REGOLAMENTO DATA BREACH

(art.33 e 34 Regolamento UE 2016/679 in materia di Privacy)

Sommario

1. RIFERIMENTI NORMATIVI

- Decreto Legislativo 10 agosto 2018 n, 101 “Disposizioni per l’adeguamento della Normativa Nazionale alle disposizioni del 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)”
- Regolamento (UE) 2016/679 del Parlamento Europeo 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), in particolare gli articoli 33 (Notifica all’Autorità di Controllo), 34 (notifica agli interessati) e 28 (Responsabile del trattamento)
- D.Lgs. 196/2003 Codice per la protezione dei dati personali
- Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679.
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015
- D.Lgs. 82/2005 Codice dell’Amministrazione Digitale (CAD)
- artt. 331 e 361 del Codice di Procedura Penale (obbligo di denuncia da parte del pubblico ufficiale)
- Decreto 9 gennaio 2008 del ministero degli interni in attuazione della Legge 155/2005 sulle infrastrutture critiche
- Decreto del Presidente del Consiglio dei Ministri 1 aprile 2008 “Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività” previste dall'articolo 71, comma 1-bis del decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale».G.U. 21 giugno 2008, n. 144.

2. DEFINIZIONE DATA BREACH

L'art. 33 del GDPR recita che: "In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'art. 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".

Per "Data Breach" si intende un evento in conseguenza del quale si verifica una "violazione dei dati personali". Nello specifico, l'articolo 4 p.12 del GPDR definisce la violazione dei dati personali come 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.

Le Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679 precisano la nozione di violazione come di seguito riportata:

Nel parere 03/2014 sulla notifica delle violazioni, il Gruppo di lavoro ha spiegato che le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni14:

• "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, accesso15 o distruzione accidentali o non autorizzati di dati personali.

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse. Ci si potrebbe chiedere se una perdita temporanea della disponibilità dei dati personali costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica. 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 e 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. Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza" ai sensi dell'articolo 4, punto 12.

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 registrazioni16. 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.

La mancata notifica può comportare ulteriori accertamenti da parte del Garante poiché può rappresentare un indizio di carenze che, se accertate, possono dar luogo a sanzioni. Tutti gli eventi di Data Breach, compresi quelli per cui non sono necessarie le notifiche, devono essere documentati (art. 33 par. 5 del GDPR) su un Registro delle Violazioni.

3. PROCESSO DI NOTIFICAZIONE DATA BREACH

Prima che si verifichi un incidente di sicurezza occorre predisporre le procedure, gli strumenti e l'organizzazione per gestire l'evento fortuito al meglio.

3.1 PIANIFICAZIONE

I Soggetti Competenti devono individuare e predisporre i mezzi tecnologici ed organizzativi per:

- Individuare
- Analizzare
- Rispondere alle potenziali violazioni dei dati anche coinvolgendo i fornitori.

3.2 GESTIONE DELL'EVENTO

In caso di accertamento di violazione che rientra nella definizione di Data Breach, sarà opportuno seguire i seguenti step del processo di notificazione:

1. Acquisizione della notizia da parte dei soggetti preposti al ricevimento/raccolta della violazione che provvederanno ad attivare i passi successivi;
2. Analisi tecnica dell'evento;
3. Contenimento del danno;
4. Valutazione della gravità dell'evento;
5. Notifica al Garante Privacy;
6. Altre segnalazioni dovute;
7. Comunicazione agli interessati, dove necessario;
8. Inserimento dell'evento nel Registro delle Violazioni;
9. Azioni correttive specifiche e per analogia.

4. ACQUISIZIONE DELLA NOTIZIA

La segnalazione di un Data Breach può essere interna o esterna all'Ente.

- INTERNAMENTE:

- Da personale dipendente
- Da personale convenzionato/collaboratori ecc.

- ESTERNAMENTE:

- Da parte degli organi Pubblici (Agid, Polizia, altre Forze dell'Ordine, giornalisti, ecc.)
- Da parte del DPO
- Da parte dei Responsabili esterni del trattamento
- Da parte degli interessati
- Da parte di ulteriori soggetti.

La segnalazione deve essere inoltrata ai soggetti preposti quali Riceventi mediante:

- Posta elettronica;
- Avvertimento verbale/telefonico in ogni caso.

Dal momento in cui i soggetti predetti vengono a conoscenza dell'evento, decorre il termine delle 72 ore previsto dalla normativa per l'invio della notifica all'Autorità di controllo. Tale termine è ridotto a 48 ore nel caso in cui i trattamenti oggetto dell'evento rientrino in quelli previsti dalle misure di sicurezza e modalità di scambio dei dati personali tra Amministrazioni Pubbliche - 2 luglio 2015 (Pubblicato sulla Gazzetta Ufficiale n. 179 del 4 agosto 2015).

5. ANALISI TECNICA DELL'EVENTO

I Riceventi, dopo un'analisi preliminare, attivano il Gruppo di Gestione, sotto la supervisione del Coordinatore del Gruppo Privacy. Il Gruppo che gestisce gli incidenti, è responsabile, sulla base delle rispettive competenze, in base alla tipologia della violazione, dell'analisi tecnica dell'evento, delle azioni da mettere in atto tempestivamente per il contenimento del danno, avvalendosi della collaborazione delle figure preposte.

In particolare, una volta verificato che l'evento segnalato si configuri effettivamente come un "Data Breach" (Analisi Preliminare), verranno svolte tutte le operazioni necessarie a raccogliere gli elementi per una valutazione dell'evento (Analisi Approfondita) ai fini della notifica al Garante della Privacy. È importante sottolineare che, anche nel caso in cui dall'Analisi Preliminare emerga che la segnalazione non ha i caratteri del Data Breach, è necessario registrarla nel Registro delle Violazioni.

Durante l'Analisi Approfondita, dovranno essere accertate le circostanze della violazione, le conseguenze e i relativi rimedi. Si precisa che l'art. 33 paragrafo n. 4 del DGPR recita "Qualora nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo". Pertanto, sarà fondamentale raccogliere il maggior numero di informazioni e, anche in caso queste non siano per il momento ritenute esaustive, effettuare la notificazione.

Nello specifico verrà effettuato, in un tempo consigliabile non superiore a 8 – 10 ore:

- Il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità) o altro evento (cfr Linee Guida sulla notifica delle Violazioni dei dati personali ai sensi del Regolamento UE 2016/79 WP 250 Par. 1. punto 2)
- L'identificazione dei dati violati/distrutti/compromessi e relativi trattamenti;
- L'identificazione degli interessati;
- Il contenimento del danno come di seguito descritto:
    - Limitazione degli effetti dell'incidente,
    - Raccolta delle prove forensi nel caso sia ipotizzato un reato,
    - Determinazione delle azioni possibili di ripristino,

- Valutazione delle eventuali vulnerabilità collegate con l'incidente,
- Individuazione delle azioni di mitigazione delle vulnerabilità individuate,
- Valutazione dei tempi di ripristino,
- Gestione della comunicazione con i Clienti, con CERT e con i media,
- Ripristino dei dati, dei sistemi, dell'infrastruttura e delle configurazioni,
- Verifica dei sistemi recuperati.

Tutte le operazioni effettuate devono essere tracciate e riconducibili a specifiche persone.

6. VALUTAZIONE DELLA GRAVITA' DELL'EVENTO

Il Coordinatore del Gruppo Privacy, con il supporto dei soggetti competenti, dovrà appurare se l'evento merita di essere notificato al Garante della Privacy e con quali modalità (notifica unica o per fasi). Insieme ai soggetti interni di ausilio alla fase di analisi tecnica, si dovrà:

- Informare il RPD;
- Accertare la probabilità o meno che l'evento abbia comportato dei rischi per i diritti e la libertà delle persone (cioè quando si è verificato una distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati, sia che questi dati siano trattati all'interno che all'esterno);
- Effettuare la notifica al Garante, se necessaria;
- Verificare, successivamente, se sia necessaria una seconda notifica più approfondita, di conseguenza ad una analisi tecnica supplementare;
- Effettuare una comunicazione all'Autorità giudiziaria competente, se necessaria.

L'art. 33 paragrafo n. 1 chiarisce che non vi è obbligo di notifica della violazione quando è "improbabile" che questa comporti un rischio per i diritti e le libertà delle persone fisiche, ovviamente il giudizio che determina l'improbabilità del rischio deve essere riportato nel Registro delle Violazioni.

A questo proposito, i Garanti europei nelle loro linee guida, precisano che la mancata comunicazione può essere sanzionata ma che nessuna sanzione è prevista nel caso di comunicazione incompleta o di comunicazione non necessaria. Nella fase di Valutazione, sulla base delle informazioni predisposte in fase di Pianificazione, occorre innanzitutto stabilire se nell'incidente sono coinvolti i dati personali. In caso di risposta positiva occorre valutare l'impatto sugli interessati. Se si tratta di una violazione di riservatezza occorre verificare che le misure di sicurezza (es.: cifratura dei dati) in vigore rendano improbabile l'identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note). In caso di perdita di integrità o disponibilità di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati.

Se in tale modo i rischi per gli interessati sono trascurabili, la procedura può terminare, dopo aver documentato il processo e le scelte operate: le misure messe in atto sono state adeguate alla minaccia. La fase di Miglioramento può essere innescata per incrementare ulteriormente la protezione del dato, ma non è obbligatoria.

Nel caso che i rischi per l'interessato non siano trascurabili occorre procedere come di seguito:

1. Si ha il dovere di notificare al Garante, questo può presentarsi in 3 sottocasi:
    a. il Comune è Titolare del/i trattamenti dei dati coinvolti nell'incidente
    b. il Comune è contitolare del trattamento con delega alla notifica

c. il Comune è Responsabile del trattamento con delega alla notifica.

2. il Comune non ha nemmeno potenzialmente il dovere di notificare all'Autorità Garante: questo quando il Comune agisce come Responsabile del trattamento per conto di altro Titolare, senza delega alla notifica al Garante.

Nella seconda ipotesi il Comune deve comunicare al Titolare la sospetta violazione e/o l'incidente di sicurezza riguardante dati personali al Titolare stesso nei modi convenuti con la massima tempestività e mettersi a disposizione di quest'ultimo per approfondimenti e contenimento dei danni.

Nella prima ipotesi occorre valutare, seguendo le indicazioni dei documenti sopracitati, se il rischio per gli interessati è probabile. In questa fase come prima indicazione occorre assumere come rischio il massimo risultante dall'analisi fatta in fase di Pianificazione. L'analisi del caso specifico deve portare ad una valutazione specifica. L'analisi dei rischi per gli interessati deve dare le giuste priorità agli sforzi di contenimento dell'incidente, nonché fare proseguire la procedura nel caso in cui la soglia sia superata. In ogni caso va condotta la fase di Miglioramento.

Qualora i contorni della compromissione non siano chiari si può attendere fino ad un massimo di 72 ore prima di effettuare una notifica. Alla scadenza delle 72 ore è opportuno fare una comunicazione significando che questa è l'inizio di una notifica in fasi. Si può valutare di fare una notifica cumulativa se una stessa compromissione ha riguardato la stessa tipologia di dati con le stesse modalità.

Per completare la comunicazione, se temporalmente fattibile, occorre individuare:

- Le misure di contenimento adottate
- Il numero anche approssimativo di interessati
- Il periodo di violazione
- Se si ritiene di informare o meno gli interessati e le relative motivazioni
- Le misure di contenimento del danno da suggerire agli interessati
- Il carattere transfrontaliero e la nazionalità degli interessati o meno
- Le azioni di miglioramento intraprese.

7. NOTIFICA AL GARANTE DELLA PRIVACY

Come accennato, la notifica di una violazione al Garante è resa obbligatoria dall'art. 33 del GDPR nei casi in cui si verifichi una violazione dei dati personali, a meno che sia improbabile che tale violazione presenti un rischio per i diritti e le libertà delle persone fisiche. La notifica, effettuata dal Referente Ufficio Privacy, sulla base del Modello reso disponibile dal Garante della privacy (allegato C) dovrà contenere i seguenti elementi:

- La descrizione della violazione dei dati personali compresi, ove possibile le categorie e il numero approssimativo di interessati in questione nonché le categorie ed il numero approssimativo di registrazioni dei dati personali in questione;
- L'indicazione del nome ed i relativi dati di contatto del DPO;
- La descrizione delle probabili conseguenze della violazione;
- L'indicazione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e che, se del caso, per attenuare i possibili effetti negativi;
- Nello specifico, la notifica al Garante sarà effettuata dal Titolare tramite PEC e per

conoscenza al DPO, con indicazione del DPO come punto di contatto con il Garante.

Se l'estensione della compromissione è chiara e non si sono verificati episodi analoghi si deve procedere alla notifica all'Autorità.

I contenuti della notifica sono specificati dal GDPR e dai documenti citati.

8. ALTRE SEGNALAZIONI DOVUTE

Il Referente Ufficio Privacy, con il supporto dei soggetti preposti, dovrà verificare la necessità di informare altri organi quali:

- CERT-PA (in caso di incidenti informatici ai sensi della Circolare Agid n. 2/2017 del 18.04.2017);
- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti);
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche).
- Al Gestore di Identità Digitale e ad Agid nel caso in cui si individui un uso anomalo di un'identità SPID (Sistema Pubblico di Identità Digitale).

9. COMUNICAZIONE AGLI INTERESSATI

In caso di elevato rischio per la libertà e i diritti degli individui, si provvederà ad informare gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio. La comunicazione agli interessati, secondo quanto previsto dal paragrafo n. 3 dell'art. 34 del GDPR, non è richiesta 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;
- 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;
- la comunicazione richiederebbe sforzi sproporzionati.

In tal caso, si procede invece ad una comunicazione pubblica o a una misurazione simile, tramite la quale gli interessati sono informati con analoga efficacia.

La comunicazione deve contenere, ai sensi dell'art. 34, le seguenti informazioni:

- il nome e i dati di contatto del RPD o di altro punto di contatto;
- la descrizione delle 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.

A valle della decisione di notificare l'Autorità Garante, occorre valutare se è il caso di notificare anche gli interessati. A tale scopo va valutata la gravità del rischio per gli interessati e i loro diritti. Se il rischio è grave occorre individuare:

- La fattibilità di contattarli singolarmente oppure la necessità di procedere con pubblicazioni su diversi mezzi di comunicazione (sito web, quotidiani, radio, tv)
- le misure di contenimento che gli stessi interessati possano mettere in atto per minimizzare i

rischi

- Le forme di comunicazione più comprensibili per gli interessati (mezzi, lingue, linguaggio) come indicato nelle Linee guida elaborate dal Gruppo Art. 29 in materia di trasparenza (WP 260), definite in base alle previsioni del Regolamento (UE) 2016/679.

Anche di queste fasi deve essere prodotta e conservata appropriata documentazione.

10. INSERIMENRO DELL'EVENTO NEL REGISTRO DELLE VIOLAZIONI

L'art. 33 paragrafo n. 5 del DGPR, prescrive al Titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma. Pertanto, il Gruppo Ricezione Data Breach è Responsabile dell'inserimento di tutte le attività indicate sopra nel registro delle violazioni, che devono essere documentate, tracciabili, e in grado di fornire evidenza nelle sedi competenti.

Tale procedura deve essere diffusa a tutti i soggetti deputati al trattamento dei dati personali che, a diverso titolo, potranno e dovranno essere di ausilio al Titolare del trattamento.

11. MIGLIORAMENTO

Le azioni previste in questa fase sono:

- Analisi della relazione dettagliata sull'incidente
- Reiterazione del processo di Gestione del rischio informativo
- Eventuale revisione di questo documento (se necessaria) e di eventuali altri documenti collegati (es. Analisi del rischio, Misure di sicurezza)
- Individuazione di controlli che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi
- Revisione del Sistema di Gestione della Privacy
- Revisione delle relazioni con Clienti e Fornitori
- Revisione annuale della procedura.