in quanto Titolare del trattamento, è tenuto a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (data breach), incluse eventuali notifiche all'Autorità di controllo competente ed eventuali comunicazioni agli interessati;

Visto:

- il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati, di seguito "GDPR");
- il Decreto Legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, così come modificato dal Decreto Legislativo 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE»;
- il Decreto Legislativo 18 maggio 2018, n. 51, recante Attuazione della direttiva (UE) 2016/680 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;
- le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" (WP250) del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali del 3 ottobre 2017, come modificate il 10 ottobre 2022 e 28 marzo 2023 dal Comitato Europeo per la protezione dei dati;
- i Provvedimenti del Garante per la protezione dei dati personali sulla notifica delle violazioni dei dati personali (Data breach) n. 157 del 30 luglio 2019 e n. 209 del 27 maggio 2021 - Procedura telematica per la notifica di violazioni di dati personali (Data breach);

Considerato che:

- in caso di violazione dei dati personali, il Titolare del trattamento è tenuto a notificare tale evento al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la

violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (artt. 33 e 55 del GDPR, art. 2-bis del D.Lgs. 196/2003);

- il Titolare del trattamento è tenuto altresì a notificare la violazione dei dati personali al Garante con le modalità di cui all'art. 33 del Regolamento anche con riferimento al trattamento effettuato a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvo che il trattamento medesimo sia effettuato dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del Pubblico Ministero (artt. 26 e 37, comma 6, del D.Lgs. n. 51/2018);
- per «violazione dei dati personali» (data breach) si intende la 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, punto 12 del GDPR; art. 2, comma 1, lett. m, del D.Lgs. n. 51/2018);
- per la omessa notifica di data breach all'Autorità di controllo o per l'omessa comunicazione agli interessati o per entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, sono previste pesanti sanzioni amministrative (art. 83 GDPR), il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato totale annuo dell'esercizio precedente, se superiore, nonché le misure correttive di cui all'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati);
- inoltre, l'art. 82 prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere il risarcimento del danno dal soggetto al quale l'obbligo (violato) era imposto, salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile;
- lo stesso GDPR, all'art. 83 paragrafo 2, indica dei fattori che possono mitigare o aggravare la violazione e, tra questi, un elemento che può sicuramente mitigare il livello sanzionatorio, a fronte di una violazione, è legato al comportamento del Titolare che possa dimostrare come, intervenendo con tempismo ed appropriatezza, abbia fatto il possibile per ridurre la gravità, la natura e la durata della violazione;

Dato atto che con deliberazione della Giunta n. 218 del 26/06/2018 ad oggetto "Regolamento (UE) 2016/679 del 27/04/2016 in materia di protezione dei dati personali e loro libera circolazione – Disposizioni operative in materia di incidenti di sicurezza e di violazioni dei dati personali ed adozione del registro degli incidenti di sicurezza e delle violazioni dei dati personali (Data breach – par. n. 5 art. 33 GDPR)", si era dato corso all'approvazione di una prima procedura in materia, che attualmente necessita di aggiornamento in relazione alle evoluzioni delle strutture organizzative dell'ente e alle revisioni delle linee guida in materia emanate dagli Enti preposti;

Ritenuto pertanto:

a) di fondamentale importanza predisporre una procedura organizzativa interna aggiornata per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali, per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per l'Ente. A tale riguardo si precisa che sono già state attivate procedure a tutela della sicurezza dei dati, tra cui:

- l'adozione di misure organizzative e tecniche per garantire un livello di sicurezza adeguato al rischio connesso al trattamento dei dati personali e alle altre informazioni trattate, comprese misure volte al tempestivo ripristino della disponibilità in caso di incidente sulla sicurezza;
- l'organizzazione, a cadenza periodica, di corsi di formazione per i dipendenti/collaboratori sui principi cardine della normativa sul trattamento dati, sulla sicurezza dei dati personali e dei sistemi;

- la predisposizione di un sistema di protezione, mediante apposite misure tecniche, quali firewall, antivirus, dell'accesso a internet e ai dispositivi elettronici;

b) di valenza strategica per l'Ente:

- sensibilizzare il personale in ordine alle responsabilità in materia di protezione dei dati personali ed all'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli incidenti sulla sicurezza (inclusi i data breach);
- definire processi per identificare, tracciare e reagire ad un incidente sulla sicurezza e ad un data breach, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio, nonché stabilire se, in caso di data breach, si renda necessario procedere alla notifica al Garante e alla comunicazione agli Interessati;
- definire ruoli e responsabilità per la risposta agli incidenti sulla sicurezza ed i data breach;
- assicurare un adeguato flusso comunicativo all'interno della struttura comunale tra le parti interessate;
- stabilire che le procedure contemplate siano applicabili a tutte le attività svolte dal Titolare, con particolare riferimento alla gestione di tutti gli archivi e documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati, anche con il supporto di fornitori esterni;
- stabilire che il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia; considerato che le procedure medesime sono rivolte a tutti i soggetti che, a qualsiasi titolo, trattano dati personali di competenza del Titolare, quali:
  - i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto contrattuale intercorrente - abbiano accesso ai dati personali trattati nel corso delle prestazioni richieste per conto del Titolare del trattamento;
  - qualsiasi soggetto (persona fisica o persona giuridica) diverso da quelli indicati alla lettera precedente che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare. In particolare, ogniqualvolta il Titolare si trovi ad affidare il trattamento di dati ad un soggetto terzo, in qualità di responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di data breach sia oggetto di comunicazione, al fine di obbligare il responsabile ad informare il Titolare del trattamento immediatamente, senza ingiustificato ritardo, di ogni potenziale evento di violazione di dati personali;

Visto il documento "Disposizioni operative in materia di incidenti di sicurezza e di violazione di dati personali (Data breach)" ed i relativi allegati:

1) matrice di assegnazione delle responsabilità
2) Informativa sul trattamento dei dati personali
3) modulo per la segnalazione incidenti/violazioni di dati personali
4) facsimile notifica di una violazione dei dati personali al Garante

e ritenute le stesse adeguate sotto il profilo operativo alle esigenze dell'ente;

Valutata pertanto l'opportunità di procedere alla relativa approvazione;

Visti:

- il Regolamento sull'Ordinamento degli Uffici e dei Servizi;
- il D.Lgs. 267/2000 e s.m.i;
- Visto il D.Lgs. n. 165/2001 e s.m.i.;

Atteso che la presente proposta di deliberazione è corredata dai pareri favorevoli espressi dalla Dirigente del settore Segreteria Generale dott.ssa Maria Giovanna Gambino, dal Dirigente del Settore Lavori Pubblici Ing. Antonio Morrone e come Dirigente ad interim. per il settore Urbanistica, dal Dirigente del settore Polizia locale dott. Federico Battel, dalla Dirigente del settore Istruzione dott.ssa Gloria Gerlero e dal Dirigente del Settore Finanze dott. Roberto Salvaia in ordine alla regolarità tecnica;

Preso atto del parere sfavorevole sulla delibera espresso dalla Segretaria Comunale dott.ssa Annamaria Lorenzino, si approva ugualmente la delibera in quanto il parere non inficia la legittimità del provvedimento ma esprime contrarietà alla procedura di acquisizione multipla dei pareri di regolarità tecnica espressi dal dirigenti;

Di dare atto che la presente deliberazione non comporta riflessi diretti o indiretti sulla situazione economico - finanziaria o sul patrimonio dell'Ente e pertanto, ai sensi del medesimo articolo, non necessita del parere di regolarità contabile;

Con voti unanimi espressi nelle forme previste dall'art. 11 del Regolamento per il funzionamento della Giunta comunale;

DELIBERA

1) di approvare, per le motivazioni in narrativa esposte che qui si intendono integralmente richiamate, le "Disposizioni operative in materia di incidenti di sicurezza e di violazione di dati personali (Data breach)" del Comune di Pinerolo, e relativi allegati da 1) a 4), che costituiscono parte integrante e sostanziale della presente deliberazione;

2) di demandare la concreta attuazione delle misure regolamentari minime contenute nelle disposizioni operative al personale operante all'interno dell'Ente nelle sue articolazioni gerarchiche e secondo le loro rispettive funzioni e competenze;

3) di disporre che al presente provvedimento venga assicurata la massima diffusione presso tutto il personale operante presso l'Ente e presso i soggetti esterni qualificabili in termini di responsabili del trattamento e la pubblicazione sul sito web istituzionale;

4) di disporre che, in conformità all'art. 125 del D.Lgs. 267/2000, la presente deliberazione, contestualmente all'affissione all'albo pretorio, sia trasmessa in elenco ai capigruppo consiliari;

5) di dichiarare, con separata votazione, a voti unanimi espressi nelle forme previste dall'art. 11 del Regolamento per il funzionamento della Giunta comunale, la presente deliberazione immediatamente eseguibile ai sensi e per gli effetti dell'art. 134, comma 4, del D.Lgs. 267/2000, al fine di garantire la sollecita operatività delle disposizioni in oggetto.

CITTÀ di PINEROLO

DISPOSIZIONI OPERATIVE IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Approvato con Deliberazione della Giunta Comunale n. 57 del 28.02.2024

Indice

GLOSSARIO

- **GDPR** - Regolamento Europeo in materia di protezione dei dati personali nonché della libera circolazione di tali dati che abroga la direttiva 95/46/CE sulla stessa materia. Pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04/05/2016, entrato in vigore il 24/05/2016 e diventerà definitivamente applicabile in via diretta in tutti i paesi UE a partire dal 25/05/2018. L'acronimo GDPR si riferisce al termine anglosassone "*General Data Protection Regulation*" mentre l'acronimo RGPD si riferisce alla definizione nazionale "Regolamento Generale sulla Protezione dei Dati".
- **GPDP** – Garante privacy - Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996 n. 765, quale autorità amministrativa pubblica di controllo indipendente, il GDPR identifica questa figura denominandola "Autorità di controllo" (vedasi art.li n. 51 e successivi del GDPR).
- **Titolare del trattamento** - l'Amministrazione Comunale, nella persona del legale rappresentante – Sindaco pro-tempore, che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali.
- **Responsabile del trattamento** - soggetto pubblico o privato, che tratta dati personali per conto del Titolare del trattamento.
- **Data Breach** – evento in conseguenza del quale si verifica una "**violazione dei dati personali**". Con il termine "data breach" si intende un incidente di sicurezza in cui dati: personali, sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato.
- **DPO** – (Data protection officer) Responsabile della protezione dei dati personali.
- **Referenti privacy –** dipendenti designati all'interno di ogni settore organizzativo per gli adempimenti e processi relativi al GDPR – (es. aggiornamento applicativo informatico di ente DPM).
- **RTD** – Responsabile per la Transizione Digitale. Coordinamento dello sviluppo di sistemi informativi e servizi online in conformità ai principi di *data protection by default* e *by design.*
- **Rtd** – Responsabile del trattamento delegato: fornitore esterno a cui è stata assegnata una attività di Trattamento.

INTRODUZIONE

Per "***Data Breach*"** si intende un evento in conseguenza del quale si verifica una "**violazione dei dati personali**". Con questo termine ci si riferisce ad un incidente di sicurezza in cui dati: personali, sensibili, protetti o riservati vengono: distrutti, consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato.

L'art. 33 del GDPR impone al titolare del trattamento di **notificare all'autorità di controllo la violazione di dati personali entro settantadue ore dal momento in cui il titolare ne viene a conoscenza**.

Il termine delle settantadue ore non è perentorio, tuttavia nel caso in cui questo termine sia superato, unitamente alla notifica occorre giustificare i motivi del ritardo. La notifica al garante non è necessaria quando sia improbabile che la violazione dei dati personali presenti un rischi per i diritti e le libertà delle persone fisiche.

Il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati) e la imposizione di sanzioni amministrative (secondo l'art. 83 GDPR, l'importo può arrivare a 10.000.000 di euro o al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore).

La mancata notifica può inoltre dare luogo ad ulteriori accertamenti da parte del Garante in quanto può rappresentare un indizio di carenze più profonde e strutturali che se accertate possono dar luogo ad ulteriore irrogazione di sanzioni.

Inoltre quando la violazione dei dati è suscettibile di presentare rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve comunicare la violazione all'interessato senza ingiustificato ritardo (art. 33 del GDPR).

Tutti gli eventi di "data breach", compresi quelli per cui non sono necessarie le notifiche, devono essere documentati dal Titolare ivi incluse le circostanze, le conseguenze e i provvedimenti adottati su un registro tenuto, per estensione, secondo le indicazioni fornite dal Garante.

E' importante tenere presente che, ai sensi dell'art. 24 del GDPR, il Titolare deve mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato in conformità del regolamento europeo.

DEFINIZIONE DI VIOLAZIONE DEI DATI ("*DATA BREACH*")

Come in precedenza accennato, per **"Violazione di dati**" o "***data breach***" si intende "l*a 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 GDPR).

In particolare si intende un evento in grado di provocare (*Considerando 75 GDPR*) danni fisici, materiali o immateriali alle persone fisiche (perdita di controllo dei dati personali, limitazioni nei diritti, discriminazione, furto, usurpazione di identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione perdita di riservatezza di dati protetti da segreto professionale, danni economici o sociali ecc..).

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 o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Si possono distinguere tre categorie di violazioni di dati:

a) **violazione della riservatezza**: quando si ha una divulgazione di dati o un accesso agli stessi non autorizzato o accidentale;
b) **violazione dell'integrità**: quando il dato è alterato in modo accidentale o non autorizzato;
c) **violazione della disponibilità**: quando in modo accidentale o per dolo il Titolare non accede ai dati o i dati sono stati distrutti.

Una violazione di dati personali può comprendere una o tutte e tre le categorie o anche loro combinazioni.

Una violazione della riservatezza o dell'integrità del dato è facilmente individuabile. Meno chiara è l'individuazione di una violazione della disponibilità del dato. Ci sarà sempre una violazione della disponibilità del dato nel caso di perdita o distruzione permanente dei dati. L'indisponibilità dei dati è quindi da considerare una violazione quando potrebbe avere un impatto significativo sui diritti e le libertà delle persone fisiche. Non si tratta invece di una violazione quando l'indisponibilità è dovuta a interruzioni programmate per la manutenzione.

A titolo esemplificativo e non esaustivo, le violazioni di dati personali possono includere:

1. divulgazione di dati personali a soggetti non autorizzati;
2. perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
3. perdita o furto di documenti cartacei;
4. distruzione accidentale di documenti cartacei o banche dati;
5. infedeltà aziendale (ad esempio: Data Breach causato da una persona interna che, avendo autorizzazione ad accedere ai dati, ne produce una copia che viene distribuita in ambiente pubblico);
6. accesso abusivo (ad esempio: Data Breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
7. casi di pirateria informatica (usurpazione delle credenziali di accesso – fishing);
8. banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
9. virus o altri attacchi al sistema informatico o alla rete aziendale;
10. violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o armadi contenenti archivi con informazioni riservate);
11. smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
12. invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

A CHI SONO RIVOLTE QUESTE DISPOSIZIONI

Queste disposizioni **sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento**:
a) i lavoratori dipendenti, nonché coloro che a qualsiasi titolo, e quindi a prescindere dal tipo di rapporto contrattuale intercorrente, abbiano accesso ai dati personali trattati nel corso delle prestazioni richieste per conto del Titolare del trattamento;
b) qualsiasi soggetto (persona fisica o persona giuridica) diverso dal destinatario interno che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento, abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare;
Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.
La definizione dei ruoli e delle responsabilità che spettano ad ogni interessato per l'esecuzione delle attività relative alle varie fasi è espressa sotto forma di matrice "RACI", in Allegato 1).

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI

L'Amministrazione è tenuta, **entro 72 ore dalla conoscenza di una violazione di dati personali** che presenti un rischio per i diritti e le libertà degli interessati, alla notifica al Garante e, in caso di accertata elevata gravità del rischio, alla comunicazione agli interessati.
Le informazioni relative all'incidente devono essere raccolte e trasmesse al più presto all'indirizzo violazionedati@comune.pinerolo.to.it.
Se al momento della rilevazione dell'incidente di sicurezza non è disponibile una descrizione particolareggiata dell'evento, è comunque essenziale **procedere immediatamente alla comunicazione dell'incidente per una sollecita valutazione di gravità, anche con informazioni incomplete**.
La valutazione sarà integrata con le informazioni che vengono acquisite nella prosecuzione dell'indagine.

Il Sindaco, su proposta del RTD e del DPO, individua un gruppo di supporto per la gestione delle segnalazioni delle violazioni dei dati denominato **"Unità di risposta"** e composto dal DPO, dal RTD e dai dipendenti preventivamente incaricati al presidio dell'indirizzo violazionedati@comune.pinerolo.to.it.
A seconda del caso il gruppo può includere anche il fornitore nominato Responsabile del Trattamento.

1. Fase 1. Procedura interna di rilevazione e segnalazione di una potenziale violazione

Per garantire il rispetto dei tempi di risposta imposti dal GDPR (72 ore), è necessario segnalare al team di risposta (violazionedati@comune.pinerolo.to.it) **senza immotivato ritardo**, e comunque **non oltre 8 ore dall'avvenuta conoscenza** di un incidente di sicurezza, un'eventuale violazione dei dati personali trattati dall'Amministrazione.
È opportuno segnalare qualsiasi tipo di incidente di sicurezza, anche lieve e connesso ai dati personali, per consentire di valutare la gravità e le conseguenze per gli interessati e aggiornare il "Registro delle violazioni dei dati", che permette una costante analisi del rischio e di predisporre adeguate misure di prevenzione.

1.1. Rilevazione di un incidente di sicurezza

Chi	Chiunque ne venga a conoscenza (soggetti autorizzati, personale, collaboratori, fornitori, Responsabile del trattamento, utenti esterni, DPO)
A chi	Dirigente del Settore, Referenti privacy e Titolare per conoscenza
Quando	Immediatamente
Come	Comunicando l'incidente di sicurezza al Dirigente del Settore e ai Referenti privacy, anche per le vie brevi (telefonicamente, di persona, via e-mail)

Ogni dipendente, collaboratore o soggetto che a qualsiasi titolo ha accesso ai dati personali trattati "da" o "per conto" dell'Amministrazione, deve individuare e segnalare **immediatamente** al responsabile della propria struttura e al referente organizzativo privacy, una violazione dei dati (anche se solo sospetta), che abbia colpito il suo sistema o il suo ufficio.

Nel caso in cui la segnalazione sia raccolta da persone fisiche esterne all'ente è opportuno che chi riceve la segnalazione provveda anche a raccogliere informazioni di contatto sul/i segnalatori (indirizzo di reperibilità, numeri telefonici, indirizzo di posta elettronica). Chi raccoglie la segnalazione dovrà inoltre fornire al segnalante un'informativa circa le modalità e finalità con cui i dati conferiti saranno trattati. E' opportuno che l'informativa sia resa per iscritto. Nell'allegato n. 5 al provvedimento con cui si approva il presente documento è riportato un modello utilizzabile per rendere tale informativa a chi segnala un "*data breach*" (presunto o effettivo).

È opportuno segnalare qualsiasi tipo di incidente di sicurezza, anche lieve e connesso ai dati personali, per consentirne la gestione e valutare la gravità e le conseguenze per gli interessati. Ciò consentirà all'Amministrazione di mantenere un registro degli incidenti aggiornato, che permette una costante analisi del rischio e di predisporre adeguate misure di prevenzione.
Nel caso in cui il computer fisso, il pc portatile, hard disk, chiavette USB o altri supporti di memoria fossero oggetto di furto o smarrimento, occorre segnalare immediatamente l'avvenimento.
Vanno segnalati anche tutti gli incidenti comunque correlati ai dati personali, quali furto di informazioni effettuate online, cancellazione accidentale di informazioni, comunicazione di informazioni a terzi per errore. Ciò anche se non vi è stato un comportamento intenzionale alla base, ma un evento accidentale.
Va inteso come *data breach* anche un attacco di *phishing* andato a buon fine, ossia l'aver fornito o diffuso credenziali e dati tecnici a un soggetto terzo.

1.2. Prima valutazione delle possibili conseguenze e contromisure

Chi	Dirigente del Settore, Referenti privacy
Quando	Immediatamente dopo la ricezione della segnalazione
Come	Coordinando la raccolta delle informazioni, eventualmente con il supporto degli amministratori di sistema della struttura

Appena riceve una segnalazione, il Dirigente del Settore, anche tramite i referenti privacy coinvolti e, se necessario, con supporto degli amministratori di sistema competenti, deve:

a) coordinare la raccolta delle informazioni nel più breve tempo possibile;

b) valutare se si tratta di una violazione di dati "personali";

c) disporre l'adozione delle contromisure necessarie per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi;

d) trasmettere il modello per la segnalazione delle violazioni a violazionedati@comune.pinerolo.to.it .

1.3. Segnalazione all'Unità di risposta (violazionedati@comune.pinerolo.to.it)

Chi	Dirigente del Settore, Referenti privacy
A chi	Unità di risposta (DPO, RTD e collaboratori designati e Titolare p.c.)
Quando	Immediatamente e comunque **non oltre 8 ore** dalla conoscenza dell'evento
Come	Inviando il *"Modulo per la segnalazione incidenti/violazioni di dati personali"* a violazionedati@comune.pinerolo.to.it

Se l'incidente di sicurezza ha comportato la violazione di dati "personali", il responsabile della struttura e i referenti organizzativi privacy devono fornire tempestivamente informazioni più dettagliate possibile su ciò che è accaduto, compilando l'apposito **modulo di segnalazione** (in Allegato 3).
Il modulo compilato, **entro 8 ore** lavorative dall'avvenuta conoscenza dell'evento, deve essere trasmesso al team di risposta all'indirizzo violazionedati@comune.pinerolo.to.it.
Se al momento della rilevazione dell'incidente di sicurezza non è disponibile una descrizione particolareggiata dell'evento, è comunque essenziale procedere immediatamente alla comunicazione **anche con informazioni incomplete**.
Le informazioni più importanti sono:

A. tipo di dati violati;

B. dati particolari (ex sensibili) eventualmente violati;

C. numero di soggetti coinvolti;

D. soggetti minori eventualmente coinvolti;

E. estensione dell'incidente di sicurezza;

F. periodo temporale dell'incidente;

G. misure di sicurezza adottate;

H. cifratura o meno dei dati violati.

2. Fase 2. Gestione della segnalazione da parte dell'Unità di risposta

L'Unità di risposta, in collaborazione con i soggetti segnalanti, i responsabili e i referenti privacy delle relative strutture, celermente a:

1. Valutare l'impatto dell'incidente di sicurezza
2. Individuare le possibili contromisure
3. Notificare la violazione al Garante (se necessario)
4. Comunicare la violazione agli interessati coinvolti (se necessario)
5. Aggiornare il Registro delle violazioni dei dati personali

2.1. Valutazione di gravità dell'incidente di sicurezza

Chi	DPO e team di risposta, in collaborazione con il dirigente e i referenti privacy del settore interessato
Quando	Immediatamente, appena ricevuta la segnalazione
Come	Valutando il **rischio** [= gravità *x* probabilità] dell'impatto della violazione sui diritti degli interessati, in base a parametri predeterminati

L'Amministrazione, per mezzo del DPO e dell'Unità di risposta, in collaborazione con i soggetti segnalanti e coinvolti dall'incidente di sicurezza, valuta l'impatto della violazione dei dati personali per i diritti e le libertà delle persone fisiche, al fine di stabilire il **rischio** *[= gravità x probabilità]* e le **conseguenti azioni** che deve intraprendere:
a) adozione di misure per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi;
b) notifica della violazione al Garante privacy, a meno che sia improbabile un rischio per i diritti e le libertà delle persone fisiche;
c) comunicazione agli interessati, se il rischio è elevato *[gravità x probabilità]*^{n}.

La tabella seguente presenta i principali fattori che devono essere considerati nella valutazione di impatto della gravità di una violazione sulla base delle informazioni raccolte.

FATTORI DA CONSIDERARE PER LA VALUTAZIONE DELLA GRAVITÀ DELLA VIOLAZIONE	
Gravità e probabilità	Valutazione della gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche e della probabilità che tale impatto si verifichi
Tipo di violazione	Divulgazione, Distruzione e Modifica, Perdita
Causa della violazione	Interna, esterna identificata, non identificabile
Natura, carattere sensibile e volume dei dati personali	Categorie particolari di dati o combinazione di dati personali, grandi quantità di dati personali relative a molte persone coinvolti nella violazione
Facilità di identificazione delle persone fisiche	Facilità di identificazione, diretta o indiretta tramite abbinamento con altre informazioni, di specifiche persone fisiche sulla base dei dati personali compromessi dalla violazione
Gravità delle conseguenze per le persone fisiche	Danno potenziale alle persone fisiche che potrebbe derivare dalla violazione comprese le categorie degli interessati e dei dati personali coinvolti e la permanenza a lungo termine delle conseguenze del danno (furto di identità, danni fisici, disagio psicologico, danni di immagine/reputazione)
Caratteristiche particolari del titolare	Nel contesto delle sue attività istituzionali l'Università è, in particolare, titolare dei dati personali trattati per le finalità di ricerca
Caratteristiche particolari dell'interessato	La violazione coinvolge in particolare dati personali di minori o altre persone fisiche vulnerabili
Numero di persone fisiche coinvolte	Numero di persone fisiche coinvolte nella violazione

Quale ausilio al processo decisionale riguardo all'assolvimento degli obblighi in materia di **«Notifica di una violazione dei dati personali all'autorità di controllo»** (art.33 GDPR) e di **«Comunicazione di una violazione dei dati personali all'interessato»** (art.34 GDPR), verrà utilizzata la procedura di "Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali" messa a disposizione dal Garante nella sezione del sito istituzionale dedicata alla "Notifica di una violazione dei dati personali" (in allegato 4 facsimile della comunicazione), all'indirizzo:
https://servizi.gpdp.it/databreach/s/self-assessment .

2.2. Adozione di contromisure e azioni correttive

Chi	DPO e Unità di risposta
Quando	Contestualmente alla valutazione di impatto
Come	in collaborazione con il responsabile della struttura, i referenti privacy e gli amministratori di sistema delle strutture coinvolte

L'Unità di risposta, in collaborazione con il dirigente responsabile, i referenti privacy e gli amministratori di

sistema, individua le misure che possono essere adottate per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.
La tempestività dell'adozione delle contromisure **può ridurre il rischio** per i diritti e le libertà degli interessati, facendo venir meno l'obbligo di notifica al Garante privacy o di comunicazione agli interessati.

2.3. Notifica della violazione al Garante (se necessario)

Chi	Titolare del trattamento, sentito DPO
A chi	Garante per la protezione dei dati personali
Quando	senza ingiustificato ritardo → necessità di motivazione se la notifica non avviene **entro 72 ore dalla conoscenza** della violazione
Come	Inviando il Modello di notifica data breach tramite la procedura on line prevista all'indirizzo **https://servizi.gpdp.it/databreach/s/scelta-auth**

Se la violazione dei dati personali rappresenta un **rischio** per i diritti e le libertà delle persone fisiche, **il Titolare del trattamento o suo delegato, sentito il DPO**, deve notificare il modulo compilato al Garante privacy tramite la procedura telematica dedicata alla "Notifica di una violazione dei dati personali (data breach)" sulla relativa sezione del sito istituzionale.
La notifica al Garante deve essere effettuata dal titolare del trattamento senza ingiustificato ritardo e, ove possibile, **entro 72 ore dalla conoscenza** della violazione, mediante i sistemi telematici indicati nel sito istituzionale del Garante.
In caso di ritardo, è necessario motivare le **ragioni del ritardo** che hanno impedito la tempestività della notifica.
Se al momento della rilevazione dell'incidente di sicurezza non è disponibile una descrizione particolareggiata dell'evento, è comunque essenziale procedere immediatamente alla comunicazione anche con **informazioni incomplete**. La documentazione verrà integrata in un secondo momento, in collaborazione con il Garante privacy.

2.4. Comunicazione agli interessati coinvolti (se necessario)

Chi	Responsabile della protezione dei dati (DPO)
A chi	Persone fisiche i cui dati personali sono stati violati (interessati)
Quando	Senza ingiustificato ritardo
Come	Contattando direttamente gli interessati oppure rendendo nota la violazione e le possibili conseguenze mediante pubblicazione accessibile alle categorie di interessati

Se la violazione dei dati presenta un rischio "elevato" per i diritti e le libertà delle persone fisiche, la comunicazione agli interessati deve essere fatta senza indugio. L'eventuale ritardo nella notificazione deve essere giustificato. La comunicazione agli interessati deve contenere:
a) il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
b) la descrizione delle probabili conseguenze della violazione dei dati personali;
c) la descrizione delle misure adottate, o di cui si propone l'adozione da parte dell'Amministrazione, per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.

La comunicazione avviene preferibilmente su base individuale per e-mail se disponibile(PEC o ordinaria) ed eventualmente via posta raccomandata se noti i recapiti.
Se la segnalazione diretta agli interessati richiede uno sforzo ritenuto sproporzionato, è possibile utilizzare forme di comunicazione pubblica (es. comunicazione su sito istituzionale), a condizione che questa modalità non rappresenti a sua volta un rischio per la protezione dei dati personali degli interessati.

2.5. Registro delle violazioni dei dati personali

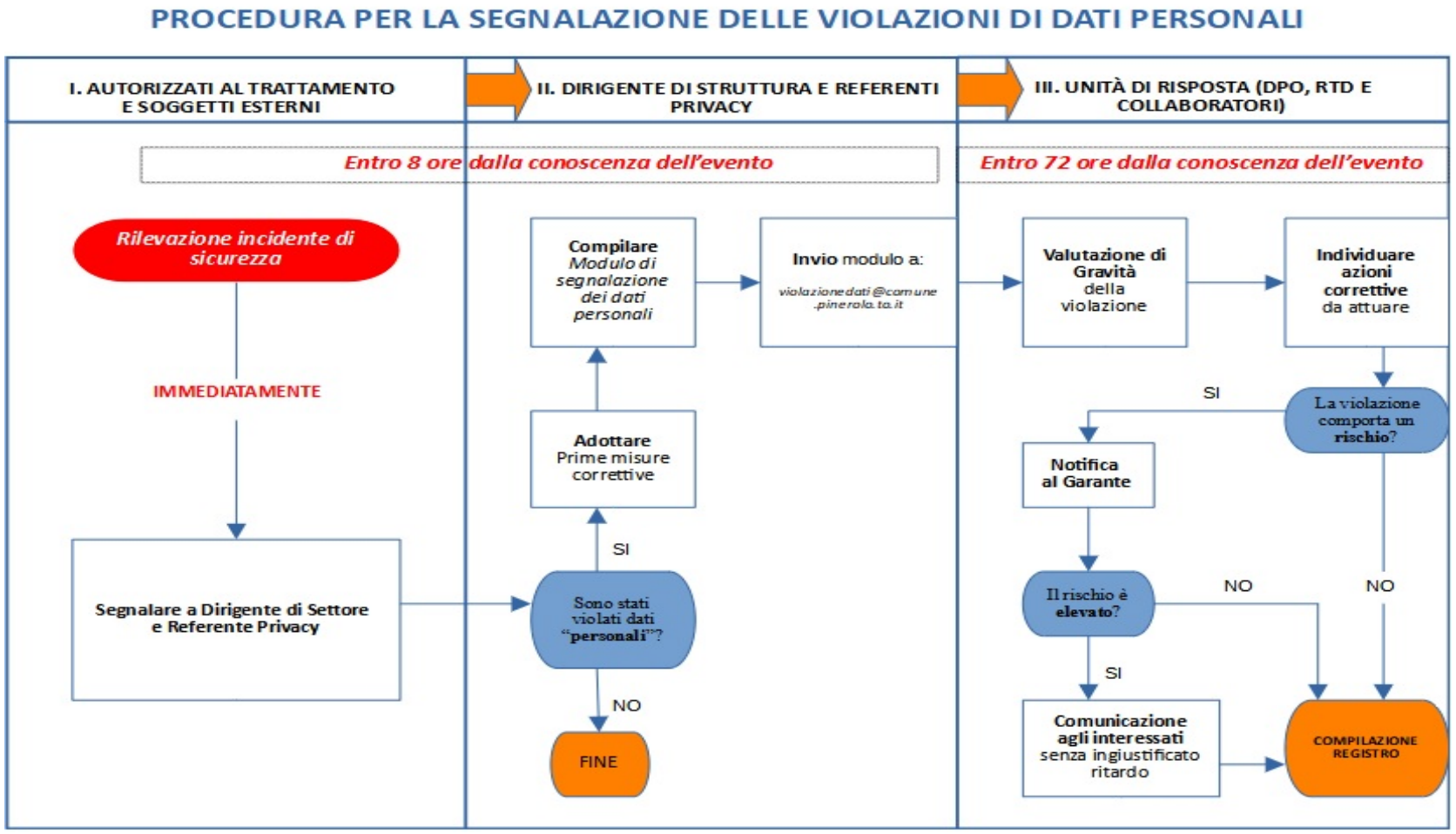
Indipendentemente dalla valutazione circa la necessità di procedere a notificazione o comunicazione della violazione di dati personali, l'unità di risposta documenta tutte le violazioni di dati personali, ai sensi dell'art. 33, par. 5, GDPR, annotandole nell'apposito Registro disponibile nell'applicativo informatico di gestione degli adempimenti connessi al GDPR.

Il Registro data breach è regolarmente aggiornato dall'Unità di risposta di risposta supportata dal DPO ed è messo a disposizione del Garante per la protezione dei dati personali, qualora ne faccia esplicita richiesta.

Elenco allegati

Allegato 1 – Matrici RACI.
Allegato 2 – Informativa da rendere a chi effettua una segnalazione di "data breach".
Allegato 3 – Modulo per la segnalazione violazione di dati personali.
Allegato 4 – Facsimile comunicazione al garante.

DIAGRAMMA PROCEDURA



MATRICE DI ASSEGNAZIONE DELLE RESPONSABILITÀ

In questa sezione del documento, sotto forma di matrice "RACI" sono poste in relazione le principali risorse umane con le attività delle quali sono responsabili per l'attuazione delle varie fasi del processo di "*data breach*".
Di seguito sono fornite due diverse matrici, la prima contempla le attività da eseguire in caso di "*data breach*" impattante su risorse informatiche mentre la seconda per le attività relative ad incidente su risorse analogiche.
Nel caso di "*data breach*" che impatti sia su risorse informatiche che analogiche si dovranno seguire entrambe le matrici per la parte di riferimento.

Ruoli chiave

La matrice prende la propria denominazione dalle iniziali dei ruoli previsti (in lingua inglese) per l'esecuzione delle attività dei processi aziendali. I ruoli previsti dalla matrice sono:

- **A - (Accountable)** è il responsabile dell'attività e/o colui che la approva (ci può essere una sola A per ogni attività);
- **R - (Responsible)** è il responsabile dell'esecuzione dell'attività, la dirige o per conto del quale l'attività è eseguita (possono esserci più R per ogni attività);
- **C - (Consulted)** rappresenta i soggetti che i responsabili (A ed R) avranno bisogno di consultare o che eseguono attività sotto la loro supervisione;
- **I – (Informed)** sono i soggetti (fisici o giuridici, interni od esterni) che non hanno bisogno di essere coinvolti attivamente nella parte del progetto in capo all'ente ma che devono essere informate relativamente a come progredisce o alle quali è necessario rivolgersi per le parti non di competenza del comune.

Definizione delle figure coinvolte

Figura	Descrizione della figura
Titolare	Intera amministrazione comunale, le azioni sono compiute dal suo legale rappresentate (Sindaco) o suo sostituto
Segretario Comunale	Segretario Comunale
Resp. Anticorruzione e Trasparenza	Responsabile Anticorruzione e Trasparenza (art. 7 L. 190/2012 e art. 43D,Lgs n. 33/2013)
RPD	Responsabile della protezione dei dati (art. 37 GDPR)
Responsabile/i interno del trattamento	Soggetto delegato dal Titolare per sovrintendere alle operazioni di trattamento
Responsabile del Trattamento Esterno	Soggetto esterno nominato "Responsabile" dal Titolare (art. 28 GDPR)
Resp. Sistemi informativi	Soggetto delegato dal Titolare per sovrintendere alle operazioni di trattamento eseguite con strumenti informatici. La figura può coincidere con quella di responsabile per la transizione al digitale (art. 17 CAD)
Resp. Conservazione digitale/sostitutiva	Soggetto nominato ai sensi del DPCM 03/12/2013 (regole tecniche in materia di conservazione)
RTD/Resp. Archivi	Soggetto nominato Responsabile per la transizione al digitale e del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (art. 3 DPCM 3/12/2013 e art. 61 D.P.R. 445/2000)
Resp. Violazione	Colui o coloro a cui è attribuibile la violazione di sicurezza
Garante Privacy	Autorità nazionale a tutela dei diritti derivanti dalle norme sulla protezione dei dati personali
Forze dell'ordine	Organo di polizia o Magistratura a cui viene denunciata la violazione di sicurezza se ne ricorrono gli estremi
Interessati	Persone fisiche i cui dati sono stati coinvolti nell'incidente

Una persona fisica può ricoprire anche simultaneamente più figure.
Ne caso di assenza o indisponibilità si devono utilizzare i criteri di sostituzione previsti dalla normativa o nei provvedimenti interni appositamente assunti, in particolare:

- il sindaco è sostituito dal Vicesindaco e nel caso dal Consigliere anziano o loro delegato;
- il Segretario Generale è sostituito dal Vice Segretario o loro delegato;
- i Delegati al trattamento ed il Delegato ai Sistemi informativi sono sostituite dai soggetti previsti con i decreti sindacali per la sostituzione delle figure dirigenziali.

Allegato 1

Matrice RACI per “data breach” impattante su risorse analogiche

fasi							
Figure coinvolte	Rilevazione Acquisizione	Gestione Tecnica e Analisi	Valutazione	Notifica al Garante	Segnalazioni (Forze dell'ordine)	Comunicazioni interessati e riscontri	Registrazione della violazione
Titolare / Sindaco	I	I	A	A	A	R	A
Segretario Comunale	I	I	C	I	I	I	I
Resp. Anticorruzione e Trasparenza		C	C	I	I	I	I
RPD	C	C	C	R	C	R	C
Responsabile/i interno al trattamento	R	R	R	C	R	R	R
Resp. Trattamento Esterno (se coinvolto)	R	R/A	R	C	R	R	C
Resp. comunicazione		I	I	I		C	I
RTD/Resp. Archivi	A	A/R	C	C	R	A	I
Resp. Violazione		C	I		I		
Garante Privacy				I		I	I
Forze dell'ordine					I		
Interessati						I	

Matrice RACI per “data breach” impattante su risorse informatiche

fasi							
Figure coinvolte	Rilevazione Acquisizione	Gestione Tecnica e Analisi	Valutazione	Notifica al Garante	Segnalazioni (Forze dell'ordine)	Comunicazioni interessati e riscontri	Registrazione della violazione
Titolare / Sindaco	I	I	A	A	A	R	A
Segretario Comunale	I	I	C	I	I	I	I
Resp. Anticorruzione e Trasparenza		C	C	I	I	I	I
RPD	C	C	C	R	C	R	C
Responsabile/i interno al trattamento	R	R	R	C	R	C	R
Resp. Trattamento Esterno (se coinvolto)	R	R/A	R	R	R	R	C
Responsabile comunicazione		I	I	I		C	I
Resp. Sistemi Informativi	R	C	C	C	R	R	C
Resp. Conservazione digitale/sostitutiva	R	I	C	I	I	I	I
RTD/Resp. Archivi	A	R	R	R	R	A	I
Resp. Violazione		C	I		I		
Garante Privacy				I		I	I
Forze dell'ordine					I		
Interessati						I	

CITTÀ di PINEROLO

Allegato 2

Informativa sul trattamento dei dati personali

Resa ai sensi degli artt.li n. 13 e n. 14 del Regolamento Europeo n. 679/2016 (GDPR - General Data Protection Regulation) relativa al seguente trattamento di dati personali.

Soggetti interessati: Sono interessate al trattamento dei dati coloro che segnalano al Comune una violazione di dati personali o malfunzionamenti che abbiano comportato, causino o possano causare un rischio per i diritti e le libertà delle persone fisiche.
Il trattamento dei dati oggetto della presente informativa sarà sempre improntato ai principi di correttezza, liceità, trasparenza e di tutela della riservatezza e dei diritti dei soggetti interessati. Inoltre si forniscono le informazioni di seguito riportate:

Titolare del trattamento è l'Amministrazione del Comune di Pinerolo (con sede in Piazza Vittorio Veneto 1, 10064 - Pinerolo TO – Italia; e-mail: protocollo@comune.pinerolo.to.it - PEC: protocollo.pinerolo@cert.ruparpiemonte.it ; Centralino telefonico: +39 0121.361.111 – sito web: http://www.comune.pinerolo.to.it) questo ente tratterà i dati personali da Lei conferiti con modalità anche informatiche e telematiche. Soggetti delegati: Dirigenti di tutti i settori dell'Amministrazione Comunale.

Responsabile per la protezione dei dati (DPO): Il Titolare, ai sensi dell'art. n. 37 del Regolamento Europeo 679/2016, ha designato il Responsabile della Protezione ANCI DIGITALE SPA; Referente incaricato Avv. Fabrizio Brignolo, e-mail: fabrizio.brignolo@libero.it, PEC: brignolo.fabrizio@ordineavvocatiasti.eu, recapito telefonico: + 39 0141/436252.

Attenzione: Poiché i recapiti dell'ente e del DPO possono variare con il trascorrere del tempo (in particolare quelli che riguardano gli indirizzi di posta elettronica i numeri di telefono come può essere diverso lo stesso soggetto incaricato come DPO) prima di inoltrare comunicazioni o richieste al Comune o al DPO è sempre necessario verificare l'esattezza delle informazioni in questione anche per via telefonica o consultando il sito internet ufficiale dell'ente dove le informazioni sui recapiti sono rese pubbliche e mantenute aggiornate.
Finalità e liceità (base giuridica) del trattamento: I trattamenti a cui saranno sottoposti i dati personali, che saranno acquisiti e periodicamente aggiornati, hanno le finalità previste di:
1) Adempiere ad obblighi previsti da leggi, regolamenti e normativa comunitaria, ovvero in esecuzione di disposizioni impartite da autorità a ciò legittimate o esecuzione di compiti nell'interesse pubblico in materia di protezione e tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. In particolare con riferimento alle violazioni di dati personali che possono comportare (accidentalmente o in modo illecito) la: distruzione, perdita, modifica, divulgazione o l'accesso non autorizzati ai dati personali trasmessi, conservati o comunque trattati da parte del comune di Pinerolo.
2) La finalità di protezione e tutela delle persone di cui al punto precedente può comportare azioni, svolte nell'interesse pubblico, di prevenzione, accertamento, o repressione di reati o comportamenti fraudolenti.
Il trattamenti dei dati saranno effettuato per ottemperare alle disposizioni contenute:
3) Nel Regolamento Europeo n. 679/2016 in materia di protezione dei dati personali nonché della libera circolazione di tali dati.
4) Nella normativa nazionale in materi di sicurezza tra cui: Codice Penale, del D.Lgs, n. 83/2005 (Codice dell'Amministrazione Digitale), della Circolare dell'Agenzia per l'Italia Digitale n. 2/2017, del D.Lgs m. 65/2018 (di recepimento della direttiva UE n. 2016/1148 del Parlamento Europeo e del Consiglio – direttiva NIS).
Natura obbligatoria o facoltativa nel conferimento dei dati: tenuto conto delle finalità illustrate in precedenza, il conferimento dei dati è facoltativo tuttavia il loro mancato, parziale o inesatto conferimento potrebbe comportare l'impossibilità di individuare ed accertare violazioni di dati personali o malfunzionamenti che causino o possano causare un rischio per i diritti e le libertà delle persone fisiche. L'artificioso parziale o inesatto conferimento dei dati potrebbe dare inoltre ad azioni legali da parte di questo Ente.

Destinatari o categorie di destinatari (ambito di diffusione/comunicazione dei dati): I dati personali saranno:

- trattati dal Titolare e dalle persone da lui autorizzate o incaricate;
- potranno essere inseriti in atti e documenti conservati negli archivi, anche elettronici, dell'ente e/o inviati in conservazione sostitutiva in conformità alle norme sulla conservazione della documentazione amministrativa;
- comunicati al garante per la Protezione dei dati Personali;
- comunicati all'Agenzia per l'Italia Digitale o a strutture in essa ricomprese
- comunicati alla Magistratura;
- comunicati alle forze dell'ordine;
- eventualmente comunicati a strutture europee costituite nell'ambito della protezione dei dati personali.

Trasferimento a terzi dei dati: I dati oggetto della presente informativa non saranno trasferiti in paesi terzi né ad organizzazioni internazionali;

Periodo di conservazione dei dati: ai sensi del Codice Civile (artt.li n. 822 e n. 824 – demanio pubblico), del D.Lgs n. 42/2004 (patrimonio culturale nazionale) e della normativa in materia di documentazione amministrativa i dati gestiti dagli enti pubblici sono inalienabili ed appartengono al patrimonio culturale nazionale. La loro eventuale distruzione (scarto archivistico) è subordinata ad autorizzazione ministeriale. Inoltre i dati possono anche essere inseriti all'interno di atti e documenti destinati all'archiviazione. Pertanto non è possibile stimare il momento in cui i dati saranno cancellati o se lo saranno. Ne consegue che al termine del trattamento i dati a cui ci si riferisce con questa informativa non saranno distrutti ma sottoposti ad operazioni di trattamento limitate (conservazione, archiviazione, ricerca e consultazione oltre ad eventuale utilizzo per scopi statistici e per adempimenti legali) in conformità alle norme sulla documentazione amministrativa.

Processi decisionali automatizzati (compresa la profilazione) che determinano effetti giuridici o che incidano sulla persona: Per profilazione si intende l'elaborazione automatizzata dei dati personali eseguita per valutare determinati aspetti personali di una persona fisica (ad esempio analisi: del rendimento professionale, della situazione economica, della salute, delle preferenze personali o degli interessi - art. n. 4 punto n. 4 del GDPR). Un processo automatizzato può sovrapporsi o risultare da una profilazione ma può anche non essere connesso alla profilazione (a puro titolo di esempio: se l'ingresso in locali dove si svolgono determinate attività è consentito unicamente mediante una tessera personale elettronica è un processo decisionale automatizzato che non implica profilazione, se però vengono monitorati orari di accesso e attività svolte in quegli orari per inviare delle promozioni o organizzare delle attività siamo di fronte ad un processo decisionale automatizzato che crea profilazione i cui effetti incidono sulla persona).

Il comune di Pinerolo, per i trattamenti di cui alla presente informativa, non esegue unicamente processi decisionali automatizzati ne esegue profilazione degli interessati ai trattamenti.

Diritto di reclamo all'autorità di controllo. Il soggetto interessato dal trattamento di cui alla presente informativa ha diritto di presentare reclamo all'Autorità di controllo nei tempi e modi definiti dall'Autorità stessa (Per l'Italia: Garante per la protezione dei dati personali www.garanteprivacy.it);

Diritti degli interessati. Gli interessati potranno, in qualunque momento, esercitare i diritti di accesso ai dati personali, di rettifica, di cancellazione, di limitazione, di opposizione del trattamento che li riguarda, di portabilità di cui agli artt.li dal n. 15 al n. 20 del Regolamento Europeo 679/2016 attraverso l'invio di una richiesta all'Amministrazione Comunale anche tramite email ad uno degli indirizzi indicati in precedenza.

Come in precedenza precisato l'esercizio di uno o più dei sopracitati diritti potrebbe comportare l'impossibilità di individuare ed accertare ed eventualmente perseguire violazioni di dati personali o malfunzionamenti che causino o possano causare un rischio per i diritti e le libertà delle persone fisiche. L'esercizio di questi diritti potrebbe inoltre comportare l'impossibilità da parte di questo Ente di adottare le misure necessarie al contenimento di una violazione in corso o ad evitare che si verifichino future violazioni.

Modifiche alla presente informativa: Questo documento è aggiornato al maggio 2018. Il Comune di Pinerolo si riserva il diritto di aggiornare la presente informativa in qualsiasi momento;

Ulteriori dati e notizie: Sul sito web del comune (www.comune.pinerolo.to.it) sono pubblicati e mantenuti aggiornati alcuni documenti che descrivono le attività di trattamento eseguite dall'ente (come il regolamento per il trattamento dei dati sensibili o il registro delle attività di trattamento); questi documenti sono liberamente consultabili e scaricabili.

Allegato 3

MODULO PER LA SEGNALAZIONE INCIDENTI/VIOLAZIONI DI DATI PERSONALI

All'Unità di risposta
Comune di Pinerolo
violazionedati@comune.pinerolo.to.it

Le informazioni di ogni incidente di sicurezza che può comportare la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati dal Comune di Pinerolo devono essere raccolte nel presente modulo e segnalate immediatamente (e comunque non oltre le 8 ore dalla conoscenza) all'indirizzo violazionedati@comune.pinerolo.to.it

È comunque essenziale procedere immediatamente alla comunicazione dell'incidente per una prima valutazione del rischio per i diritti e le libertà degli interessati, anche con informazioni incomplete, che verranno integrate in un momento successivo.

SEZ. A – DATI DEL SOGGETTO CHE EFFETTUA LA SEGNALAZIONE

A.1. SEGNALANTE

Nome e cognome del segnalante: _____

Ufficio o ente di riferimento: _____

Telefono: _____ Email: _____

A.2. SOGGETTO CHE RACCOGLIE LA SEGNALAZIONE ESTERNA

Nome e cognome: _____

Ufficio o ente di riferimento: _____

Telefono: _____ Email: _____

SEZ. B – INFORMAZIONI DI SINTESI SULL'INCIDENTE/VIOLAZIONE

B.1. Informazioni sull'incidente

Data e ora dell'incidente (anche approssimativi se non sono noti): _____

Data e ora in cui il dirigente di settore è venuto a conoscenza dell'incidente: _____

Luogo dell'incidente: _____

Modalità con la quale il dirigente di settore è venuto a conoscenza dell'incidente:

_____

B.2. Breve descrizione dell'incidente:

_____

_____

B.3. Ambito del trattamento dei dati coinvolti:

_____

_____

B.4. Tipo di incidente:

□ Lettura (è stato effettuato un accesso ai dati ma i dati non sono stati copiati)
□ Copia (dati sono ancora presenti sui sistemi dell'Università ma copiati dall'autore della violazione)
□ Alterazione (dati sono presenti sui sistemi del titolare ma sono stati alterati)
□ Cancellazione (dati non sono più sui sistemi del titolare ma non sono in possesso dell'autore della violazione)
□ Furto (dati non sono più sui sistemi del titolare ma sono presumibilmente in possesso dell'autore della violazione)
□ Indisponibilità (dati presenti sui sistemi del titolare ma non disponibili per un certo periodo di tempo)
□ Altro: _____

B.5. Causa dell'incidente:

□ Azione intenzionale interna
□ Azione accidentale interna
□ Azione intenzionale esterna
□ Azione accidentale esterna
□ Sconosciuta
□ Altro: _____

B.6. Categorie di dati personali oggetto dell'incidente:

□ Dati anagrafici/codice fiscale
□ Dati di contatto (es: indirizzo email, numero di telefono)

□ Dati di accesso e di identificazione (es. username, password, altro)
□ Dati economico finanziari (es. pagamenti, numero carta di credito, numero di conto corrente)
□ Dati relativi alla fornitura di servizi di comunicazione elettronica (es. log relativi al traffico Internet)
□ Dati giudiziari
□ Dati di profilazione
□ Dati relativi a documenti di identificazione (es. carta d'identità, passaporto, patente, CNS)
□ Dati di localizzazione
□ Dati personali idonei a rivelare l'origine razziale ed etnica
□ Dati personali idonei a rivelare le opinioni politiche
□ Dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere
□ Dati personali idonei a rivelare l'adesione a partiti, sindacati
□ Dati relativi alla vita sessuale e all'orientamento sessuale
□ Dati relativi alla salute
□ Dati genetici
□ Dati biometrici
□ Altro: _____

B.7. Volume (anche approssimativo) dei dati personali coinvolti nell'incidente:
□ Indicare il volume di dati personali coinvolti: _____
□ Indicare una stima dei dati personali coinvolti: _____
□ Il volume dei dati personali non è noto

B.8. Categorie di interessati coinvolti:
□ Cittadini
□ Personale tecnico e amministrativo
□ Studenti
□ Pazienti
□ Minori
□ Soggetti con disabilità
□ Vulnerabili (es: vittime di violenza o abusi, rifugiati, richiedenti asilo)
□ Altri Utenti: _____

B.9. Numero (anche approssimativo) di interessati coinvolti nell'incidente:
□ Indicare il numero di interessati coinvolti: _____
□ Indicare una stima del numero di interessati coinvolti: _____
□ Il numero non è noto

B.10. L'incidente coinvolge interessati di altri paesi:
□ UE (indicare quali): _____
□ EXTRA UE (indicare quali): _____
□ NO

SEZ. C – INFORMAZIONI DI DETTAGLIO SULL'INCIDENTE/VIOLAZIONE

C.1 Descrizione dettagliata dell'incidente di sicurezza:

_____
_____
_____

C.2 Descrizione delle categorie di dati personali oggetto dell'incidente:

_____
_____
_____

C.3 Dispositivi oggetto dell'incidente:

□ Archivio fisico (documento cartaceo)
□ Computer/Laptop
□ Server
□ Storage
□ Rete
□ Dispositivo mobile (smartphone, tablet, …)
□ File o parte di un file
□ Strumento di backup
□ Altro: _____

C.4 Ubicazione dei dispositivi oggetto dell'incidente:

_____
_____

C.5 Descrizione delle misure di sicurezza tecniche ed organizzative, in essere al momento dell'incidente, adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolte:

_____
_____
_____

SEZ. D - POSSIBILI CONSEGUENZE E GRAVITÀ DELL'INCIDENTE/VIOLAZIONE

D.1 Potenziali conseguenze dell'incidente sugli interessati:

In caso di perdita di riservatezza:

□ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa o dalla disciplina di riferimento

□ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati

□ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito

□ Altro: _____

In caso di perdita di integrità:

□ I dati sono stati modificati e resi inconsistenti

□ I dati sono stati modificati mantenendo la consistenza

□ Altro: _____

In caso di perdita di disponibilità:

□ Mancato accesso a servizi

□ Malfunzionamento e difficoltà nell'utilizzo di servizi

□ Altro: _____

D.2 Ulteriori considerazioni sulle possibili conseguenze:

_____

_____

_____

D.3 Descrizione dell'impatto della violazione sui diritti e le libertà degli interessati coinvolti:

□ Perdita del controllo dei dati personali

□ Limitazione dei diritti

□ Discriminazione

□ Furto o usurpazione d'identità

□ Frodi

□ Perdite finanziarie

□ Decifratura non autorizzata della pseudonimizzazione

□ Pregiudizio alla reputazione

□ Perdita di riservatezza dei dati personali protetti da segreto professionale

□ Conoscenza da parte di terzi non autorizzati

□ Qualsiasi altro danno economico o sociale significativo: _____

_____

_____

SEZ. E – MISURE ADOTTATE A SEGUITO DELL'INCIDENTE/VIOLAZIONE

E.1 Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati:

_____
_____
_____

E.2 Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future:

_____
_____
_____

SEZ. F - ULTERIORI INFORMAZIONI RELATIVE ALL'INCIDENTE/VIOLAZIONE

F.1 L'incidente è stato notificato ad altre autorità di controllo:

□ SI (indicare quali): _____
□ NO

F.2 L'incidente è stato segnalato all'autorità giudiziaria o di polizia:

□ SI
□ NO

F.3 Altre informazioni utili alla valutazione e gestione dell'incidente/violazione:

_____
_____
_____

Data _____ Ora _____

Firma

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

V.2021-04

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

Questo servizio *online* per la notifica di una violazione dei dati personali deve essere utilizzato esclusivamente da soggetti (pubbliche amministrazioni, imprese, associazioni, partiti, professionisti, ecc.) che trattano dati personali in qualità di titolari del trattamento.

Per rivolgersi al Garante in qualità di interessato, per lamentare una violazione della disciplina in materia di protezione dei dati personali, occorre inviare una segnalazione (art. 144 del Codice in materia di protezione dei dati personali) che il Garante può valutare anche ai fini dell'emanazione di provvedimenti correttivi, oppure proporre un reclamo (art. 77 del Regolamento (UE) 2016/679 e artt. da 140-*bis* a 143 del Codice in materia di protezione dei dati personali).

Maggiori informazioni sono disponibili sul sito istituzionale del Garante (https://www.gpdp.it/web/guest/home/diritti/come-agire-per-tutelare-i-tuoi-dati-personali).

Facsimile a titolo dimostrativo non utilizzabile per l'invio della notifica al Garante.

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

A) Dati del soggetto che effettua la notifica

Il soggetto che effettua la notifica è la persona fisica che, per conto titolare del trattamento, tramite questa procedura *online* notifica una violazione dei dati personali al Garante, assumendosi la responsabilità circa la veridicità delle informazioni fornite. Pertanto, la notifica dovrà essere effettuata dal rappresentante legale del titolare del trattamento o da un altro soggetto che agisce su sua delega.

Il sottoscritto Cognome[1*] …….. Nome[1*] …….
E-mail[2*] ……
nella sua qualità[3] di

0 rappresentante legale

0 delegato del rappresentante legale

Cognome[4*] …….. Nome[4*] …….

notifica la seguente violazione di dati personali e ☐ dichiara di aver preso visione dell'informativa sul trattamento dei dati personali e di essere consapevole che chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice in materia di protezione dei dati personali (*Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*) o dell'art. 44 del d.lgs. 51/2018 (*Falsità in atti e dichiarazioni al Garante*), salvo che il fatto non costituisca più grave reato.

———————————

[1] Indicare il **Cognome** e il **Nome** del soggetto che effettua la notifica (e che successivamente dovrà apporre la sua firma digitale, conformemente alle istruzioni che riceverà via e-mail).

[2] Indicare un indirizzo **E-mail** valido per la ricezione delle istruzioni per il completamento della procedura di notifica. Nel caso venga indicata una casella PEC, verificare che la stessa sia abilitata alla ricezione di messaggi di posta elettronica ordinaria. Si consiglia, inoltre, di verificare che il messaggio non sia stato spostato automaticamente o per errore nella cartella "spam" o "posta indesiderata.

[3] Indicare se il soggetto che effettua la notifica è il "rappresentante legale" del Titolare del trattamento dati – di cui alla successiva Sez. C - oppure se agisce in **qualità** di "delegato del rappresentante legale.

[4] Qualora la notifica venga effettuata su delega del rappresentante legale è necessario indicare il Cognome ed il Nome del soggetto delegante (il rappresentante legale).

B) Tipo di notifica

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore (**Prima notifica**). Qualora e nella misura in cui il titolare del trattamento non disponga di tutte le informazioni, può fornirle in fasi successive (**Notifica integrativa**) senza ulteriore ingiustificato ritardo (cfr. art. 33, par. 4, del Regolamento).

0 ***Prima notifica***

0 a) Completa

0 b) Preliminare[1]

La notifica viene effettuata

0 ai sensi dell'art. 33 del RGPD

0 ai sensi dell'art. 26 d.lgs. 51/2018

0 ***Notifica integrativa***[2]

0 c) fascicolo n. [3*] ..... PIN [3*] .....

———————————

[1] Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione impegnandosi ad effettuare una successiva notifica integrativa per completare il processo di notifica.

[2] Il titolare del trattamento, avvalendosi delle previsioni di cui all'art. 33 par. 4 del Regolamento, integra una precedente notifica.

[3] È necessario inserire il numero del fascicolo ed il relativo PIN. Il numero di **fascicolo** unitamente al PIN sono indicati nella e-mail, indirizzata al soggetto che ha effettuato la prima notifica, con la quale è stata comunicata la corretta conclusione della procedura.

B1) Motivo dell'integrazione

Se procedi con la notifica integrativa per i motivi a) o b) troverai le informazioni che hai già fornito con l'ultima notifica e che potrai modificare. Il suo contenuto, previa integrazione o modifica, annulla e sostituisce la precedente.

Se la notifica che intendi integrare è stata trasmessa con le precedenti modalità non troverai le informazioni che hai già fornito, e non sarà possibile compilare la sez. C e i punti 2 e 3 della sez. F. La notifica integrativa, ed il suo contenuto, integrerà e sostituirà la precedente notifica.

1. Si procede all'integrazione per:

- 0 a) Fornire ulteriori informazioni senza completare il processo di notifica
- 0 b) Fornire ulteriori informazioni e completare il processo di notifica
- 0 c) Completare il processo di notifica senza fornire ulteriori informazioni
- 0 d) Annullare una precedente notifica per le seguenti motivazioni:

C) Titolare del trattamento

1. *Il titolare del trattamento è:*

Indicare l'eventuale registro all'interno del quale è censito il Titolare/Responsabile del trattamento che effettua la comunicazione. A tal fine si rappresenta che (cfr. DL 19 ottobre 2012, n. 179) tutte le imprese costituite in forma societaria e tutte le imprese individuali iscritte al registro delle imprese o all'albo delle imprese artigiane, nonché tutti i professionisti iscritti ad Ordini o Collegi professionali sono censiti all'interno dell'Indice nazionale dei domicili digitali delle imprese e dei professionisti (INIPEC). Inoltre, tutte le pubbliche amministrazioni (es. scuole, comuni, ecc.) sono iscritte nell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA).

0 Censito nell'Indice nazionale dei domicili digitali delle imprese e dei professionisti
(INI-PEC www.inipec.gov.it - art. 6-bis Codice Amministrazione Digitale - D.Lgs n. 82/2005)

0 Censito nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi - *(Tipologie Enti: Pubbliche Amministrazioni)*
(*IPA www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs n. 82/2005*)

0 Non censito in nessuno dei due precedenti indici

2. *Dati del titolare del trattamento*

Indicare le informazioni relative al Titolare del trattamento (nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).

Denominazione* .....
Codice Fiscale [1]* ..... Soggetto privo di C.F./P.IVA italiana ☐
Stato* .....
Provincia* ..... Comune* ..... CAP* .....
Indirizzo* .....
Telefono* .....
E-mail[2]* .....
PEC[2]* .....

———————————

[1] In relazione all'indicazione del Codice Fiscale si rappresenta che:

- I soggetti censiti nell'indice IPA appartenenti alla categoria "Pubbliche Amministrazioni" **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora ne siano in possesso);
- Le imprese censite nell'indice INI-PEC **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora non coincidente con il Codice Fiscale);
- I professionisti censiti nell'indice INI-PEC **devono** indicare il numero di Partita IVA utilizzato per lo svolgimento dell'attività professionale;
- Solo i soggetti stranieri o le organizzazioni prive di Codice Fiscale e P.IVA devono selezionare la casella "Soggetto Privo di CF/P.IVA".

[2] Per i soggetti che risultano essere censiti in uno degli indici INI-PEC o IPA è **obbligatorio** fornire l'indirizzo PEC, mentre il conferimento dell'indirizzo e-mail è facoltativo. Per i soggetti che non risultano essere censiti in uno dei due citati indici, o che operano in un altro Stato, è obbligatorio fornire un valido indirizzo e-mail, mentre il conferimento della PEC è facoltativo.

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

C1) Rappresentante del titolare del trattamento non stabilito nello Spazio Economico Europeo

Il titolare del trattamento non stabilito nello Spazio Economico Europeo, qualora offra beni o servizi a interessati nello Spazio Economico Europeo, oppure effettui il monitoraggio del loro comportamento (cfr. art. 3, par. 2, del Regolamento), è tenuto, ai sensi dell'art. 27 del Regolamento, a designare per iscritto un rappresentante in uno dei Paesi dello Spazio Economico Europeo in cui si trovano i predetti interessati, fatti salvi i casi in cui il trattamento è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati o dati relativi a condanne penali e reati, ed è improbabile che presenti un rischio per i diritti e le libertà degli interessati, oppure il trattamento è effettuato da autorità o organismi pubblici.

1. Rappresentante del titolare del trattamento

0 a) Compila la sezione

0 b) Procedi con la notifica senza compilare questa sezione

2. Dati del rappresentante del titolare del trattamento

Denominazione[1*] .....

Codice Fiscale/P.IVA* ..... Soggetto privo di C.F./P.IVA italiana ☐

Stato* .....

Provincia* ..... Comune* ..... CAP* .....

Indirizzo* .....

Telefono* .....

E-mail[2*] .....

PEC[2*] .....

———————————

[1] Indicare le informazioni relative al Rappresentante del titolare del trattamento (nel caso di impresa indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).

[2] È obbligatorio fornire almeno un recapito tra E-mail e PEC.

D) Dati di contatto per informazioni relative alla violazione

Il titolare del trattamento deve comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni (cfr. art. 33, par. 3, lett. b), del Regolamento).

o ***1) Responsabile della protezione dei dati***

- o i cui dati di contatto sono stati già comunicati con la comunicazione protocollo[1*] n.……..
- o i cui dati di contatto sono stati già comunicati al Garante, ma al momento non si dispone[2] del numero di protocollo della relativa comunicazione

Cognome* …… Nome* ……..
E-mail* ……..
Recapito telefonico per eventuali comunicazioni* ……

o ***2) Altro soggetto***

Cognome* …… Nome* ……..
E-mail* ……..
Recapito telefonico per eventuali comunicazioni* ……
Funzione rivestita* ……

———————————

[1] Indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD.

[2] Selezionare questa opzione se al momento della compilazione non è possibile reperire il numero di protocollo assegnato alla comunicazione dei dati di contatto che sarà comunicato con una successiva notifica integrativa.

E) Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare, responsabile[1])

Denominazione[2*] ……

Codice Fiscale[3*] ……Soggetto privo di C.F./P.IVA ☐

Ruolo O Contitolare O Responsabile

Denominazione[2*] ……

Codice Fiscale[3*] ……Soggetto privo di C.F./P.IVA ☐

Ruolo O Contitolare O Responsabile

Denominazione[2*] ……

Codice Fiscale[3*] ……Soggetto privo di C.F./P.IVA ☐

Ruolo O Contitolare O Responsabile

———————————

[1] In tale tipologia rientra anche l'altro responsabile (c.d. sub-responsabile) di cui all'art. 28, par. 2, del RGPD o all'art. 18, comma 2, del d.lgs. 51/2018.

[2] Nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale.

[3] In relazione all'indicazione del Codice Fiscale si rappresenta che:

- I soggetti censiti nell'indice IPA appartenenti alla categoria "Pubbliche Amministrazioni" **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora ne siano in possesso);
- Le imprese censite nell'indice INI-PEC **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora non coincidente con il Codice Fiscale);
- I professionisti censiti nell'indice INI-PEC **devono** indicare il numero di Partita IVA utilizzato per lo svolgimento dell'attività professionale;

  Solo i soggetti stranieri o le organizzazioni prive di Codice Fiscale e P.IVA devono selezionare la casella "Soggetto Privo di CF/P.IVA".

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

F) Informazioni sulla violazione

1. *Momento in cui è avvenuta la violazione*

- o a) Il ___ /___ /_____
- o b) Dal ___/___ /_____ (la violazione è ancora in corso)
- o c) Dal ___/___ /_____ al ___ /___ /_____
- o d) In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. *Modalità con la quale il titolare è venuto a conoscenza della violazione*

- o a) Rilevazione da parte del titolare[1]
- o b) Comunicazione da parte del responsabile del trattamento
- o c) Segnalazione da parte di un interessato
- o d) Segnalazione da parte di un soggetto esterno
- o e) Notizie stampa
- o f) Altro

3. *Momento in cui il titolare è venuto a conoscenza della violazione*

Data …… **Ora** ……..

4. *Motivi del ritardo (in caso di notifica oltre le 72 ore)*

5. *Natura della violazione*

[ ] a) Perdita di riservatezza[2]
[ ] b) Perdita di integrità[3]
[ ] c) Perdita di disponibilità[4]

6. *Causa della violazione*

[ ] a) Azione intenzionale interna
[ ] b) Azione accidentale interna
[ ] c) Azione intenzionale esterna
[ ] d) Azione accidentale esterna
[ ] e) Sconosciuta

[ ] **f)** Non ancora determinata

7. *Descrizione della violazione*[5]

8. *Descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione*

9. *Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti*

10. Categorie di interessati coinvolti nella violazione

[ ] a) Dipendenti/Consulenti
[ ] b) Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
[ ] c) Associati, soci, aderenti, simpatizzanti, sostenitori
[ ] d) Soggetti che ricoprono cariche sociali
[ ] e) Beneficiari o assistiti
[ ] f) Pazienti
[ ] g) Minori
[ ] h) Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
[ ] i) Altro

[ ] l) Categorie ancora non determinate

11. Numero (anche approssimativo) di interessati coinvolti nella violazione

o a) N. …….. interessati
o b) Circa n. …….. interessati
o c) Non determinabile
o d) Non ancora determinato

12. Categorie di dati personali oggetto di violazione

[ ] a) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
[ ] b) Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
[ ] c) Dati di accesso e di identificazione (username, password, customer ID, altro…)
[ ] d) Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
[ ] e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
[ ] f) Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
[ ] g) Dati di profilazione
[ ] h) Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
[ ] i) Dati relativi all'ubicazione
[ ] l) Dati che rivelano l'origine razziale o etnica
[ ] m) Dati che rivelano le opinioni politiche
[ ] n) Dati che rivelano le convinzioni religiose o filosofiche
[ ] o) Dati che rivelano l'appartenenza sindacale
[ ] p) Dati relativi alla vita sessuale o all'orientamento sessuale
[ ] q) Dati relativi alla salute
[ ] r) Dati genetici

[ ] s) Dati biometrici
[ ] t) Altro

[ ] u) Categorie ancora non determinate

13. *Numero (anche approssimativo) di registrazioni[6] dei dati personali oggetto di violazione*

o a) N. ……..
o b) Circa n. ……..
o c) Non determinabile
o d) Non ancora determinato

14. *Descrizione di dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati*

15. *Allegati*

[ ] Intendo allegare un documento contenente ulteriori informazioni

———————————

1. Es. verifiche interne, monitoraggi, ecc
2. Diffusione/ accesso non autorizzato o accidentale
3. Modifica non autorizzata o accidentale
4. Impossibilità di accesso o distruzione non autorizzata o accidentale
5. Indicare le circostanze in cui si è verificata la violazione e le cause, tecniche o organizzative, che l'hanno determinata
6. Ad esempio numero di fatture, ordini, referti, immagini, record di un database o numero di transazioni.

G) Probabili conseguenze della violazione

1. Probabili conseguenze della violazione per gli interessati

1.1. In caso di perdita di riservatezza:

[ ] a) I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
[ ] b) I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
[ ] c) I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
[ ] d) Altro

[ ] e) In corso di valutazione[4]

1.2. In caso di perdita di integrità:

[ ] a) I dati sono stati modificati e resi inconsistenti
[ ] b) I dati sono stati modificati mantenendo la consistenza
[ ] c) Altro

[ ] d) In corso di valutazione[4]

1.3. In caso di perdita di disponibilità:

[ ] a) Mancato accesso a servizi
[ ] b) Malfunzionamento e difficoltà nell'utilizzo di servizi
[ ] c) Altro

[ ] d) In corso di valutazione[4]

1.4. Ulteriori considerazioni sulle probabili conseguenze

2. Potenziale impatto per gli interessati

[ ] a) Perdita del controllo dei dati personali
[ ] b) Limitazione dei diritti
[ ] c) Discriminazione
[ ] d) Furto o usurpazione d'identità
[ ] e) Frodi
[ ] f) Perdite finanziarie
[ ] g) Decifratura non autorizzata della pseudonimizzazione
[ ] h) Pregiudizio alla reputazione
[ ] i) Perdita di riservatezza dei dati personali protetti da segreto professionale
[ ] l) Conoscenza da parte di terzi non autorizzati
[ ] m) Qualsiasi altro danno economico o sociale significativo

[ ] n) Non ancora definito

3. Gravità del potenziale impatto per gli interessati

o a) Trascurabile
o b) Bassa
o c) Media
o d) Alta
o e) Non ancora definita

Motivazioni

4. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

H) Misure adottate a seguito della violazione

1. Misure tecniche e organizzative adottate (o di cui si propone l'adozione[1]) per porre rimedio alla violazione e attenuarne i possibili effetti negativi per gli interessati

2. Misure tecniche e organizzative adottate (o di cui si propone l'adozione[1]) per prevenire simili violazioni future

3. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

———————————

1. Nella descrizione distinguere le misure adottate da quelle in corso di adozione

I) Valutazione del rischio per gli interessati

Non sono state fornite alcune delle informazioni (es. categorie e numero di interessati, categorie e numero di registrazioni di dati personali, probabili conseguenze della violazione, ecc.) di cui il titolare del trattamento dovrebbe tenere conto nella valutazione del rischio per i diritti e le libertà degli interessati derivante dalla violazione dei dati personali. Pertanto si invita il titolare del trattamento a prestare particolare attenzione nella compilazione della presente sezione, fornendo le motivazioni che lo hanno portato a ritenere che la violazione dei dati personali sia suscettibile, o meno, di presentare un rischio elevato per gli interessati.

Il Regolamento (spec. cons. nn. 75 e 76) suggerisce che, di norma, nella valutazione del rischio si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità dei rischi per i diritti e le libertà degli interessati e che tali rischi dovrebbero essere determinati in base a una valutazione oggettiva.
Le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018, individuano i seguenti fattori da considerare – a fronte di una violazione dei dati personali – nella valutazione del rischio per i diritti e le libertà degli interessati: il tipo di violazione; la natura, il carattere sensibile e il volume dei dati personali; la facilità di identificazione degli interessati; la gravità delle conseguenze per gli interessati; le caratteristiche particolari dell'interessato; le caratteristiche particolari del titolare del trattamento dei dati; nonché il numero di interessati coinvolti.

1. Il titolare del trattamento ritiene[1] che:

- o a) la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- o b) la violazione non sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- o c) siano necessari ulteriori elementi per effettuare la valutazione del rischio per i diritti e le libertà delle persone fisiche

Motivazioni

2. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

L) Comunicazione della violazione agli interessati

Si evidenzia che, 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 è tenuto, ai sensi dell'art. 34 del Regolamento, a comunicare la violazione agli interessati coinvolti senza ingiustificato ritardo, a meno che sia soddisfatta una delle condizioni previste dal par. 3 del citato articolo.

1. La violazione è stata comunicata direttamente agli interessati?

- o a) Sì, è stata comunicata il ___/___/_____
- o b) No, sarà comunicata entro il ___/___/_____
- o c) No, sono tuttora in corso le dovute valutazioni
- o d) No, perché la violazione non è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- o e) No e non sarà comunicata perché:

[ ] e1) il titolare ha messo in atto 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 (es. cifratura);

Descrivere le misure applicate

[ ] e2) il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

Descrivere le misure adottate

[ ] e3) detta comunicazione richiederebbe sforzi sproporzionati. Il titolare ha proceduto o procederà con una comunicazione pubblica o una misura simile, tramite la quale gli interessati sono o saranno informati con analoga efficacia.

Descrivere la modalità tramite la quale gli interessati sono stati informati

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

2. Numero di interessati a cui è stata comunicata la violazione

N. …….. interessati

3. Canale utilizzato per la comunicazione agli interessati

[ ] a) SMS
[ ] b) Posta cartacea
[ ] c) Posta elettronica
[ ] d) Altro

4. Contenuto della comunicazione agli interessati

5. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

M) Altre informazioni

1. La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[1]?

O Sì O No

Indicare a quale organismo e in virtù di quale norma

2. È stata effettuata la segnalazione all'autorità giudiziaria o di polizia?

O Sì O No

Note

———————————

1. Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

N) Informazioni relative a violazioni transfrontaliere

Un trattamento transfrontaliero (cfr. art. 4, punto 23), del Regolamento) è un trattamento che ha luogo nell'ambito di stabilimenti in più di un Paese dello Spazio Economico Europeo (di cui fanno parte gli Stati membri dell'Unione Europea, nonché l'Islanda, il Liechtenstein e la Norvegia), oppure che ha luogo nell'ambito di un unico stabilimento in un Paese dello Spazio Economico Europeo, ma che può avere impatti significativi sui diritti e sulle libertà di interessati in più di un Paese dello Spazio Economico Europeo.

1. ***La violazione riguarda un trattamento transfrontaliero effettuato da un titolare stabilito all'interno dello Spazio Economico Europeo?***

   - o a) Sì
   - o b) No
   - o c) Sono tuttora in corso le dovute valutazioni

2. ***Indicare l'autorità di controllo capofila[1]***

   - o a) Garante per la protezione dei dati personali
   - o b) Altra autorità di controllo: [Selezionare]
   - o c) Non si dispone di elementi per individuare l'autorità di controllo capofila

3. ***Indicare i Paesi dello Spazio Economico Europeo in cui si trovano stabilimenti del titolare, specificando quelli coinvolti nella violazione, o in cui si trovano gli interessati coinvolti nella violazione***

	Stabilimenti del titolare	Stabilimenti coinvolti nella violazione	Interessati coinvolti nella violazione
Italia	[ ]	[ ]	[ ]
Austria	[ ]	[ ]	[ ]
Belgio	[ ]	[ ]	[ ]
Bulgaria	[ ]	[ ]	[ ]
Cipro	[ ]	[ ]	[ ]
Croazia	[ ]	[ ]	[ ]
Danimarca	[ ]	[ ]	[ ]
Estonia	[ ]	[ ]	[ ]
Finlandia	[ ]	[ ]	[ ]
Francia	[ ]	[ ]	[ ]
Germania	[ ]	[ ]	[ ]
Grecia	[ ]	[ ]	[ ]
Irlanda	[ ]	[ ]	[ ]
Islanda	[ ]	[ ]	[ ]
Lettonia	[ ]	[ ]	[ ]
Liechtenstein	[ ]	[ ]	[ ]
Lituania	[ ]	[ ]	[ ]

Lussemburgo	[ ]	[ ]	[ ]
Malta	[ ]	[ ]	[ ]
Norvegia	[ ]	[ ]	[ ]
Paesi Bassi	[ ]	[ ]	[ ]
Polonia	[ ]	[ ]	[ ]
Portogallo	[ ]	[ ]	[ ]
Rep. Ceca	[ ]	[ ]	[ ]
Romania	[ ]	[ ]	[ ]
Slovacchia	[ ]	[ ]	[ ]
Slovenia	[ ]	[ ]	[ ]
Spagna	[ ]	[ ]	[ ]
Svezia	[ ]	[ ]	[ ]
Ungheria	[ ]	[ ]	[ ]

4. *Indicare le altre autorità di controllo a cui è stata eventualmente notificata la violazione*

[ ] Austria - Data Protection Authority
[ ] Belgio - Data Protection Authority
[ ] Bulgaria - Commission for Personal Data Protection
[ ] Cipro - Office of the Commissioner for Personal Data Protection
[ ] Croazia - Personal Data Protection Agency - AZOP
[ ] Danimarca - Data Protection Agency
[ ] Estonia - Data Protection Inspectorate
[ ] Finlandia - Office of the Data Protection Ombudsman
[ ] Francia - CNIL - National Commission for Informatics and Liberties
[ ] Germania - Federal Commissioner for Data Protection and Freedom of Information (BfDI)
[ ] Germania (Baden-Wurttemberg) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Bavaria - Private Sector) - Bavarian Lander Office for Data Protection Supervision (BayLDA)
[ ] Germania (Bavaria - Public sector) - Lander Commissioner for Data Protection (BayLfD)
[ ] Germania (Berlin) - Berlin Commissioner for Data Protection and Freedom of Information
[ ] Germania (Brandenburg) - Lander Commissioner for Data Protection and the Right for Access to Information
[ ] Germania (Bremen) - Lander Commissioner for Data Protection and Freedom of Information - Free Hanseatic city of Bremen
[ ] Germania (Hamburg) - Hamburg Commissioner for Data Protection and Freedom of Information
[ ] Germania (Hesse) - Hessian Commissioner for Data Protection and Freedom of Information
[ ] Germania (Lower Saxony) - Lander Commissioner for Data Protection (LfD)
[ ] Germania (Mecklenburg-Western Pomerania) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (North Rhine-Westphalia) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Rhineland-Palatinate) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saarland) - Independent Data Protection Center Saarland - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saxony) - Saxon Data Protection Commissioner
[ ] Germania (Saxony-Anhalt) - Lander Commissioner for Data Protection
[ ] Germania (Thuringia) - Thuringian Lander Commissioner for Data Protection and Freedom of Information (TLfDI)
[ ] Grecia - Hellenic Data Protection Authority
[ ] Irlanda - Data Protection Commission (DPC)

[ ] Islanda - Data Protection Authority
[ ] Lettonia - Data State Inspectorate
[ ] Liechtenstein - Data Protection Authority
[ ] Lituania - State Data Protection Inspectorate
[ ] Lituania - The Office of Inspector of Journalist Ethics
[ ] Lussemburgo - National Commission for Data Protection (CNPD)
[ ] Malta - Office of the Information and Data Protection Commissioner
[ ] Norvegia - Norwegian Data Protection Authority
[ ] Paesi Bassi - Authority for Personal Data
[ ] Polonia - Office for the Protection of Personal Data
[ ] Portogallo - National Commission for Data Protection (CNPD)
[ ] Rep. Ceca - Office for Personal Data Protection
[ ] Romania - National Supervisory Authority For Personal Data Processing
[ ] Slovacchia - Office for Personal Data Protection
[ ] Slovenia - Information Commissioner
[ ] Spagna - Spanish Agency for Data Protection
[ ] Svezia - Data Protection Authority
[ ] Ungheria - National Authority for Data Protection and Freedom of Information

[ ] Intendo allegare copia (in lingua inglese) della notifica effettuata

———————————

1. L'autorità di controllo dello stabilimento principale in cui ha luogo il trattamento o dello stabilimento unico del titolare del trattamento

O) Informazioni relative a violazioni che riguardano trattamento effettuato da un titolare stabilito al di fuori dello Spazio Economico Europeo

Il Regolamento si applica anche al trattamento di dati personali di interessati che si trovano nello Spazio Economico Europeo, effettuato da un titolare del trattamento che non è stabilito nello Spazio Economico Europeo, laddove tale trattamento riguardi: a) l'offerta di beni o la fornitura di servizi a interessati nello Spazio Economico Europeo, oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dello Spazio Economico Europeo (cfr. art. 3, par. 2, del Regolamento)

1. ***La violazione riguarda un trattamento, a cui si applica il Regolamento, effettuato da un titolare stabilito al di fuori dello Spazio Economico Europeo?***

   o a) Sì
   o b) No

2. ***Indicare gli altri Paesi dello Spazio Economico Europeo in cui si trovano gli interessati coinvolti nella violazione***

   [ ] Austria
   [ ] Belgio
   [ ] Bulgaria
   [ ] Cipro
   [ ] Croazia
   [ ] Danimarca
   [ ] Estonia
   [ ] Finlandia
   [ ] Francia
   [ ] Germania
   [ ] Grecia
   [ ] Irlanda
   [ ] Islanda
   [ ] Lettonia
   [ ] Liechtenstein
   [ ] Lituania
   [ ] Lussemburgo
   [ ] Malta
   [ ] Norvegia
   [ ] Paesi Bassi
   [ ] Polonia
   [ ] Portogallo
   [ ] Rep. Ceca
   [ ] Romania
   [ ] Slovacchia
   [ ] Slovenia
   [ ] Spagna

[ ] Svezia
[ ] Ungheria

3. *Indicare le altre autorità di controllo a cui è stata eventualmente notificata la violazione*

[ ] Austria - Data Protection Authority
[ ] Belgio - Data Protection Authority
[ ] Bulgaria - Commission for Personal Data Protection
[ ] Cipro - Office of the Commissioner for Personal Data Protection
[ ] Croazia - Personal Data Protection Agency - AZOP
[ ] Danimarca - Data Protection Agency
[ ] Estonia - Data Protection Inspectorate
[ ] Finlandia - Office of the Data Protection Ombudsman
[ ] Francia - CNIL - National Commission for Informatics and Liberties
[ ] Germania - Federal Commissioner for Data Protection and Freedom of Information (BfDI)
[ ] Germania (Baden-Wurttemberg) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Bavaria - Private Sector) - Bavarian Lander Office for Data Protection Supervision (BayLDA)
[ ] Germania (Bavaria - Public sector) - Lander Commissioner for Data Protection (BayLfD)
[ ] Germania (Berlin) - Berlin Commissioner for Data Protection and Freedom of Information
[ ] Germania (Brandenburg) - Lander Commissioner for Data Protection and the Right for Access to Information
[ ] Germania (Bremen) - Lander Commissioner for Data Protection and Freedom of Information - Free Hanseatic city of Bremen
[ ] Germania (Hamburg) - Hamburg Commissioner for Data Protection and Freedom of Information
[ ] Germania (Hesse) - Hessian Commissioner for Data Protection and Freedom of Information
[ ] Germania (Lower Saxony) - Lander Commissioner for Data Protection (LfD)
[ ] Germania (Mecklenburg-Western Pomerania) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (North Rhine-Westphalia) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Rhineland-Palatinate) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saarland) - Independent Data Protection Center Saarland - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saxony) - Saxon Data Protection Commissioner
[ ] Germania (Saxony-Anhalt) - Lander Commissioner for Data Protection
[ ] Germania (Thuringia) - Thuringian Lander Commissioner for Data Protection and Freedom of Information (TLfDI)
[ ] Grecia - Hellenic Data Protection Authority
[ ] Irlanda - Data Protection Commission (DPC)
[ ] Islanda - Data Protection Authority
[ ] Lettonia - Data State Inspectorate
[ ] Liechtenstein - Data Protection Authority
[ ] Lituania - State Data Protection Inspectorate
[ ] Lituania - The Office of Inspector of Journalist Ethics
[ ] Lussemburgo - National Commission for Data Protection (CNPD)
[ ] Malta - Office of the Information and Data Protection Commissioner
[ ] Norvegia - Norwegian Data Protection Authority
[ ] Paesi Bassi - Authority for Personal Data
[ ] Polonia - Office for the Protection of Personal Data
[ ] Portogallo - National Commission for Data Protection (CNPD)
[ ] Rep. Ceca - Office for Personal Data Protection
[ ] Romania - National Supervisory Authority For Personal Data Processing
[ ] Slovacchia - Office for Personal Data Protection
[ ] Slovenia - Information Commissioner

[ ] Spagna - Spanish Agency for Data Protection
[ ] Svezia - Data Protection Authority
[ ] Ungheria - National Authority for Data Protection and Freedom of Information

[ ] Intendo allegare copia (in lingua inglese) della notifica effettuata

CITTÀ di PINEROLO

SETTORE ORGANIZZAZIONE
PROGRAMMAZIONE E CONTROLLO
Servizio Ricerca finanziamenti
Tel. 0121 361309
annamaria.lorenzino@comune.pinerolo.to.it

Alla Segreteria Generale

Servizio Affari Generali

Oggetto: Parere contrario alla proposta di deliberazione n. 52/2024

Esprimo parere sfavorevole sulla proposta di deliberazione della Giunta comunale n. 52/2024, per la richiesta apposizione dei pareri di regolarità tecnica da parte di tutti i Dirigenti per le seguenti ragioni:

1) la proposta è l'aggiornamento di una procedura operativa sui "Data breach" già approvata dalla Giunta nel 2018 con la deliberazione n. 218, sulla quale l'allora Dirigente assegnatario del servizio "CED" non aveva ritenuto necessario socializzare il rischio dell'istruttoria apponendo lui solo il parere di regolarità tecnica;

2) il Regolamento sul sistema dei controlli interni, approvato dal Consiglio comunale n. 6 del 05/03/2013 prevede all'art. 5 che il controllo preventivo di regolarità amministrativa (oggi confluito nel solo parere di regolarità tecnica) sia esercitato dal **Dirigente competente per materia**. La disposizione è confermata dalle disposizioni regolamentari dell'art. 58, comma 2 lett. b) e dell'art. 63 comma 3 del Regolamento di contabilità del Comune nelle quali si prevede che il parere di regolarità tecnica sia apposto dal **Responsabile del servizio interessato**. Nel caso in specie il servizio interessato è il CED, assegnato alla dott.ssa Gambino dal 27/03/2023;

3) il parere è una dichiarazione di giudizio relativa alla fase preparatoria del provvedimento con la quale si attesta la completezza e la regolarità dell'istruttoria. L'apposizione del parere di regolarità tecnica di tutti i Dirigenti comporterebbe la rinnovazione e sovrapposizione completa dell'istruttoria da parte di ciascuno di essi. Il regolamento di contabilità nei casi in cui prevede il parere plurimo dei Dirigenti, introduce limiti circoscrivendone perimetro e contenuto. L'art. 16, comma 7 del regolamento, per la deliberazione di approvazione del PEG, precisa che: "*Il parere di regolarità tecnica del Segretario Generale e dei Responsabili dei Servizi certifica:*
a) la fattibilità degli obiettivi contenuti nel PEG in relazione alle risorse assegnate. Tale parere deve essere espresso ***da ogni Responsabile del servizio e fa diretto riferimento agli obiettivi che sono loro assegnati****;*
b) la coerenza degli obiettivi del PEG con gli obiettivi strategici ed operativi definiti nel Documento Unico di Programmazione (DUP), ai fini delle verifiche di cui all'art. 170, c. 7 del D.Lgs. 267/2000 e s.m.i..
La rinnovazione completa dell'istruttoria da parte di ciascun Dirigente, è ritenuto da parte di scrive, un dannoso e inutile dispendio di tempo, di energie e di lavoro;

4) la valenza strategica delle "disposizioni operative in materia di incidenti di sicurezza e di violazione dei dati personali" è indubbia e interessa e coinvolge, sia pure con intensità diversa, i singoli Dirigenti. Tuttavia, chi scrive, ritiene che, anziché chiedere a tutti l'apposizione del parere di regolarità tecnica, senza confondere le fasi dell'istruttoria e dell'esecuzione della deliberazione, sarebbe stato opportuno informare i Dirigenti prima del caricamento della proposta di deliberazione nell'applicativo e, al fine di dare attuazione alle disposizioni operative da introdurre, organizzare una breve spiegazione in occasione di una Consulta dei Dirigenti;

5) temo inoltre che il coinvolgimento dei Dirigenti nella fase istruttoria di questa deliberazione comporti l'avvio della prassi inutile e dispendiosa di chiamare in causa più Dirigenti, a prescindere dalla "**competenza per materia**", ogni qualvolta la proposta incida su servizi di diversi settori; situazione che si verifica con elevata frequenza.

Il parere che esprimo è per le anzidette ragioni sfavorevole **ai sensi dell'art. 1, comma 2 della L. 241/1990 in base al divieto di aggravamento del procedimento.**

Il Segretario Generale
Dr.ssa Annamaria Lorenzino

Documento informatico firmato digitalmente ai sensi del T.U. 445/200 e del D. Lgs. 82/2005 e rispettive norme collegate, il quale sostituisce il documento cartaceo e la firma autografa. Trasmissione eseguita in ottemperanza dell'art. 47 del D.Lgs 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) come modificato dalla Legge 17/12/2012 n. 221 recante "Ulteriori misure per la crescita" (G.U. n. 249 del 18/12/2012).