COMUNE DI PECETTO TORINESE

Sede Municipale di via Umberto I n.3
Tel. 0118609218/9 - Fax 0118609073
sito www.comune.pecetto.to.it - mail: info@comune.pecetto.to.it
Pec: info@pec.comune.pecetto.to.it

Regolamento (UE) 2016/679 relativo alla protezione dei dati personali

Guida per la gestione delle violazioni di dati personali (Data Breach)

Rev. 1.0

Ottobre 2019

Sommario

1. Premessa

Il presente documento costituisce una "**Guida**" a beneficio dei dipendenti dell'Ente incaricati dello svolgimento delle attività di trattamento dei dati e dei Responsabili delle attività di Trattamento dei Dati svolte per conto del Comune (Titolare del Trattamento).

Documenti di riferimento
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 - RGDP)
D. Lgs. 196 del 30 giugno 2003, recante il "Codice in materia di protezione dei dati personali", come modificato, da ultimo, dal D. Lgs. 10 agosto 2018, numero 101
Linee-guida del Gruppo "Articolo 29" in materia di notifica delle violazioni di dati personali, approvate, in via definitiva, il 6 febbraio 2018. Il Gruppo di lavoro "Articolo 29" ("Art. 29 WP") è il gruppo di lavoro europeo indipendente che ha trattato questioni relative alla protezione della vita privata e dei dati personali fino al 25 maggio 2018 (entrata in vigore del RGPD)
"**Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali**" del Garante per la protezione dei dati personali

Quanto di seguito descritto dovrà essere integrato e modificato in relazione all'**evoluzione normativa** italiana ed europea, delle **migliori pratiche** che si considereranno nel tempo e delle **prassi** che si svilupperanno all'interno dell'Ente.

2. Che cosa è una violazione dei dati personali?

All'articolo 4, punto 12, il Regolamento definisce la "violazione dei dati personali" come "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".

Tabella riepilogativa delle tipologie di effetti delle violazioni	
Distruzione	Ogni qual volta i dati non esistono più o non esistono più in una forma che sia di qualche utilità per il Titolare del Trattamento
Danno	Quando i dati personali sono stati modificati, corrotti o non sono più completi;
Perdita	Nel caso in cui i dati personali potrebbero comunque esistere, ma il Titolare del Trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso[1].
Trattamento non autorizzato o illecito	Quando viene effettuata una divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure quando viene svolta qualsiasi altra forma di trattamento in violazione del

[1] Un esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati dei clienti del titolare del trattamento; oppure il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un ransomware (malware del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso.

	regolamento

Violazione dei dati personali e incidente di sicurezza
Una violazione è un tipo di **incidente di sicurezza**. In caso di incidente di sicurezza, come indicato all'articolo 4, punto 12, il Regolamento si applica soltanto in caso di **violazione di dati personali**. La conseguenza di una violazione è che il Titolare del Trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del Regolamento. **Mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali**.

3. Tipologia di violazioni dei dati personali

Nel parere 03/2014 sulla notifica delle violazioni, il Gruppo di lavoro "Articolo 29" ha spiegato che le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni:

Violazione della **riservatezza**	In caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali
Violazione dell'**integrità**	In caso di modifica non autorizzata o accidentale dei dati personali
Violazione della **disponibilità**	In caso di perdita, accesso[2] o distruzione accidentali o non autorizzati di dati personali

Occorre considerare che:

- una violazione può riguardare **contemporaneamente** la **riservatezza**, l'**integrità** e la **disponibilità** dei dati personali, nonché qualsiasi combinazione delle stesse;
- stabilire se vi sia stata una violazione della riservatezza o dell'integrità è relativamente semplice, meno evidente può essere determinare se vi è stata una violazione della disponibilità;
- se si è verificata una **perdita** o una **distruzione permanente** dei dati personali sarà sempre considerata una violazione della **disponibilità**.

Esempi di perdita di disponibilità possono essere i seguenti:

- quando i dati vengono **cancellati accidentalmente** o da una **persona non autorizzata**;
- quando la chiave di decifratura di dati crittografati viene **persa** e il Titolare del Trattamento non è in grado di **ripristinare** l'accesso agli stessi ricorrendo a un **backup**;
- in caso di interruzione del servizio abituale di un'organizzazione dovuto ad esempio ad un'**interruzione di corrente** o ad un attacco da "**blocco di servizio**" ("denial of service") che rende i dati personali indisponibili per un tempo significativo.

[2] L'accesso è una componente fondamentale della "disponibilità". In tal senso, si veda il documento NIST SP80053rev4, che definisce la "disponibilità" come la "garanzia di un accesso e un uso tempestivi e affidabili delle informazioni", nonché la norma ISO/IEC 27000:2016, che definisce la "disponibilità" come la "proprietà di essere accessibile e utilizzabile su richiesta da un soggetto autorizzato.

Perché l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione?

L'articolo 32 del Regolamento ("Sicurezza del Trattamento") spiega che, nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, la capacità di **assicurare su base permanente**

- la **riservatezza**
- l'**integrità**
- la **disponibilità**
- la **resilienza** dei sistemi e dei servizi di trattamento

e la capacità di **ripristinare tempestivamente** la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".

Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una **violazione**, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche.

Come nel caso della perdita o distruzione permanente dei dati personali (o comunque di qualsiasi altro tipo di violazione), una violazione che implichi la perdita temporanea di disponibilità dovrebbe essere **documentata** in conformità all'articolo 33, paragrafo 5. Ciò aiuta il titolare del trattamento a **dimostrare l'assunzione di responsabilità** all'autorità di controllo, che potrebbe chiedere di consultare tali registrazioni. Tuttavia, a seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all'autorità di controllo e la comunicazione alle persone fisiche coinvolte.

Il Titolare del Trattamento dovrà valutare la **probabilità** e la **gravità** dell'impatto dell'indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche. Conformemente all'articolo 33, il Titolare del Trattamento dovrà effettuare la notifica a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Questo punto dovrà chiaramente essere **valutato caso per caso**.

Va notato che, sebbene una perdita di disponibilità dei sistemi del Titolare del Trattamento possa essere solo temporanea e non avere un impatto sulle persone fisiche, è importante che il Titolare del Trattamento consideri tutte le possibili **conseguenze** della violazione, poiché quest'ultima potrebbe comunque dover essere segnalata per altri motivi.

4. La notifica di una violazione di dati personali: la comunicazione all'Autorità di controllo ai sensi dell'articolo 33 del GDPR

Il Regolamento (UE) 2016/679 afferma[3] che una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare **danni fisici**, **materiali** o **immateriali** alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Pertanto, non appena viene a **conoscenza** di un'avvenuta violazione dei dati personali, il Titolare del Trattamento deve **notificare** la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che non sia in grado di dimostrare che, conformemente al principio di **responsabilizzazione**, è

[3] Regolamento (UE) 679/2016, Considerando 85

improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Quando il Titolare può considerarsi a conoscenza di una violazione
Questo punto solleva la questione relativa al momento in cui il Titolare del Trattamento può considerarsi "**a conoscenza**" di una violazione. Il Gruppo di lavoro "Articolo 29" ritiene che il Titolare del Trattamento debba considerarsi "a conoscenza" nel momento in cui è **ragionevolmente certo** che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali. Il Titolare del Trattamento è quindi tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate. Il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione: in alcuni casi sarà relativamente evidente, fin dall'inizio, che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, l'accento dovrebbe essere posto sulla **tempestività** dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere **misure correttive** ed effettuare la **notifica**, se necessario.

Esempi di violazioni che richiedono notifica	
1	In caso di perdita di una chiave USB contenente dati personali non crittografati spesso non è possibile accertare se persone non autorizzate abbiano avuto accesso ai dati. Tuttavia, anche se il Titolare del Trattamento non è in grado di stabilire se si è verificata una violazione della riservatezza, si ritiene che tale caso debba essere notificato, in quanto sussisterebbe una ragionevole certezza del fatto che potrebbe essersi verificata una violazione della disponibilità; il titolare del trattamento si considera venuto "a conoscenza" della violazione nel momento in cui si è accorto di aver perso la chiave USB.
2	Un terzo informa il titolare del trattamento di aver ricevuto accidentalmente i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata. Dato che al titolare del trattamento è stata presentata una prova evidente di una violazione della riservatezza, non vi è dubbio che ne sia venuto "a conoscenza".
3	Un titolare del trattamento rileva che c'è stata una possibile intrusione nella sua rete. Controlla quindi i propri sistemi per stabilire se i dati personali ivi presenti sono stati compromessi e ne ottiene conferma. Ancora una volta, dato che il titolare del trattamento ha una chiara prova di una violazione non può esserci dubbio che sia venuto "a conoscenza" della stessa.
4	Un criminale informatico viola il sistema del titolare del trattamento e lo contatta per chiedere un riscatto. In tal caso, dopo aver verificato il suo sistema per accertarsi dell'attacco, il titolare del trattamento dispone di prove evidenti che si è verificata una violazione e non vi è dubbio che ne sia venuto a conoscenza.
5	Inoltre, va osservato che se si verifica una violazione **in assenza di backup** dei dati personali crittografati si è in presenza di una violazione della disponibilità che potrebbe presentare rischi per le persone fisiche e pertanto potrebbe richiedere la notifica. Analogamente, laddove si verifichi una violazione che implichi la perdita di dati crittografati, anche se esiste una copia di backup dei dati personali si potrebbe comunque trattare di una violazione soggetta a segnalazione, a seconda del periodo di tempo necessario per **ripristinare** i dati dal backup e

	dell'effetto che la mancanza di disponibilità ha sulle persone fisiche. Come afferma l'articolo 32, paragrafo 1, lettera c), un importante fattore di sicurezza è "**la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico**".

	Esempi di violazioni che non richiedono la notifica
1	L'articolo 33, paragrafo 1, chiarisce che se è "improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche" tale violazione non è soggetta a notifica all'autorità di controllo. Un esempio potrebbe essere quello di dati personali già disponibili pubblicamente, la cui divulgazione non costituirebbe un rischio probabile per la persona fisica.
2	Una violazione che non richiederebbe la notifica all'autorità di controllo sarebbe la perdita di un dispositivo mobile crittografato in maniera sicura, utilizzato dal titolare del trattamento e dal suo personale. Se la chiave di cifratura **rimane in possesso** del Titolare del Trattamento e non si tratta dell'unica copia dei dati personali, questi ultimi sarebbero **inaccessibili** a qualsiasi pirata informatico. Ciò significa che è improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati in questione. Se in seguito diventa evidente che la chiave di cifratura è stata **compromessa** o che il software o l'algoritmo di cifratura è **vulnerabile**, il rischio per i diritti e le libertà delle persone fisiche cambia e potrebbe quindi essere necessaria la notifica.

Crittografia sicura e violazione dei dati
Nel caso in cui i dati non siano stati effettivamente crittografati in maniera sicura si incorrerà nel mancato rispetto dell'articolo 33 se il Titolare del Trattamento non effettua la notifica all'autorità di controllo. Di conseguenza, nel selezionare il software di cifratura, il titolare del trattamento deve valutare attentamente la **qualità** e la **corretta attuazione** della cifratura offerta, capire il livello di protezione effettivamente offerto e se quest'ultimo è **appropriato** in ragione dei rischi presentati. Il Titolare del Trattamento dovrebbe avere familiarità con le specifiche modalità di funzionamento del prodotto di cifratura. Ad esempio, un dispositivo può essere crittografato una volta spento, ma non mentre è in modalità stand-by. Alcuni prodotti che utilizzano la cifratura dispongono di "chiavi predefinite" che devono essere modificate da ciascun cliente per essere efficaci. La cifratura potrebbe essere considerata adeguata dagli esperti di sicurezza al momento della sua messa in atto, ma diventare **obsoleta** nel giro di pochi anni, il che significa che può essere messo in discussione il fatto che i dati siano sufficientemente crittografati dal prodotto in questione e che quest'ultimo fornisca un livello appropriato di protezione.

5. La comunicazione di una violazione di dati personali: la comunicazione agli interessati ai sensi dell'articolo 34 del GDPR

In alcuni casi, oltre a effettuare la notifica all'autorità di controllo, il Titolare del Trattamento è tenuto a comunicare la violazione alle **persone fisiche interessate**. L'articolo 34, paragrafo 1, afferma 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 comunica la violazione all'interessato senza ingiustificato ritardo".

La soglia per la comunicazione delle violazioni alle persone fisiche è più elevata rispetto a quella della notifica alle autorità di controllo, pertanto non tutte le violazioni dovranno essere comunicate agli interessati, il che li protegge da inutili disturbi arrecati dalla notifica.

Il Regolamento afferma che la comunicazione di una violazione agli interessati dovrebbe avvenire "**senza ingiustificato ritardo**", il che significa "**il prima possibile**".
L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro **informazioni specifiche** sulle misure che questi possono prendere per **proteggersi**[4].

L'articolo 34, paragrafo 2, del Regolamento precisa che "La comunicazione all'interessato (…) deve descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d)".

In sostanza, il Titolare del Trattamento deve fornire, secondo tale disposizione, almeno le seguenti informazioni:

- una descrizione della **natura** della violazione;
- il **nome** e i **dati di contatto** del Responsabile della Protezione dei Dati o di altro punto di contatto;
- una descrizione delle probabili **conseguenze** della violazione;
- una descrizione delle **misure adottate** o di cui si propone l'adozione da parte del Titolare del Trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

In linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo **sproporzionato**; in tal caso, si procede a una **comunicazione pubblica** o a una misura simile che permetta di informare gli interessati con analoga efficacia (articolo 34, paragrafo 3, lettera c).

Esempi di metodi trasparenti di comunicazione agli interessati da una violazione	
1	La messaggistica diretta (ad esempio messaggi di posta elettronica, SMS, messaggio diretto)
2	Banner o notifiche su siti web di primo piano
3	Comunicazioni postali e pubblicità di rilievo sulla stampa

Una semplice comunicazione all'interno di un comunicato stampa o di un blog aziendale non costituirebbe un mezzo efficace per comunicare una violazione all'interessato.

[4] Regolamento (UE) 679/2016, Considerando 86

Quando non è richiesta una comunicazione agli interessati	
L'articolo 34, paragrafo 3, stabilisce tre condizioni che, se soddisfatte, non richiedono la comunicazione agli interessati in caso di violazione	
1	Il Titolare del Trattamento ha applicato misure tecniche e organizzative **adeguate** per proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali **incomprensibili** a chiunque non sia autorizzato ad accedervi
2	Immediatamente dopo una violazione, il Titolare del Trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche
3	Qualora contattare gli interessati richiederebbe uno **sforzo sproporzionato**, ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione o non siano mai stati noti.

Conformemente al **principio di responsabilizzazione**, il Titolare del Trattamento dovrebbe essere in grado di dimostrare all'autorità di controllo di soddisfare una o più di queste condizioni[5].

Necessità di comunicazione nel caso cambi la situazione
Sebbene la comunicazione possa inizialmente non essere richiesta se non vi è alcun rischio per i diritti e le libertà delle persone fisiche, la situazione potrebbe **cambiare** nel corso del tempo e il rischio dovrebbe essere **rivalutato**. Se il Titolare del Trattamento decide di non comunicare una violazione all'interessato, l'articolo 34, paragrafo 4, spiega che l'autorità di controllo può richiedere che lo faccia, qualora ritenga che la violazione possa presentare un rischio elevato per l'interessato. In alternativa, può ritenere che siano state soddisfatte le condizioni di cui all'articolo 34, paragrafo 3, nel qual caso la comunicazione all'interessato non è richiesta. Qualora stabilisca che la decisione di non effettuare la comunicazione all'interessato non sia fondata, l'autorità di controllo può prendere in considerazione l'esercizio dei poteri e delle sanzioni a sua disposizione

[5] Cfr. articolo 5, paragrafo 2, del RGPD.

6. Gestione di una violazione interna al Comune: procedura e misure specifiche

È stato redatto uno specifico documento denominato "**Procedura per la gestione delle Violazioni dei dati personali | Data Breach**" con lo scopo di indicare puntualmente alla struttura comunale le opportune modalità di gestione di un data breach, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento (UE) 679/2016, e della disciplina interna per la definizione della organizzazione delle attività di trattamento e per la gestione delle Violazioni dei dati personali.

In questo documento sono sintetizzate le regole per garantire il rispetto dei principi esposti ed è descritta la **procedura operativa** che l'organizzazione deve seguire nella gestione di un data breach, sotto i diversi aspetti che riguardano:

- la mappa delle **responsabilità** che individua i **ruoli** e i **compiti** all'interno dell'organizzazione;
- il sistema di **rilevazione** dei Data Breach;
- una procedura per la **gestione** dei Data Breach;
- le modalità di **aggiornamento** del **Registro delle Violazioni**.

È necessario che sia data notizia a tutti i dipendenti in merito alla citata procedura mediante idonea circolare.

7. Gestione di una violazione presso un Responsabile Esterno del Trattamento

Quando un terzo agisce in qualità di Responsabile Esterno della attività di Trattamento svolte per conto e nell'interesse del Comune, in caso di violazione dei dati personali, **deve informare l'Ente** (che agisce in qualità di Titolare) **senza ingiustificato ritardo** e non al più tardi di 24 ore dal momento in cui ha conoscenza della violazione, inviando una **comunicazione via mail** (ove possibile via PEC):

Successivamente sarà tenuto a **collaborare** con il Comune per consentirgli di adempiere agli obblighi previsti dalla normativa agli articoli 33 e 34 del Regolamento.