Linee guida del Consiglio regionale del Friuli Venezia Giulia per la gestione delle violazioni di dati personali (data breach) e la loro eventuale comunicazione all'Autorità e ai soggetti interessati ai sensi del Regolamento (UE) 2016/679 (GDPR).

1- Obiettivi del Documento

Il presente documento ha l'obiettivo di fornire un quadro chiaro e dettagliato delle procedure da seguire in caso di violazioni di dati personali, comunemente note come "data breach" all'interno degli uffici del Consiglio regionale FVG, al fine di garantire una gestione efficace e tempestiva delle violazioni, minimizzando i rischi per i diritti e le libertà degli interessati.

Queste linee guida sono state redatte in conformità con il Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea (Regolamento (UE) 2016/679) e si applicano a tutti i dati personali trattati dai dipendenti, collaboratori, tirocinanti del Consiglio regionale e da terze parti, sia in formato cartaceo che elettronico.

2-Riferimenti Normativi e documenti

Le principali fonti normative di riferimento per la gestione delle violazioni dei dati personali sono:

- Regolamento UE 2016/679, con particolare attenzione alle disposizioni relative la notifica delle violazioni all'Autorità di controllo, agli interessati e la responsabilità del trattamento. (articoli 33, 34 e 28 e C 85, C86, C87 e C 88),

- Codice per la protezione dei dati personali (D.Lgs. 196/2003, come modificato dal Decreto Legislativo 101 del 10 agosto 2018 per allineare la normativa nazionale al Regolamento UE 2016/679 (GDPR)

- Codice dell'Amministrazione Digitale (CAD D.Lgs. 82/2005).

- Linee guida EDPB 09/2022, riguardanti gli obblighi di notifica delle violazioni dei dati personali secondo il GDPR, che hanno aggiornato le Linee guida WP250 del 2018.

- Linee guida EDPB 01/2021 su esempi riguardanti la notifica di violazione dei dati.

Queste norme stabiliscono i requisiti e le procedure che il Titolare del trattamento deve seguire per notificare le violazioni dei dati personali all'Autorità di controllo e, se necessario, agli interessati e sono soggette a possibili aggiornamenti anche in base a eventuali interventi del Comitato europeo per la protezione dei dati – EDPB e del Garante per la protezione dei dati personali.

3- Definizione di Violazione dei Dati

Secondo l'articolo 4, paragrafo 12, del Regolamento (UE) 2016/679 (GDPR) una "violazione dei dati personali" consiste in una 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.

Secondo le Linee guida EDPB 09/2022 le violazioni si suddividono in tre categorie principali:

- Violazione della riservatezza: Divulgazione o accesso non autorizzati o accidentali ai dati.

- Violazione dell'integrità: Modifica non autorizzata o accidentale dei dati.

- Violazione della disponibilità: Perdita o distruzione accidentali o non autorizzate dei dati.

La valutazione del rischio derivante da una violazione dei dati personali - che deve tener conto della probabilità e della gravità del suo impatto sulle persone fisiche i cui dati sono stati coinvolti (C75 e C76 GDPR) - è un importante adempimento che, conformemente al principio di responsabilizzazione, spetta al Titolare del trattamento e dalla quale deriva il corretto adempimento dell'obbligo di notifica della violazione all'Autorità di controllo e dell'eventuale obbligo di comunicazione agli interessati.

4-Principali soggetti coinvolti

Il Titolare del trattamento è obbligato a notificare all'Autorità di controllo (Garante per la protezione dei dati personali), entro 72 ore dalla scoperta, violazioni dei dati personali che presentino un rischio per i diritti e le libertà degli interessati. In caso di rischio elevato, è inoltre necessario informare tempestivamente gli interessati.

Il Responsabile del trattamento: Il Responsabile del trattamento informa il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione e lo assiste.

Il Responsabile della Protezione dei Dati (RPD), svolge un ruolo cruciale di consulenza per il Titolare del trattamento e funge da punto di riferimento per gli interessati e per l'Autorità di controllo. Il RPD garantisce la conformità dell'operato, nella gestione delle violazioni dei dati personali, alle normative sulla protezione dei dati.

5-Processo di notifica del data breach

In caso di violazione dei dati personali è necessario gestire questi passaggi:

- acquisizione della notizia e attivazione delle procedure di gestione;
- analisi dell'evento;
- valutazione della gravità dell'evento;
- notifica all'Autorità di controllo, se necessario;
- comunicazione agli interessati, se necessario;
- registrazione dell'evento nel Registro delle violazioni;
- azioni correttive specifiche e preventive.

Acquisizione della notizia

Il Responsabile del trattamento, nonché qualsiasi dipendente, collaboratore o terza parte che rilevi una sospetta violazione (data breach) dei dati personali trattati dal Consiglio regionale, deve darne notizia al Dirigente responsabile della struttura cui fa capo l'attività di trattamento oggetto della violazione, al Segretario generale e al RPD.

La segnalazione può avvenire tramite posta elettronica o avvertimento verbale/telefonico e deve fornire una prima descrizione dell'incidente.

Ai sensi dell'art. 33 del GDPR, dal momento in cui viene acquisita la notizia da parte del Titolare del trattamento, inizia a decorrere il termine di 72 ore per la eventuale notifica all'Autorità di controllo.

Analisi dell'Evento

Il Segretario generale - in collaborazione con il Responsabile del trattamento, il Dirigente responsabile della struttura interessata e il RPD - deve completare rapidamente un'istruttoria preliminare per raccogliere le seguenti informazioni minime sull'incidente:

- data/ora della rilevazione;

- descrizione dell'incidente e la natura della violazione;

- tipologia e quantità dei dati coinvolti;

- numero di interessati e sistemi coinvolti;

- probabili conseguenze e misure adottate o previste.

Ogni operazione deve essere tracciata e documentata.

Valutazione della Gravità dell'Evento

Il Segretario generale - in collaborazione con il Responsabile del trattamento, il Dirigente responsabile della struttura interessata e il RPD - valuta se l'incidente comporta un potenziale rischio per i diritti e le libertà degli interessati. Questa valutazione dovrà considerare:

- categorie particolari di dati coinvolti;

- la quantità dei dati personali e/o di soggetti interessati;

- il potenziale impatto sui diritti degli interessati;

- l'accessibilità dei dati compromessi da parte di terzi non autorizzati.

Se all'esito della valutazione, il rischio per i diritti e le libertà degli interessati risulta:

- assente: non sarà necessaria alcuna notifica, annotazione nel Registro delle violazioni;

- presente: dovere di notifica all'Autorità di controllo (art. 33 GDPR)[1]

- elevato: dovere di notifica all'Autorità di controllo e di comunicazione agli interessati. (art. 34 GDPR)[2]

[1] **Articolo 33 Notifica di una violazione dei dati personali all'autorità di controllo**
1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 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. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) 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;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

[2] **Articolo 34 Comunicazione di una violazione dei dati personali all'interessato**
1. 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.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) ed).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

Qualora Il Segretario generale, in collaborazione con il RPD, ritenga non sussistere l'esigenza di notifica all'Autorità di controllo, la procedura termina; il caso di "data breach" viene archiviato e le risultanze dell'istruttoria finale vengono riportate nel Registro delle violazioni.

Se dall'istruttoria svolta, la probabilità di rischio risulta presente, si procede con la notifica all'Autorità di controllo e, se necessario, agli interessati.

Notifica al Garante della Privacy

Se la violazione presenta un rischio per i diritti e le libertà delle persone fisiche, il Segretario generale, in collaborazione con il RPD, deve notificare, tramite PEC, senza ingiustificato ritardo e, se possibile, entro 72 ore, l'incidente all'Autorità di controllo competente (Garante per la protezione dei dati personali), includendo tutte le informazioni raccolte durante l'istruttoria preliminare. Se le informazioni non sono complete, possono essere fornite in fasi successive.

In particolare la notifica deve contenere:

- una descrizione della natura della violazione occorsa, compresi, ove possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di registrazioni dei dati personali;

- nome e dati di contatto del RPD e del Segretario generale;

- descrizione delle probabili conseguenze della violazione dei dati personali;

- descrizione delle misure adottate o di cui si propone l'adozione, per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

A partire dal 01/07/2021 la notifica di una violazione di dati personali deve essere inviata all'Autorità di controllo tramite un'apposita procedura telematica. E' operativo il servizio del Garante (https://servizi.gpdp.it/databreach/s/) per supportare i Titolari del trattamento negli adempimenti previsti in caso di violazioni dei dati personali (data breach).

Comunicazione agli interessati

Se la violazione comporta un rischio elevato per i diritti e le libertà delle persone fisiche, il Segretario generale, in collaborazione con il RPD, deve informare anche gli interessati senza ingiustificato ritardo.

La comunicazione agli interessati, deve includere con linguaggio semplice e chiaro:

- una descrizione della violazione;

- nome e dati di contatto del RPD e del Segretario generale;

- le misure adottate o proposte per mitigare i possibili effetti negativi;

- le misure che gli interessati possono adottare per proteggersi ulteriormente.

La comunicazione agli interessati non è necessaria:

---

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

- se sono state adottate misure tecniche e organizzative adeguate alla protezione dei dati personali trattati e se tali misure erano state applicate ai dati oggetto della violazione;

- qualora siano state adottate misure successive che assicurano che il rischio elevato per i diritti e le libertà degli interessai non sia più probabile che si concretizzi.

La comunicazione può essere diretta o, se troppo onerosa, effettuata tramite avviso pubblico.

Registro delle violazioni

Tutte le violazioni devono essere documentate nel Registro delle violazioni, anche quelle che non richiedono notifica. Questo Registro, deve contenere la descrizione della natura degli incidenti e le possibili cause, le misure adottate per la risoluzione, le eventuali notifiche effettuate, le azioni correttive implementate per prevenire future violazioni.

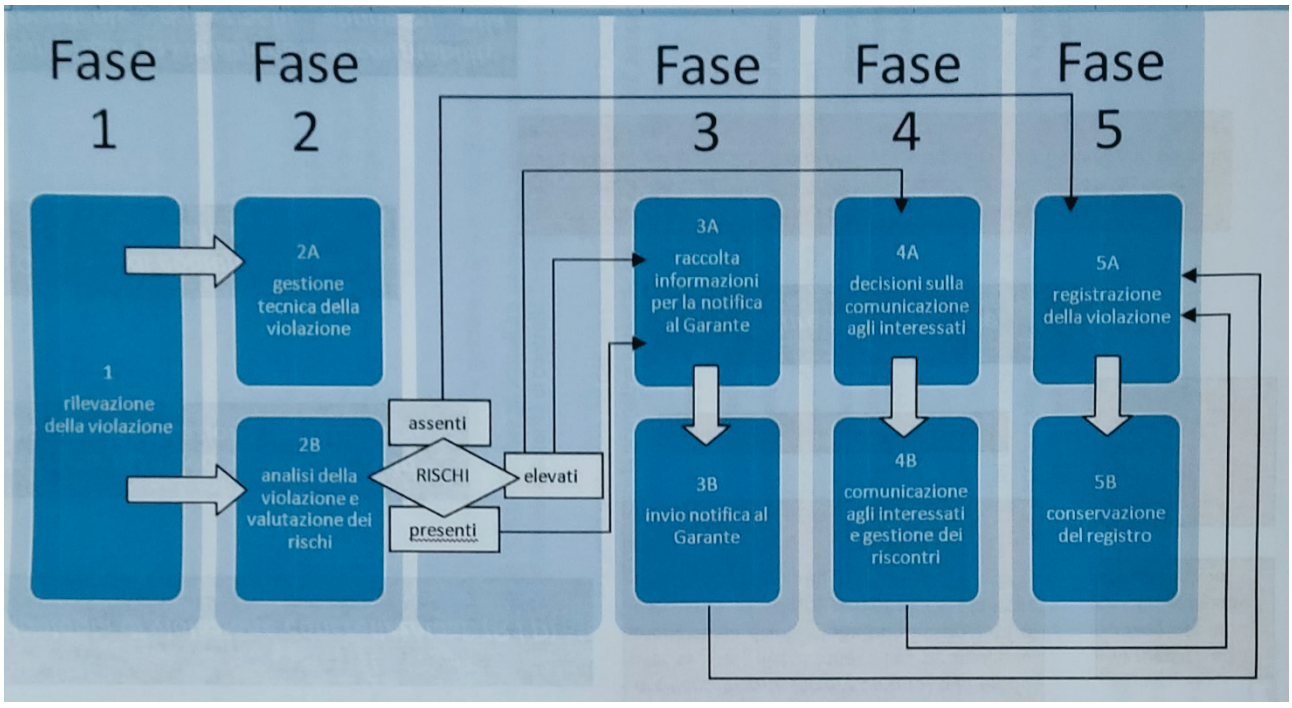
Miglioramento continuo

Dopo la gestione dell'evento, il Segretario generale, in collaborazione con il RPD e il Responsabile del trattamento, deve condurre un'analisi dettagliata per identificare eventuali lacune nelle misure di sicurezza e proporre miglioramenti per prevenire violazioni future.

Formazione e consapevolezza

Il Consiglio regionale promuove la formazione di tutti i dipendenti e collaboratori sulle procedure di rilevazione e gestione delle violazione dei dati personali (data breach) per garantire le migliori pratiche di sicurezza in relazione a possibili minacce.

Schema riepilogo obblighi di verifica:



Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: STEFANO PATRIARCA
*CODICE FISCALE: **********
DATA FIRMA: 24/06/2024 18:13:09

NOME: MAURO BORDIN
*CODICE FISCALE: **********
DATA FIRMA: 26/06/2024 14:32:36