Gestione Data Breach

PROCEDURA PER DATA BREACH

SCOPO

Il Titolare del trattamento ha nominato un Responsabile del trattamento (DPO), individuato in Pietro Lanzetta.

La presente procedura regolamenta la gestione degli eventi di Data Breach o quelli che vengono, in prima battuta considerati come tali.

DEFINIZIONI

Ai fini della presente procedura, valgono le seguenti definizioni:

a) Titolare del trattamento: "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".

b) Responsabile del trattamento: "La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento ai sensi dell'art. 28 GDPR".

c) Incaricato del trattamento: "La persona fisica che nell'ambito della struttura aziendale del Titolare è autorizzata a effettuare attività di trattamento di dati personali".

d) DPO: "Il Responsabile del trattamento come individuato dalla Sezione 4 (artt. 37-39) del Regolamento (UE) n. 2016/679".

e) Dato personale: "Qualunque informazione relativa a persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, generica, psichica, economica, culturale o sociale".

f) Trattamento: "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

TEAM CRISI

La presente procedura è condivisa con i membri del Team crisi all'atto della loro nomina.

Il team crisi è composto da:

- Segretario comunale
- Responsabili degli uffici e servizi

Il Team informa delle proprie attività il Responsabile per la protezione dei dati nominato, richiedendo allo stesso pareri e supporto secondo quanto previsto dalla presente procedura.

INCIDENTI INFORMATICI, INCIDENTI AGLI ARCHIVI CARTACEI E DATA BREACH

Il GDPR definisce violazione dei dati personali o Data Breach "*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*" (art. 4, n. 12).

Le indicazioni di cui alla presente sezione della Procedura valgono per qualsiasi tipologia di Incidente

(informatico o agli archivi cartacei) da cui possa derivare un Data Breach.

Eventi di Data Breach possono riguardare sia casi cui è connesso un rischio marginale (es. perdita di una chiavetta USB di un dipendente), che casi più critici di furto o perdita di intere basi dati, quali, a titolo esemplificativo, le banche dati gestite o documenti presenti nei suoi archivi.

Nel caso si verificasse una delle casistiche riportate di seguito, o un analogo scenario, è fondamentale chiedersi se e quale tipo di Dati personali sono coinvolti nell'evento, e, di conseguenza, procedere alla segnalazione dell'Incidente:

- ✓ furto o smarrimento di PC, laptop, smartphone, tablet aziendali contenenti Dati personali;
- ✓ furto o smarrimento di documenti cartacei contenenti Dati personali;
- ✓ furto o smarrimento di dispositivi portatili di archiviazione, come chiavette USB e hard disk esterni, contenenti Dati personali;
- ✓ perdita o modifica irreparabile di archivi contenenti Dati personali in formato cartaceo o digitale (ad esempio, a causa di una errata cancellazione o modifica dai sistemi o dagli archivi digitali aziendali che non possa essere ripristinata attraverso l'uso di un backup);
- ✓ diffusione impropria di Dati personali, per mezzo di:
  - o invio di e-mail contenente Dati personali al destinatario errato;
  - o invio di e-mail con un file contenente Dati personali allegato erroneamente;
  - o esportazione fraudolenta o errata di Dati personali dai sistemi aziendali;
- ✓ virus o altri attacchi al sistema informatico o alla rete del Titolare;
- ✓ divulgazione di dati confidenziali a persone non autorizzate;
- ✓ violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- ✓ richiesta di invio di documenti e file contenenti Dati personali da parte di un esterno che si finge fraudolentemente un collega, collaboratore e/o altro soggetto e conseguente invio allo stesso di tali documenti e file;
- ✓ segnalazione da parte di un fornitore di un evento di Data Breach sui propri sistemi che ha interessato o potrebbe potenzialmente interessare Dati personali del Titolare del trattamento.

GESTIONE EVENTO DI DATA BREACH

Ai sensi dell'art. 33 del Regolamento (UE) n. 2016/679, il Titolare del trattamento , in caso sia consapevole di una violazione dei Dati personali trattati, è tenuto:

(i) informare il Garante Privacy entro e non oltre le 72 ore successive all'avvenuta conoscenza della violazione (a meno che non sia improbabile che la violazione dei Dati personali presenti un rischio per i diritti e le libertà degli Interessati);

(ii) nel caso in cui tale violazione sia suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, a informare senza ritardo anche gli stessi Interessati.

A tal fine, – con il presente atto – si dota di una procedura per gli incidenti informatici e agli archivi cartacei che consenta di attivare un apposito processo per la gestione e la notifica di eventuali Data Breach.

Al fine di rendere effettivo il processo di notifica, questa procedura viene resa nota a tutti coloro che nell'ambito del rapporto di lavoro e/o di collaborazione trattano Dati personali del Titolare del trattamento.

Alla gestione di evento di Data Breach è richiesta la massima attenzione e sensibilità da parte di tutte le funzioni coinvolte.

È fatto obbligo a ciascun dipendente e collaboratore di segnalare immediatamente ogni caso di incidente informatico e/o ad archivi cartacei di cui sia venuto a conoscenza e ogni evento che potrebbe potenzialmente condurre ad una violazione di dati personali.

Le segnalazioni di Data Breach dovranno pervenire **esclusivamente** inviando una e-mail al DPO.

Nel caso in cui si renda necessario effettuare la comunicazione di Data Breach in giorni non lavorativi, si chiede cortesemente, dopo aver trasmesso la segnalazione scritta all'indirizzo mail suindicato, di avvisare telefonicamente il dott. Pietro Lanzetta.

1. Processo di gestione dell'Incidente

Al fine di consentire una gestione efficace e tempestiva delle violazioni dei Dati personali, il Titolare del trattamento adotta un processo strutturato per la gestione dei casi di Incidenti che prevede:

- ✓ Rilevazione e segnalazione dell'Incidente;
- ✓ Analisi dell'Incidente;
- ✓ Risposta ed eventuale notifica del Data Breach;
- ✓ Registrazione dell'Incidente.

2. Rilevazione e segnalazione dell'Incidente

La rilevazione e segnalazione dell'Incidente è un obbligo per tutti i dipendenti e/o collaboratori del Titolare del trattamento.

Nel caso in cui si verifichi uno degli eventi sopradescritti o in tutti gli altri casi in cui il soggetto che tratta dati personali sia consapevole di altri eventi potenzialmente rischiosi per i documenti e gli archivi, è tenuto a informare immediatamente l'Ufficio Privacy che provvede – senza indugio – a darne notizia all'Ufficio Sistemi Informativi per gli incidenti informatici e gestendo direttamente gli incidenti occorsi agli archivi cartacei.

3. Analisi dell'Incidente

A seguito della rilevazione e/o segnalazione, il Team crisi effettua una valutazione al fine di verificare che nell'incidente rilevato siano stati effettivamente violati Dati personali trattati dalla Società.

La suddetta analisi è finalizzata alla raccolta ed identificazione delle seguenti informazioni:

- ✓ categorie di Interessati cui i Dati personali violati si riferiscono (ad esempio, utenti, dipendenti, fornitori, etc.);
- ✓ categorie di Dati personali compromessi (ad esempio, Dati personali, Dati particolari, Dati giudiziari);
- ✓ tipologia di incidente: violazione della riservatezza, disponibilità o integrità (ad esempio, accesso non autorizzato, perdita, alterazione, furto, *disclosure*, distruzione, etc.).

Nell'ambito di tale analisi, il Team crisi identifica le azioni di prima risposta da intraprendere nell'immediato

per contenere gli impatti dell'incidente.

Nell'ambito dell'analisi dell'incidente, vengono identificate anche le seguenti informazioni:

- ✓ identificabilità degli Interessati i cui dati rappresentano l'oggetto della violazione;
- ✓ misure di sicurezza tecniche e organizzative che potrebbero aver parzialmente o *in toto* mitigato gli impatti relativi all'incidente;
- ✓ ritardi nella rilevazione dell'incidente;
- ✓ numero di individui interessati.

Sulla base dei suddetti parametri, si procede alla valutazione della gravità dell'incidente relativamente ai diritti ed alle libertà degli Interessati, a seconda della natura dei Dati personali (ad esempio, Dati Sensibili e/o Giudiziari), delle misure di sicurezza adottate, della tipologia di interessati (ad esempio, minori o altri soggetti vulnerabili).

4. Risposta e notifica del Data Breach

La precedente fase di analisi fornisce gli strumenti necessari a identificare e valutare le conseguenze negative e gli impatti causati dall'incidente rilevato.

Nel caso in cui dovesse risultare improbabile che l'incidente presenti rischi per i diritti e le libertà degli interessati, la notifica all'Autorità Garante risulta essere non obbligatoria. Tale valutazione è condivisa con il DPO.

Qualora al contrario dovesse risultare possibile che l'incidente abbia determinato una violazione dei dati che presenti rischi per i diritti e le libertà degli Interessati, l'Ufficio Privacy, con il supporto del DPO, procede a predisporre la notifica all'Autorità Garante secondo il modello allegato al presente atto (ALLEGATO 1).

La notifica viene effettuata all'Autorità Garante entro 72 ore dal momento in cui il Data Breach è stato rilevato.

La suddetta notifica contiene almeno le seguenti informazioni:

- ✓ natura della violazione dei dati personali (*disclosure*, perdita, alterazione, accesso non autorizzato, etc.);
- ✓ tipologie di Dati personali violati;
- ✓ categorie e numero approssimativo di Interessati cui i dati compromessi si riferiscono;
- ✓ nome e dati di contatto del DPO, che sarà l'interfaccia per Titolare del trattamento nei confronti dell'Autorità di controllo;
- ✓ probabili conseguenze della violazione dei Dati personali;
- ✓ descrizione delle misure che il Titolare del trattamento ha adottato o è in procinto di adottare al fine di mitigare le conseguenze del Data Breach;
- ✓ ove la stessa non sia presentata entro 72 ore dalla rilevazione, i motivi dell'eventuale ritardo nella comunicazione.

Qualora non sia stato possibile fornire contestualmente tutte le informazioni obbligatorie, l'Ufficio Privacy - con il supporto dell'Ufficio Sistemi Informativi (relativamente agli incidenti informatici che dovessero verificarsi) e del DPO - raccoglie quanto prima le informazioni supplementari e provvede a integrare, senza

ritardo, la notifica già inoltrata all'Autorità di Controllo.

Oltre a notificare il Data Breach all'Autorità Garante, deve essere valutata l'esigenza di procedere con la denuncia all'Autorità Giudiziaria competente, nonché con la notifica del Data Breach anche ai soggetti interessati i cui dati siano stati violati.

Per stabilire se sia necessario provvedere alla notifica agli Interessati, saranno valutati i seguenti fattori:

- ✓ il trattamento può comportare discriminazioni, furto d'identità, perdite finanziare, disturbi psicologici, pregiudizio alla reputazione, perdita di riservatezza dei Dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo;
- ✓ gli Interessati rischiano di essere privati dei loro diritti, delle libertà o venga loro impedito l'esercizio del controllo sui Dati personali che li riguardano;
- ✓ sono trattati Dati personali che rivelano l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;
- ✓ in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- ✓ sono trattati Dati personali di persone fisiche vulnerabili, in particolare minori;
- ✓ il trattamento riguarda una notevole quantità di Dati personali e un vasto numero di Interessati.

La notifica agli Interessati sarà effettuata nel caso in cui la violazione di Dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, a meno che non sia verificata almeno una delle seguenti condizioni:

- ✓ sono state applicate adeguate misure tecniche e organizzative per proteggere i dati prima della violazione, in particolare quelle in grado di renderle non intelligibili per soggetti terzi non autorizzati (ad esempio, misure di cifratura);
- ✓ a valle della rilevazione del Data Breach, sono state adottate misure per impedire il concretizzarsi dei rischi per i diritti e le libertà degli Interessati;
- ✓ la notifica del Data Breach a tutti gli Interessati singolarmente comporta uno sforzo sproporzionato rispetto al rischio. In tal caso si valuterà comunque l'opportunità di procedere a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati siano comunque informati con analoga efficacia.

L'Ufficio competente, di concerto con il DPO, valuta di volta in volta, sulla base della tipologia e del numero di Interessati, il canale di comunicazione che appare più opportuno per trasmettere la notifica agli stessi.

In ogni caso la notifica agli Interessati deve contenere quanto meno:

- ✓ nome e dati di contatto del DPO;
- ✓ descrizione delle probabili conseguenze della violazione;
- ✓ descrizione delle misure adottate o che la Società intende adottare per porre rimedio alla violazione e ridurre gli effetti negativi.

Data Breach relativo a dati personali trattati in qualità di Responsabile del trattamento

Qualora, a seguito di una segnalazione o nel corso dell'analisi preliminare di cui al precedente paragrafo 4, l'Ufficio Privacy rilevasse che la violazione qualificabile come Data Breach riguardasse dati personali di titolarità di un soggetto terzo trattati dall'Ente in qualità di Responsabile del trattamento, procede a informare senza ingiustificato ritardo il soggetto terzo titolare del trattamento.

Nel dettaglio, la comunicazione al soggetto titolare del trattamento dovrà contenere quanto meno le seguenti informazioni (oltre a quelle eventualmente richieste dallo stesso soggetto terzo titolare del trattamento):

- ✓ Descrizione della natura della violazione dei dati personali comprensiva, ove possibile, di informazioni in merito alle categorie e al numero di Interessati nonché alle categorie e al volume approssimativo di dati personali oggetto di violazione;
- ✓ Nome e dati di contatto del DPO ;
- ✓ Descrizione delle possibili conseguenze della violazione;
- ✓ Descrizione di eventuali misure già adottate o di cui si prevede l'adozione per porre rimedio alla violazione di dati personali e per attenuarne i possibili effetti negativi.

La comunicazione sarà inviata al soggetto titolare del trattamento entro 48 ore dall'avvenuta rilevazione della violazione o nel minore termine eventualmente indicato dal soggetto titolare del trattamento.

Prescrizioni per la prevenzione di Data Breach

Si adottano specifiche strategie per prevenire o minimizzare il verificarsi di Data Breach.

In primo luogo, occorre che tutti i soggetti nominati quali autorizzati al Trattamento siano consapevoli dei Dati personali che trattano attraverso i propri strumenti (anche cartacei) e dispositivi o a cui hanno accesso tramite i sistemi del Titolare del trattamento.

A tal fine, la presente procedura viene loro comunicata ed essi dovranno custodire tali Dati personali ed i relativi documenti con cura e in modo responsabile sia all'interno che all'esterno della propria area di lavoro.

Si precisa che i soggetti in questione sono già stati istruiti per mezzo di specifici atti di designazione e devono attenersi alle prescrizioni all'uopo impartite.