REGIONE DEL VENETO

giunta regionale

Linee Guida per la notifica della violazione dei dati personali ("Data Breach")

Indice

1 Introduzione 3

2 Procedura di notifica di violazione dei dati personali ("Data Breach") 3

3 L'autorità di controllo dei dati personali 4

4 Decidere se notificare la violazione all'autorità di controllo dei dati personali 4

5 Come effettuare la notifica all'autorità di controllo dei dati personali 5

6 La comunicazione della violazione dei dati personali all'interessato 5

7 Comunicazione agli interessati 6

1 Introduzione

In data 27/04/2016 il Parlamento Europeo ed il Consiglio dell'Unione Europea hanno adottato il Regolamento (UE) 2016/679 recante *"Regolamento Generale sulla Protezione dei Dati – GDPR"*, il quale detta la normativa sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonchè alla libera circolazione di tali tipologie di dati.
In applicazione del suddetto Regolamento, con DGR n. 473 del 10/04/2018 è stato designato il Responsabile della Protezione dei Dati Personali (D.P.O.) mentre con DGR n. 596 del 08/05/2018 sono state adottate misure attuative relativamente alla protezione dei dati personali e sono state impartite istruzioni per i trattamenti dei medesimi dati.

Questa procedura è destinata ad essere utilizzata in caso di incidente di qualche tipo che abbia comportato, o che si ritiene abbia provocato, una perdita di dati personali di cui la Giunta Regionale sia titolare.
Un requisito del Regolamento Generale sulla Protezione dei Dati Personali dell'Unione Europea (GDPR) è che gli incidenti che hanno impatto sui dati personali e che potrebbero comportare un rischio per i diritti e le libertà delle persone interessate devono essere segnalati all'autorità di controllo della protezione dei dati senza ingiustificato ritardo e, ove possibile, entro 72 ore dall'avvenuta conoscenza.
Nel caso in cui il termine delle 72 ore sia superato, devono essere fornite le ragioni del ritardo.

Nel caso in cui un incidente riguardi i dati personali, deve essere effettuata una valutazione in merito ai destinatari, alla tempistica ed al contenuto della comunicazione da effettuare alle persone interessate. Il GDPR prescrive che la comunicazione debba avvenire senza indebiti ritardi se la violazione può comportare un alto rischio per i diritti e libertà delle persone fisiche .

Le azioni descritte nel presente documento costituiscono linea guida nella risposta agli incidenti, da valutare nella fattispecie concreta. Infatti, l'esatta natura di un incidente e il suo impatto non possono in alcun modo essere previsti in modo certo.

2 Procedura di notifica di violazione dei dati personali ("Data Breach")

Per gli incidenti i cui effetti possono essere la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (cd. "***databreach***"), l'utente provvede a segnalare tempestivamente la situazione al ***Call Center*** per l'espletamento delle verifiche di competenza e comunica al "Delegato" al trattamento (Direttore della struttura regionale di riferimento/appartenenza) le violazioni ai dati personali o gli incidenti informatici rilevati i quali possono avere un impatto significativo sui dati personali.
Ricevuta la segnalazione, il "Delegato" al trattamento si attiverà procedendo secondo le prescrizioni contenute nelle "*Istruzioni per i trattamenti di dati personali*" approvate con DGR n. 596/2018, a cui si rinvia. Pertanto ogni Delegato, non appena venuto a conoscenza di un *databreach*, effettuerà una prima necessaria istruttoria e, valutati i rischi per i diritti e le libertà delle persone fisiche, avviserà tempestivamente la Direzione ICT e Agenda Digitale ed il Data Protection Officer - DPO.
A sua volta il Direttore della Direzione ICT e Agenda Digitale, sulla base degli esiti della predetta istruttoria del Delegato, comunicherà al Garante per la Protezione dei dati personali il *databreach*, per conto del Titolare del trattamento senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, informandone contestualmente il Data Protection Officer - DPO.

Qualora le violazioni ai dati personali riguardino un servizio erogato in "cloud" da un "service provider" esterno, attivato direttamente dal "Delegato" al trattamento, la segnalazione potrà pervenire direttamente dal "service provider" stesso. In tal caso, il "Delegato" al trattamento, una volta raccolte dal "service provider"

del servizio interessato tutte le informazioni necessarie, procederà secondo le prescrizioni sopra riportate contenute nelle *"Istruzioni per i trattamenti di dati personali"* approvate con DGR n. 596/2018.

Qualora le violazioni ai dati personali ovvero gli incidenti informatici siano rilevati "direttamente" dalla Direzione ICT e Agenda Digitale nello svolgimento della propria attività istituzionale, la medesima Struttura si occuperà dell'espletamento della procedura sopra descritta.

In estrema sintesi, una volta verificata una violazione dei dati personali i soggetti che potenzialmente devono essere informati sono:

a) l'autorità di controllo *(Garante per la Protezione dei Dati Personali)*
b) i soggetti interessati.

La notifica infatti dipende dalla valutazione del rischio che la violazione comporta per i diritti e le libertà delle persone fisiche (art. 33 del GDPR).

3 L'autorità di controllo dei dati personali

Ai fini del GDPR l'autorità di controllo dei dati personali è:

Nome:	Garante per la protezione dei dati personali
Indirizzo:	Piazza di Monte Citorio n. 121 00186 ROMA
Numero di telefono:	06.696771
Numero di fax:	06.69677.3785
Indirizzo e-mail:	garante@gpdp.it
Indirizzo PEC:	protocollo@pec.gpdp.it

4 Decidere se notificare la violazione all'autorità di controllo dei dati personali

Il GDPR prescrive che una violazione dei dati personali debba essere notificata all'autorità di controllo a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche (Art.33 del GDPR). Ciò richiede che l'Amministrazione valuti il livello di rischio prima di decidere se notificare o meno la violazione dei dati personali.

I fattori da prendere in considerazione nell'ambito della valutazione del rischio dovrebbero includere:

- se i dati personali sono stati crittografati;
- se i dati sono stati crittografati, la robustezza della crittografia impiegata;
- In che misura i dati sono stati pseudonimizzati (cioè se dai dati sia ragionevolmente possibile identificare le persone fisiche a cui essi si riferiscono);
- i dati elementari inclusi, ad es. nome, indirizzo, coordinate bancarie, dati biometrici;
- il volume di dati coinvolti,
- il numero di soggetti interessati;
- la natura della violazione, ad es. furto, distruzione accidentale;
- eventuali altri fattori ritenuti rilevanti.

Le parti coinvolte nella valutazione del rischio possono includere rappresentanti delle seguenti aree, a seconda della natura e delle circostanze della violazione dei dati personali:

- la Direzione ICT e Agenda Digitale;
- il Delegato(i) ai sensi della DGR n. 596/2018;
- il Responsabile della Protezione dei Dati (D.P.O.);
- Area/Aree interessata/e dalla violazione.

Il metodo di valutazione del rischio, il ragionamento alla sua base e le relative conclusioni devono essere documentati e sottoscritti dai rispettivi Delegati, sentita la Direzione ICT e Agenda Digitale. Il risultato della valutazione del rischio deve includere una delle seguenti conclusioni:

1) la violazione dei dati personali non necessita di notifica all'autorità di controllo;
2) la violazione dei dati personali richiede solo la notifica all'autorità di controllo;
3) la violazione dei dati personali richiede la notifica sia all'autorità di controllo, sia agli interessati.

Tali conclusioni possono essere soggette a modifiche in base sia ad ulteriori informazioni scoperte nell'ambito dell'indagine avviata a seguito della violazione subita, che ad eventuali feedback dell'autorità di controllo.

5 Come effettuare la notifica all'autorità di controllo dei dati personali

Nel caso in cui si decida di notificare all'autorità di controllo, il GDPR richiede che ciò avvenga entro 72 ore dall'avvenuta conoscenza (art. 33 del GDPR).
Se sussistono motivi legittimi per non aver fornito la notifica entro i termini richiesti, questi motivi devono essere forniti come parte della notifica.

La notifica deve essere effettuata all'autorità di controllo indicata al paragrafo, utilizzando come modello il *"Modulo per la notifica della violazione dei dati personali ("Data Breach")"*, allegato alle presenti Linee Guida.

La notifica deve contenere le seguenti informazioni:

a) la natura della violazione dei dati personali, compresi, se possibile:
   - le categorie e numero approssimativo di interessati,
   - le categorie ed il numero approssimativo di record di dati personali interessati;
   - il nome ed i recapiti del responsabile della protezione dei dati o altro punto di contatto dove possono essere ottenute ulteriori informazioni;
b) una descrizione delle probabili conseguenze della violazione dei dati personali;
c) una descrizione delle misure adottate o proposte per porre rimedio alla violazione dei dati personali, comprese, se del caso, misure per attenuare i possibili effetti negativi;
d) se la notifica non rientra entro le 72 ore, le motivazioni per le quali non è stata presentata in prima.

6 La comunicazione della violazione dei dati personali all'interessato.

Il GDPR prescrive che una violazione dei dati personali debba essere comunicata all'interessato quando la violazione dei dati personali possa comportare un elevato rischio per i diritti e le libertà delle persone fisiche *(art. 34 del GDPR)*. E' tenere nella dovuta considerazione l'aggiunta del termine *"elevato"*.

La valutazione del rischio descritta in precedenza nelle presenti Linee Giuda determinerà se il rischio per i diritti e le libertà delle persone interessate è da considerarsi come sufficientemente elevato da giustificare la comunicazione a queste ultime.

La comunicazione non è richiesta nei casi previsti dall'art. 34, paragrafo 3, del GDPR, vale a dire se è soddisfatta una delle seguenti condizioni:

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 dell'art. 34 del GDPR);

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.

7 Comunicazione agli interessati

Qualora la violazione dei dati personali richieda la comunicazione alle persone interessate, ciò dovrà avvenire senza ingiustificato ritardo.

La comunicazione alle persone interessate deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali *(art. 34 del GDPR)* e deve comprendere anche:

a) il nome ed recapiti del responsabile della protezione dei dati o altro punto di contatto dove possono essere ottenute ulteriori informazioni;

b) una descrizione delle probabili conseguenze della violazione dei dati personali;

c) una descrizione delle misure adottate o proposte per porre rimedio alla violazione dei dati personali comprese, se del caso, le misure per attenuarne i possibili effetti negativi.