CONSIGLIO REGIONALE DELL'ABRUZZO

PROCEDURA PER LA COMUNICAZIONE DI VIOLAZIONI DEI DATI PERSONALI
REG. 679/2016

Sommario

SCOPO DEL DOCUMENTO

Questo documento contiene informazioni ed istruzioni relative alla comunicazione di violazioni dei dati personali che, ai sensi del Regolamento Europeo per la Protezione dei Dati (GDPR – EU 679/2016) possano comportare rischi per i diritti e le libertà dei cittadini europei i cui dati sono stati violati (gli interessati).

INTRODUZIONE

Per data breach si intende la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati personali trattati dall'organizzazione.

Un data breach, quindi, non è solo un attacco informatico, ma può essere anche un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti contenenti dati personali (furto di un notebook di un dipendente).

La normativa (GDPR) prevede l'obbligo di comunicare alle Autorità di Controllo la violazione dei dati per i fornitori di servizi di comunicazione elettronica accessibili al pubblico, ma **solo se il Titolare ritiene probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati**.
Tutti i Titolari del trattamento sono soggetti alla norma.
La notifica dovrà avvenire entro **72 ore** e comunque "*senza ingiustificato ritardo*".

Se il Titolare ritiene che il **rischio per i diritti e le libertà degli** interessati **sia elevato, allora dovrà provvedere ad informare anche gli interessati**, sempre "senza ingiustificato ritardo".

Non è richiesta la comunicazione all'interessato nei casi indicati dall'art. 34, cioè quando:

- 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/criptazione; anonimizzazione e pseudonimizzazione**;

- 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;

- la **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.

Per valutare i fattori che determinano il rischio per le libertà e i diritti degli interessati, l'organismo consultivo europeo ha fissato i seguenti parametri:

- tipo di "breach": il tipo di violazione è un parametro per la valutazione del rischio;
- natura, numero e grado di sensibilità dei dati personali violati;

- facilità di associare i dati violati ad una persona fisica: può accadere che i dati violati non siano facilmente riconducibili ad una determinata persona fisica;
- gravità delle conseguenze per gli Interessati: quando il Titolare del trattamento percepisce il rischio che i dati oggetto della violazione possono essere utilizzati immediatamente contro gli Interessati (es. sostituzione di persona);
- numero di Interessati esposti al rischio;
- caratteristiche del Titolare del trattamento.

La notifica deve avere il contenuto previsto dall'art. 33 del GDPR:

- 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;
- 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;
- descrivere le probabili conseguenze della violazione dei dati personali;
- 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.

Il Titolare documenta le violazioni di dati personali subite, tramite un apposito **Registro delle Violazioni**, anche se non comunicate alle autorità di controllo, nonché le conseguenze e i provvedimenti adottati.
Tale documentazione dovrà essere fornita all'Autorità di Controllo in caso di accertamenti.

RESPONSABILITÀ

L'organizzazione deve assicurarsi che tutte le violazioni dei dati personali siano segnalate al Titolare del Trattamento, al Responsabile del Trattamento e/o al DPO in modo tempestivo. L'unico caso in cui la segnalazione potrebbe non essere necessaria è quando risultasse improbabile che la violazione dei dati personali possa mettere a rischio i diritti e le libertà degli interessati.

Il Titolare del trattamento e/o il Responsabile del trattamento sono responsabili di assicurare che le risposte siano complete e tempestive.

Tutti gli incaricati al trattamento e i loro responsabili di area/funzione, che trattino dati personali, sono responsabili di assicurare che una violazione dei dati personali sia segnalata al proprio superiore diretto, al Titolare, al Responsabile o al DPO (se nominati) e di fornire il maggior numero di dettagli possibile.

VALUTAZIONE DELLA VIOLAZIONE

Molte volte la tempestività della segnalazione è premiante, nei confronti della accuratezza, se non altro per allertare il più presto possibile gli organi di tutela e gli interessati coinvolti.

Spetta quindi al Titolare del Trattamento, al Responsabile del Trattamento oppure al DPO (se nominati) acquisire le informazioni utili a valutare la violazione, a segnalarla all'Autorità di Controllo e ad attuare tutte le misure necessarie e possibili per proteggere i diritti e le libertà degli interessati e per tutelare l'organizzazione da possibili danni economici e reputazionali.

Per questo l'organizzazione ha predisposto:

- Un elenco di **attività da svolgere** in caso di violazione
- Un **modulo informazioni di dettaglio** che dovranno essere utilizzate per la compilazione della comunicazione formale all'Autorità di Controllo, tramite apposito file pdf disponibile on-line sul sito del Garante.
- Un **Registro delle Violazioni** in cui registrare tutte le violazioni conosciute, anche se lievi.

ATTIVITA' DA SVOLGERE IN CASO DI VIOLAZIONE

Alla scoperta di una possibile violazione dei dati personali dovrebbero essere prese le seguenti azioni:

- Contenimento e recupero
- Valutazione del rischio
- Notifica della violazione all'Autorità di Controllo
- Analisi delle cause e interventi di miglioramento

Contenimento e recupero

- Chi è responsabile di questa attività?
  - L'individuo che ha commesso la violazione o che ha rilevato una possibile violazione, il suo Responsabile aziendale e il Responsabile di area/funzione (se esiste).
- Attività da svolgere
  - La priorità immediata è quella di **contenere la violazione** e limitarne la portata e l'impatto.
  - In caso i dati personali siano stati inviati a qualcuno non autorizzato a trattarli il personale dovrebbe:
    - dire al destinatario di non trasmetterli o discuterli con nessun altro;
    - comunicare al destinatario di distruggere o cancellare i dati personali ricevuti e farsi confermare per iscritto che sia stato fatto;
    - avvisare il destinatario di eventuali implicazioni se divulgasse ulteriormente i dati; e
    - informare gli interessati dei quali sono stati trasmessi dati personali di cosa è successo in modo che possano intraprendere le azioni necessarie per proteggersi.
  - Il Responsabile dell'area/funzione in cui si è verificata la violazione deve essere informato e deve immediatamente segnalarlo al Responsabile del trattamento, al DPO e

al Titolare del trattamento fornendo le seguenti informazioni:

- data e ora della violazione o della rilevazione della violazione;
- chi ha commesso la violazione;
- dettagli della violazione;
- numero di soggetti interessati; e
- dettagli delle azioni già intraprese in relazione al contenimento e al recupero.

Valutazione del rischio

- Chi è responsabile di questa attività?
  - Il Responsabile del trattamento o il DPO oppure il Titolare del trattamento, in ultima istanza.
- Attività da svolgere
  - Il Responsabile del trattamento, il DPO o una persona designata condurrà un'indagine sulla violazione e preparerà un rapporto. Questo rapporto seguirà le linee guida di seguito indicate per la compilazione del modulo per la comunicazione di violazione al Garante e prenderà in considerazione quanto segue:
    - Come si è verificata la violazione.
    - Il tipo di dati personali coinvolti.
    - Il numero di persone interessate dalla violazione.
    - Chi sono le persone interessate.
    - La sensibilità dei dati violati.
    - Quali danni possono arrecare agli interessati; ad esempio, ci sono rischi per la sicurezza fisica, la reputazione o la perdita finanziaria?
    - Cosa potrebbe accadere se i dati personali fossero utilizzati in modo inappropriato o illegale.
    - Per i dati personali che sono stati persi o rubati, se sono presenti misure di protezione come la crittografia, l'anonimizzazione o la pseudonimizzazione.
    - Se esistono rischi reputazionali derivanti dalla perdita di fiducia del pubblico nel servizio offerto dall'organizzazione.

Notifica della violazione all'Autorità di Controllo

- Chi è responsabile di questa attività?
  - Il Responsabile del trattamento o il DPO oppure il Titolare del trattamento, in ultima istanza. La comunicazione dovrà sempre essere inviata a nome del Titolare del trattamento.
- Attività da svolgere
  - Il Responsabile del trattamento o il DPO oppure il Titolare del trattamento, in ultima istanza, supportati dai propri specialisti informatici e legali, determineranno se la violazione debba essere notificata all'Autorità di Controllo, entro 72 ore, oppure possa essere soltanto registrata nel Registro delle Violazioni.
  - La responsabilità della comunicazione formale al Garante spetta al DPO o al Responsabile del trattamento, se nominati, oppure in ultima analisi al Titolare del

trattamento.

Valutazione della violazione e risposta

- Chi è responsabile di questa attività?
  - Il responsabile di area/funzione, coadiuvato dagli specialisti dei sistemi informativi aziendali e dal DPO.
- Azione da intraprendere
  - Una volta risolta la violazione, è necessario prendere in considerazione la causa della violazione. Potrebbe essere necessario aggiornare le politiche e procedure aziendali, condurre una formazione aggiuntiva oppure adottare misure organizzative o tecnologiche addizionali (es. incremento misure di sicurezza fisica o logica).

COMUNICAZIONE DELLA VIOLAZIONE ALL'AUTORITA' DI CONTROLLO

Riportiamo qui di seguito un estratto delle domande a cui occorrerà rispondere per effettuare una comunicazione della violazione all'Autorità di Controllo.
Questo elenco costituisce anche un'utile guida che potrà essere seguita durante le attività descritte precedentemente.
Il modulo specifico da utilizzare dovrà essere scaricato dal sito dell'Autorità di Controllo al seguente indirizzo www.garanteprivacy.it

ALL'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI
La comunicazione deve essere effettuata compilando il modulo disponibile sul sito del Garante, che richiederà obbligatoriamente di fornire tutte informazioni che seguono.

- Denominazione o ragione sociale dell'organizzazione
  - Provincia Comune
  - Cap Indirizzo
  - Nome persona fisica addetta alla comunicazione
  - Cognome persona fisica addetta alla comunicazione
  - Funzione rivestita
  - Indirizzo Email per eventuali comunicazioni
  - Recapito telefonico per eventuali comunicazioni
  - Titolare che effettua la comunicazione (se diverso)
  - Eventuali Contatti (altre informazioni)
- Natura della comunicazione
  - Nuova comunicazione
  - Inserimento ulteriori informazioni su comunicazione precedente
  - Ritiro comunicazione precedente
- Breve descrizione della violazione di dati personali
- Quando si è verificata la violazione di dati personali?
  - Il
  - Tra il e il
  - In un tempo non ancora determinato
  - E' possibile che sia ancora in corso
- Dove è avvenuta la violazione dei dati?
  - Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di dispositivi o di supporti portatili
- Modalità di esposizione al rischio?
  - Tipo di violazione
    - Lettura (presumibilmente i dati non sono stati copiati)
    - Copia (i dati sono ancora presenti sui sistemi del titolare)

        - Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
        - Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
        - Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
        - Altro:
- Dispositivo oggetto della violazione
    - Computer
    - Dispositivo mobile
    - Documento cartaceo
    - File o parte di un file
    - Strumento di backup
    - Rete
    - Altro:
- Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:
- Quante persone sono state colpite dalla violazione di dati personali?
    - N.
    - Circa ____ persone
    - Un numero (ancora) sconosciuto di persone di persone
- Che tipo di dati sono coinvolti nella violazione?
    - Dati anagrafici
    - Numero di telefono (fisso o mobile)
    - Indirizzo di posta elettronica
    - Dati di accesso e di identificazione (user name, password, customer ID, altro)
    - Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
    - Altri dati di personali (sesso, data di nascita, età, ...), dati sensibili e giudiziari
    - Ancora sconosciuto
    - Altro:
- Livello di gravità della violazione dei dati personali (secondo le valutazioni del titolare)?
    - Basso/trascurabile
    - Medio
    - Alto
    - Molto alto
- Misure tecniche e organizzative applicate ai dati colpiti dalla violazione
- La violazione è stata comunicata anche a contraenti (o ad altre persone interessate)?
    - Sì, è stata comunicata il
    - No, perché
- Qual è il contenuto della comunicazione ai contraenti (o alle persone interessate)?
- Quale canale è utilizzato per la comunicazione ai contraenti (o alle altre persone interessate)?
- Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?
- La violazione coinvolge contraenti (o altre persone interessate) che si trovano in altri Paesi UE?
    - Sì
    - No

- La comunicazione è stata effettuata alle competenti autorità di altri Paesi UE?
  - No
  - Sì

RIFERIMENTI

- Per approfondimenti e chiarimenti è possibile consultare il sito del Garante per la Protezione dei Dati Personali all'indirizzo www.garanteprivacy.it.

- Regolamento Europeo per la Protezione dei Dati Personali (GDPR - EU 6792016).

- Guida alla comunicazione di violazione dei dati personali predisposta dal Gruppo di Lavoro delle Autorità di Controllo Europee (Working Party 29):
  - **Guidelines on Personal data breach notification under Regulation 2016/679**
    - WP250rev.01
    - Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018
    - Website: http://ec.europa.eu/justice/data-protection/index_en.htm

- Politica per la Sicurezza Informatica Aziendale.