CITTA' DI COLLEGNO

Direzione ed Organizzazione

Policy per la gestione del Data Breach

REGOLAMENTO UE N. 679/2016 (GDPR)

Art. 1 - SCOPO DEL DOCUMENTO

Il presente documento ha lo scopo di descrivere le modalità operative da seguire per la rilevazione di eventuali violazioni di dati personali (c.d. "*data breach*"), la loro segnalazione, la valutazione e l'eventuale notifica all'Autorità Garante per la protezione dei dati personali e agli Interessati nel rispetto di quanto previsto dagli artt. 33 e 34 del Regolamento (UE) n. 2016/679 sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati (*GDPR*).

ART. 2 - CONTESTO NORMATIVO DI RIFERIMENTO E PRINCIPI APPLICABILI

Il presente documento è redatto in applicazione dei citati artt.33 e 34 del GDPR, tenuto conto dei provvedimenti e delle decisioni dell'Autorità per la protezione dei dati personali (Garante Privacy) e delle Linee Guida in materia emanate dal WP250, ossia dal gruppo di lavoro europeo per la protezione dei dati personali (ultimo aggiornamento 06 ottobre 2018).
Il presente documento contiene anche le indicazioni fornite dall'Agenzia Europea per la Sicurezza delle Reti e dell'Informazione (ENISA) per la valutazione della gravità delle violazioni dei dati personali.

ART. 3 - DEFINIZIONI

Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile (*interessato*); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, punto 1 GDPR).
Dati particolari: dati personali che rivelino l'origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale e il trattamento di dati genetici, dati biometrici, dati riguardanti la salute o dati riguardanti la vita sessuale o l'orientamento sessuale di una persona fisica (art. 9, co.1 GDPR).
Interessato: la persona fisica cui si riferiscono i dati personali.
Trattamento:qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, punto 2 GDPR).
Violazione dei dati personali (*Data Breach*): 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 GDPR).
Titolaredel trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di Dati Personali (art. 4, punto 7 GDPR). Nel prosieguo inteso come "Il Comune di Collegno.
Sistema Informativo Comunale (SIC): il settore del Comune di Collegno incaricato della gestione dei sistemi informativi.
Responsabiledel trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento (art. 4, punto 8 GDPR).
Data Protection Officer(DPO): la persona nominata come responsabile della protezione dei dati del Comune di Collegno ai sensidell'art. 37del GDPR.
Referente Privacy: la figura individuata all'interno del Comune di Collegno con il ruolo di coordinatore in materia di trattamento dei dati personali, individuato all'interno del Comune di Collegno nella persona del Segretario generale.

Ufficio Programmazione e Trasparenza:l'Ufficio del Comune di Collegno a supporto dell'attività del Referente Privacy.

Art. 4 - PROCEDURA OPERATIVA

4.1 Gli elementi chiave per la gestione di un Data Breach

4.1.1 Rilevazione dell'incidente di sicurezza

Qualsiasi dipendente o collaboratore che viene a conoscenza di un incidente di sicurezza o una potenziale violazione di dati personali o riceva una segnalazione a tale riguardo deve informare immediatamente tramite e-mail il proprio responsabile gerarchico del settore procedente, il Referente Privacy e il SIC.

4.1.2 Valutazione di un Data Breach

Il Comune di Collegno, in qualità di Titolare del trattamento, è tenuto ad adottare tutte le misure necessarie per garantire la protezione dei dati personali, così evitando violazioni di sicurezza che comportino 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.
Le violazioni dei dati personali possono riguardare:

- la riservatezza (in caso di divulgazione o accesso non autorizzati ai dati);
- l'integrità (in caso di alterazione non autorizzata o accidentale dei dati);
- la disponibilità (in caso di perdita accidentale o non autorizzata di accesso o distruzione dei dati).

Il Garante Privacy fornisce alcuni esempi:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Il Referente Privacy, con il supporto dell'Ufficio Programmazione e Trasparenza, il Responsabile SIC, il Dirigente del settore procedente che ha identificato l'anomalia, con il coinvolgimento del DPO, analizzano l'accaduto al fine di valutare se la violazione di dati personali si sia effettivamente verificata, considerando:

- natura della potenziale violazione di dati personali;
- categorie e numero approssimativo di soggetti interessati;
- categorie e numero approssimativo di dati personali interessati;
- tipo ed entità dei rischi per gli Interessati;
- probabili conseguenze della violazione dei dati personali, compresi potenziali danni economici e reputazionali;
- processi aziendali e sistemi informatici interessati;
- misure tecniche / organizzative non presenti o aggirate.

Se sono coinvolti processi o sistemi in outsourcing, Il Dirigente del Settore che ha il contatto con il fornitore supportato dal SIC richiede che il fornitore stesso esamini la potenziale violazione di dati e condivida azioni contingenti e tempestive.
Se all'esito dell'analisi emerge la conferma che si tratta di una violazione di dati personali, il Comune di Collegno, in qualità di Titolare del trattamento, è tenuto ad adottare tutte le misure necessarie per porre rimedio agli effetti di tale violazione, così evitando violazioni di sicurezza che comportino 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.

4.1.3 Valutazione dei rischi per i diritti e le libertà degli interessati

Per comprendere la severità o meno di una violazione dei dati personali è necessario valutare le conseguenze che derivano da essa.
La valutazione deve essere obiettiva e calcolata sulla base dell'impatto della violazione dei dati personali sugli interessati.
La valutazione deve includere un'adeguata considerazione delle circostanze specifiche della violazione, inclusa la gravità dell'impatto potenziale e la probabilità che ciò si verifichi.
Per valutare il livello di rischio associato a una violazione dei dati personali, possono essere seguite diverse metodologie riconducibili a diversi standard internazionali.
Di seguito si riporta la metodologia, proposta dall'Agenzia Europea per la Sicurezza delle Reti e dell'Informazione, i cui criteri da applicare seguono la formula:

$$SE = DPC \times EI + CB$$

SE (*Severity*)= costituisce l'impatto che può avere il Data Breach
DPC (*Data Processing Context*)= serve a valutare la criticità dei dati personali all'interno di un contesto di trattamento.
EI (*Ease of Identification*) = rappresenta la facilità di identificazione dell'interessato e può costituire parametro di correzione del DPC.
CB (*Circumstances of the Breach*) = considera le circostanze in cui si è verificato il Data Breach

DPC - Contesto del trattamento

I dati personali devono essere classificati in categorie:

- dati comuni (es. dati anagrafici, dettagli di contatto, esperienze professionali);
- dati comportamentali (es. dati sul traffico internet, informazioni su preferenze e abitudini);
- dati finanziari (degli utenti, dei consiglieri, ecc.);
- dati particolari (es. informazioni che rivelano l'origine razziale o etnica, opinioni politiche, credenze religiose, dati relativi alla salute).

Contesto del trattamento	Punteggio
Dato comune	1
Dato di comportamento	2
Dato finanziario	3
Dati particolari	4

Il punteggio indicato in tabella ed associato in via preliminare alla categoria di dato, può essere aumentato o diminuito in considerazione di altre circostanze, quali:
- il volume dei dati (ad.es grandi volume di dati comuni vedranno, pertanto, incrementato il punteggio);
- la caratteristiche dei soggetti (se si tratta di minori il punteggio andrà incrementato);
- la pubblicità del dato (se il dato è già pubblico, il punteggio andrà diminuito);
- inaccuratezza o inutilizzabilità dei dati (il punteggio potrà essere diminuito).

EI - Facilità di identificazione

La facilità di identificazione dell'interessato (EI)è un fattore di correzione del DPC. In generale, minore è la facilità di identificazione, minore è il punteggio complessivo (SE).

Facilità di identificazione	Punteggio

Trascurabile: i dati personali non rivelano altre informazioni relative a un individuo e l'identificazione dello stesso è molto improbabile	0.25
Limitato: i dati personali includono informazioni aggiuntive che potrebbero portare all'identificazione dell'individuo	0.5
Significativo: i dati personali includono ulteriori informazioni di identificazione sull'individuo ed è collegato ad altri dati.	0.75
Massimo:i dati personali includono informazioni che identificano facilmente l'individuo	1

CB - Circostanze del Data Breach

Le circostanze del Data Breach (CB) rappresentano un fattore aggravante e considerano situazioni di intento malevolo o di scarsa conoscenza degli effetti della violazione in termini di perdita di riservatezza, integrità, disponibilità.

Circostanze del Data Breach	Punteggio
Perdita di confidenzialità	0 (nessuna conoscenza riguardo al trattamento illegale)
	0,25 (danno di confidenzialità verso un numero conosciuto di interessati)
	0,5 (danno di confidenzialità verso un numero non conosciuto di interessati)
Perdita di integrità	0 (dato alterato ma senza identificazione dell'interessato o uso illecito)
	0,25 (dato alterato con possibile utilizzo illegale o scorretto, ma con possibilità di ripristino della situazione ordinaria)
	0,5 (dato alterato con possibile utilizzo illegale o scorretto, senza possibilità di ripristino della situazione ordinaria)
Perdita di disponibilità	0 (dato può essere ripristinato senza difficoltà)
	0,25 (temporanea indisponibilità)
	0.5 (definitive indisponibilità)
Intento malevolo	0,5 (il Data Breach ha creato danni al Comune e/o ai soggetti interessati)

Risultato

Il risultato derivante dal calcolo del valore dell'impatto del Data Breach (SE) può essere classificato su una scala di 4 livelli come esposto nella seguente tabella:

Severità di un data breach		
SE < 2	**Basso**	gli individui possono sperimentare piccoli inconvenienti superabili senza alcun problema (ad esempio: tempo occorrente per inserire nuovamente le informazioni, fastidio, irritazione ecc.)

Severità di un data breach		
2 ≤ SE < 3	**Medio**	gli individui possono incontrare inconvenienti significativi superabili con alcune difficoltà (ad esempio: costi supplementari, indisponibilità di accedere a servizi, paura, mancanza di comprensione, stress, disturbi fisici minori ecc.)
3 ≤ SE < 4	**Alto**	gli individui possono incontrare conseguenze significative superabili con gravi difficoltà (ad esempio: appropriazione indebita di fondi, inserimento in black list, danni alla proprietà, perdita del lavoro, chiamata in giudizio, peggioramento dello stato di salute ecc.).
4 ≤ SE	**Elevato**	gli individui possono incontrare conseguenze significative o irreversibili, che potrebbero non essere in grado di superare (ad esempio: incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte ecc.).

Nella formulazione della valutazione complessiva della severità del breach occorre tenere in considerazione altri fattori:

- il numero degli interessati ed il volume dei dati;
- eventuali misure di sicurezza adottate dal Titolare del Trattamento (ad esempio, crittografia, back-up, anonimizzazione etc..) a tutela dei dati personali oggetto di violazione dei dati personali nell'ambito del contesto in cui si è verificato l'incidente di sicurezza, che riducano l'intellegibilità dei dati o la facilità di ripristino dell'integrità e disponibilità;
- di tutti gli elementi emersi nella compilazione del questionario di cui **all'Allegato 1),** al presente per farne parte integrante e sostanziale..

4.1.4 Notifica al Garante Privacy e comunicazione ai soggetti interessati

Tenendo conto del livello di rischio identificato, il Titolare considera la notifica del Data Breach al Garante Privacy. Quando il livello di rischio per i diritti e le libertà dell'interessato è elevato, si deve, altresì, comunicare, ove necessario, ai soggetti interessati, come di seguito indicato:

- Notifica al Garante Privacy

  Il Titolare del Trattamento è tenuto, senza indebiti ritardi, ove possibile, entro 72 ore dal momento in cui è venuto a conoscenza, a notificare la violazione al Garante Privacy, a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.

  Qualora sia il Responsabile del Trattamento a venire a conoscenza di una eventuale violazione, questi è tenuto a informare tempestivamente il Titolare del Trattamento in modo che possa attivarsi.

  Come indicato dal Garante Privacy, vanno notificate unicamente le violazioni di dati personali che possono avere effetti avversi e significativi sugli individui, causando danni fisici, materiali o immateriali. Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali da parte dell'interessato, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

  La notifica al Garante Privacy va effettuata utilizzando il modello ufficiale emesso dal Garante Privacy in data 30 luglio 2019, di cui all' **Allegato 3)** al presente per farne parte integrante e sostanziale, ed inviata alla seguente e-mail: protocollo@pec.gpdp.it

Laddove non sia possibile fornire contestualmente alla notifica tutte le informazioni richieste, verrà spiegato che è necessario effettuare ulteriori indagini e gli altri dettagli saranno forniti in seguito.

- Comunicazione ai soggetti Interessati

  Oltre alla notifica al Garante Privacy, laddove la violazione di dati personali possa comportare un rischio elevato per i diritti e le libertà dei Soggetti Interessati, il Titolare del Trattamento è tenuto ad informare gli stessi senza indebito ritardo al fine di renderli consapevoli e aiutarli a prendere provvedimenti contro eventuali conseguenze negative dovute alla violazione dei loro dati.

  La comunicazione agli interessati non è obbligatoria nei casi in cui:
  - il Titolare del Trattamento ha implementato misure di sicurezza appropriate ai dati coinvolti dalla violazione (ad esempio, rendendo indecifrabili i dati attraverso tecniche di crittografia);
  - il Titolare del Trattamento ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
  - comporterebbe uno sforzo sproporzionato (in tal caso il Titolare del Trattamento fornirà dichiarazioni pubbliche o misure simili per informare gli interessati).

  La comunicazione ai soggetti interessati deve includere almeno le seguenti informazioni in un linguaggio semplice e chiaro:
  - descrizione della natura della violazione dei dati personali;
  - nome e dati di contatto del DPO e del Referente Privacy;
  - descrizione delle probabili conseguenze della violazione dei dati personali;
  - descrizione delle misure adottate o proposte per porre rimedio alla violazione di dati personali, comprese eventuali misure di attenuazione degli effetti negativi della violazione.

CASISTICA

Di seguito sono indicati alcuni esempi che possono essere utili per determinare quando notificare la violazione dei dati personali al Garante Privacy e quando, in caso di rischio elevato, ai Soggetti Interessati.

Data Breach	Notifica al Garante?	Notifica al Soggetto Interessato?
Il backup di un archivio di dati personali crittografati viene memorizzato su una chiavetta USB e questa viene rubata.	No. Se i dati sono crittografati con algoritmo avanzato e il backup dei dati può essere ripristinato in tempo utile, non è obbligatorio notificare l'incidente.	No.
Il sito online subisce un attacco informatico e vengono rubati nomi utente, password e altri dati degli utenti	Sì, se vi sono probabili conseguenze negative per i Soggetti Interessati	Sì, se la gravità delle probabili conseguenze negative per gli interessati è elevata. La notifica dipende anche dalla portata e dal tipo di dati personali sottratti, nonché dagli altri fattori indicati nel paragrafo 5.1.2
Una e-mail viene inviata agli utenti includendo il loro indirizzo e-mail come destinatari "*in chiaro*", invece che in "*ccn*"	Sì, se vi sono probabili conseguenze negative per i Soggetti Interessati. La notifica può essere ritenuta necessaria se viene interessato un numero elevato di soggetti, oppure vengono sottratti dati sensibili o se	No, ma dipende dall'ambito e dal tipo di dati personali, nonché dagli altri fattori indicati nel paragrafo 5.1.2. La notifica potrebbe non essere necessaria se viene rivelato un basso numero di indirizzi e-mail e sono coinvolti solo dati semplici

	ricorrono altri fattori che comportano rischi privacy elevati	

4.1.5 *Mitigazione e ripristino*

Il Referente Privacy, con il supporto dell'Ufficio Programmazione e Trasparenza, il responsabile SIC, il Dirigente del settore procedente che ha identificato l'anomalia, con il coinvolgimento del DPO valutano l'adozione di ulteriori azioni immediate per mitigare i rischi connessi alla violazione dei dati e definiscono un piano d'azione per evitare il ripetersi di situazioni che possano causare situazioni simili di rischio in futuro. Se sono coinvolti processi o sistemi in outsourcing, il Dirigente del Settore che ha il contatto con il fornitore, supportato dal SIC, richiede che il fornitore esamini la potenziale violazione di dati e condivida azioni contingenti e tempestive.

4.1.6 *Registro delle violazioni di dati personali*

Qualsiasi violazione di dati personali deve essere documentata, inclusi i fatti avvenuti, i suoi effetti e le misure correttive adottate. La violazione dei dati personali deve essere documentata aggiornando, con le informazioni pertinenti richieste, il registro delle violazioni dei dati personali di cui all' **Allegato 2)** al presente per farne parte integrante e sostanziale; detto registro è depositato agli atti d'ufficio del SIC.

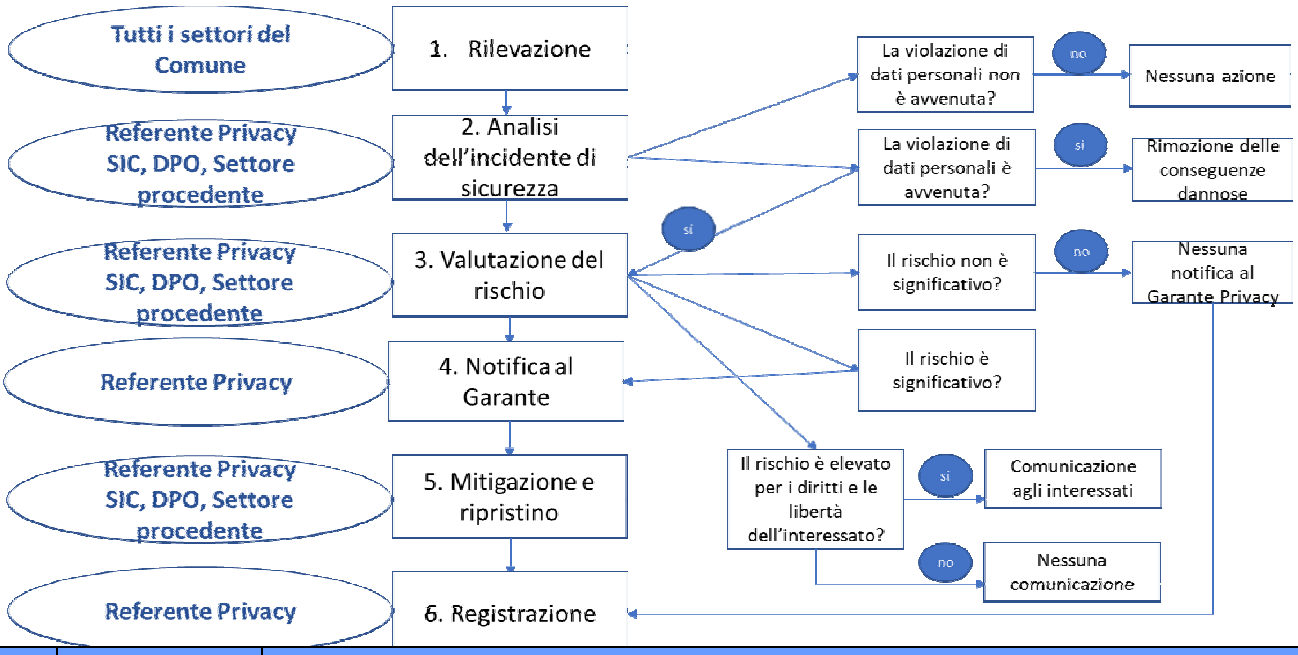
4.1.7 *Sanzioni amministrative*

In caso di mancato rispetto delle procedure di notifica della violazione, si applica la sanzione amministrativa fino a un massimo di Euro 10.000.000,00=

4.2 Diagramma di flusso

Il diagramma, di seguito riportato, illustra il processo per la gestione del Data Breach.
Le figure coinvolte sono:

- Il Referente Privacy
- Il SIC
- Il DPO (eventuale)
- Il Dirigente del Settore che ha identificato l'anomalia



	Fase	Descrizione
1	Rilevazione	Qualsiasi dipendente o collaboratore che identifichi un incidente di sicurezza o una potenziale violazione di dati personali o riceva una segnalazione a tale riguardo informa immediatamente tramite e-mail il proprio Dirigente, il Referente Privacy e il SIC.
2	Analisi dell'incidente di sicurezza	Il Referente Privacy, con il supporto dell'Ufficio Programmazione e Trasparenza, il responsabile SIC, il Dirigente del settore procedente che ha identificato l'anomalia, con il coinvolgimento del DPO,analizzano l'accaduto al fine di valutare se la violazione di dati personali si sia effettivamente verificata, considerando: ▪ natura della potenziale violazione di dati personali; ▪ categorie e numero approssimativo di soggetti interessati; ▪ categorie e numero approssimativo di dati personali interessati; ▪ tipo ed entità dei rischi per gli Interessati; ▪ probabili conseguenze della violazione dei dati personali, compresi potenziali danni economici e reputazionali; ▪ processi aziendali e sistemi informatici interessati; ▪ misure tecniche / organizzative non presenti o aggirate. Se sono coinvolti processi o sistemi in outsourcing, Il Dirigente che ha il contatto con il fornitore, supportato dal SIC, richiede che il fornitore esamini la potenziale violazione di dati e condivida azioni contingenti e tempestive. (Allegato 1 – Questionario di valutazione della violazione dei dati personali)
3	Valutazione del rischio per i diritti e le libertà degli interessati	Il Referente Privacy, con il supporto dell'Ufficio Programmazione e Trasparenza, il responsabile SIC, il Dirigente del settore procedente che ha identificato l'anomalia, con il coinvolgimento del DPO procedono ad un *risk assessment* se l'analisi preliminare ha confermato che si è verificata una violazione di dati personali. La valutazione del rischio indaga in modo tempestivo i rischi per i diritti e le libertà degli Interessati, in modo che la decisione di cui al punto 5 possa essere presa in tempo utile. Nel caso in cui siano identificati rischi, devono essere adottate misure correttive per la protezione dei dati violati.

4	Notifica	Se la violazione dei dati personali ha comportato rischi per i diritti e le libertà dei Soggetti Interessati, il Referente Privacy, con il supporto dell'Ufficio Programmazione e Trasparenza, informa il Garante Privacy circa la violazione avvenuta, entro 72 ore dal momento in cui si è venuti a conoscenza della violazione. Se viene valutato che la violazione dei dati personali possa comportare un rischio elevato per i diritti e le libertà dei Soggetti Interessati, il Referente Privacy, con il supporto dell'Ufficio Programmazione e Trasparenza dovrà prontamente comunicare la violazione ai soggetti stessi (tramite comunicazione personale o e-mail per volumi contenuti, altrimenti attraverso avviso sul sito istituzionale dell'Ente).
5	Mitigazione e ripristino	Il Referente Privacy, con il supporto dell'Ufficio Programmazione e Trasparenza, il responsabile SIC, il Dirigente del settore procedente che ha identificato l'anomalia, con il coinvolgimento del DPO, valutano l'adozione di un piano di mitigazione dei rischi connessi alla violazione dei dati e definiscono un piano d'azione per evitare il ripetersi di situazioni che possano causare situazioni simili di rischio in futuro.
6	Registrazione	Il Referente Privacy, con il supporto dell'Ufficio Programmazione e Trasparenza, ed il Responsabile SIC devono tenere un elenco delle violazioni di dati personali, contenente: ▪ natura dei dati personali coinvolti dalla violazione; ▪ categorie di dati; ▪ numero approssimativo di Soggetti Interessati; ▪ numero approssimativo di record di dati in oggetto; ▪ sistemi IT impattati; ▪ probabili conseguenze per il Comune e per gli Interessati; ▪ misure di sicurezza al momento dell'incidente; ▪ misure di sicurezza implementate successivamente all'incidente per ridurre i rischi immediati; ▪ misure di sicurezza pianificate per ridurre il ripetersi di situazioni simili; ▪ contatti del Referente Privacy e del DPO. Il registro delle violazioni di sicurezza è depositato agli atti d'ufficio del SIC (Allegato 2 – Registro delle violazioni di dati personali)

ART. 5 - ALLEGATI

- *Allegato 1:* Questionario di valutazione della violazione di dati personali
- *Allegato2:* Registro delle violazioni di dati personali
- *Allegato 3:* Modello di notifica del Data Breach al Garante Privacy

Allegato 1 – Questionario di valutazione della violazione di dati personali

Domande	Note
Che cosa è avvenuto?	*Descrivere l'incidente di sicurezza (es., divulgazione accidentale non autorizzata; perdita, distruzione; furto, attacco informatico)*

Quando è accadutol'incidente?	*Fornire informazioni sulla tempistica dell'incidente (es., accesso non autorizzato avvenuto il giorno 2 Feb 2019 alle ore 2:00 del mattino*
Quali categorie di dati sono state oggetto di incidente?	*Indicare le tipologie di dati oggetto della violazione (es., dati biografici (nome,cognome) edettagli di contatto (email))*
Quanti Soggetti Interessati sono coinvolti dalla violazione?	*Indicare il numero approssimativo di Soggetti Interessati i cui dati sono stati violati. (es., 1000)*
Quali categorie di Soggetti Interessati sono coinvolti dalla violazione?	*Indicare le categorie di Soggetti Interessati (es., dipendenti del Comune, consiglieri comunali, specifiche categorie di utenti)*
L'incidente di sicurezza coinvolge altri Paesi EU o extra EU?	*Indicare se vi sono altri Paesi esteri coinvolti (es., domiciliati esteri in Francia, in Svizzera,ecc)*
Vi sono stati casi simili in passato?	*Se sì, descrivere la situazione già successa (es., nel 2017il Comune è stato oggetto di attacco informatico avvenuto …)*
Quali sistemi / dispositivi / strumenti sono stati oggetto di incidente?	*Indicare i sistemi coinvolti dalla violazione di dati (es., workstation, smartphone, chiavette USB, etc.)*
Quali misure tecniche e organizzative di sicurezza erano attive al momento dell'incidente?	*Descrivere le misure di sicurezza in essere al momento della violazione (es., user ID e password complesse per accesso ai dati, log degli accessi al DB oggetto di attacco, crittografia del DB, DB in cloud presso il fornitore … etc)*
Sono coinvolti Responsabili esterni del trattamento?	*Se sì, indicare il Responsabile del trattamento dei dati oggetto di violazione (es., fornitore …).*
Quali tipi di rischi /danni potrebbero incorrere i Soggetti Interessati dalla violazione?	*Fornire informazioni sui rischi della violazione avvenuta e quali danni potrebbero essere / sono riscontrati per i Soggetti Interessati. (es., la perdita delle user ID e password degli utenti che usano la PEC fornita dal Comune potrebbe comportare l'accesso a comunicazioni riservate dell'utente; altri rischi finanziari, di reputazione).*
Quali iniziative sono state prese per ridurre o eliminare il rischio attuale e l'ipotesi che si possa ripetere in futuro?	*Se vi sono iniziative in corso e/o future per ridurre il disagio dell'incidente avvenuto ed evitare che si ripeta, descrivere le misure contingenti e/o pianificate (es., le vulnerabilità del sistema sono state rimosse; la password è stata rafforzata come complessità; è pianificata una revisione di tutte le utenze entro il giorno … , etc.).*

E' possibile il ripetersi della violazione?	*Descrivere le condizioni per cui potrebbe ripetersi la violazione (es., Si, il piano di rimedio delle vulnerabilità riscontrate richiede un tempo di 6 mesi; è stata data priorità alle misure … per mitigare incidenti futuri).*
Fornitore che agisce come Responsabile del trattamento di dati	
Sono formalizzati livelli di servizio relativamente alla gestione dei dati e nel caso di incidente di sicurezza?	*Se sì, descrivere gli accordi sulla gestione dei dati tra il Comune e il fornitore, anche per la gestione di violazioni di dati personali*
Che tipo di supporto ha fornito il responsabile esterno in merito all'incidente di sicurezza?	*Fornire informazioni circa la tempistica di comunicazione del Data Breach e le iniziative svolte e/o concordate con il Titolare in merito alla gestione della violazione di dati personali*

Allegato 2 – Registro delle violazioni di dati personali

ID violazione	
Descrizione della violazione	
Data / Periodo della violazione	
Categorie di dati coinvolti	
Numero di Soggetti Interessati coinvolti	
Numero di dati coinvolti	
Sistemi coinvolti	
Conseguenze e azioni di rimedio adottate	
Conseguenze / Danni per il Comune (finanziari, reputazionali, etc.)	
Conseguenze / Danni per I Sogegtti Interessati (finanziari, reputazionali, etc.)	
Misure di sicurezza tecniche e organizzative presenti al momento della violazione	

Misure di sicurezza tecniche e organizzative implementate successivamente all'incidente per ridurre i rischi immediati	
Misure di sicurezza tecniche e organizzative pianificate per evitare il ripetersi di situazioni simili	
Contatto Referente interno Privacy	
Contatto DPO	
Istituzioni informate/coinvolte per il Data Breach	
Esito Risk Assessment	
Notifica al Garante Privacy	
Notifica ai SoggettiInteressati	
Note	

Allegato 3 – Modello di Notifica al Garante Privacy

modello Notifica del Garante 30072019.pdf