PROCEDURA
“DATA BREACH MANAGEMENT”

- INDICE -

ALLEGATI

- Modulo di segnalazione di un potenziale data breach - DOC. 1

Clausola di riservatezza

Prima di procedere con la lettura del presente documento, il destinatario concorda che non comunicherà o utilizzerà le informazioni contenute qui di seguito per scopi diversi dalla valutazione del documento stesso e che esso non verrà distribuito in alcun modo a meno che non sia diversamente concordato con EKLETTA S.rl.

1. PREMESSA E SCOPO

Il presente documento definisce il processo adottato da EKLETTA Srl per la gestione degli eventi di "data breach" con impatto sui dati personali trattati, in conformità con il *General Data Protection Regulation* (Regolamento UE 2016/679, di seguito "GDPR").
La presente procedura fornisce le azioni da attuare nell'eventualità in cui si presentino eventi negativi in grado di determinare un rischio alle libertà e ai diritti delle persone fisiche.
Il presente documento rappresenta un comportamento proattivo **tale da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento** UE 2016/679.

Per "data breach" si intende una violazione, accidentale o dolosa, della sicurezza che comporta la distruzione, perdita, alterazione, diffusione non autorizzata, o l'accesso illecito, di dati personali trasmessi, memorizzati o altrimenti trattati.
La violazione dei dati personali può distinguersi in tre categorie:
-"*confidentiality breach*": in caso di divulgazione o accesso non autorizzato o accidentale a dati personali;
-"*availability breach*": in caso di alterazione non autorizzata o accidentale dei dati personali;
-" *Integrity breach*": in caso di modifica non autorizzata o accidentale di dati personali.

2. OGGETTO E AMBITO

La presente procedura si pone l'obiettivo di minimizzare l'impatto di eventi potenzialmente dannosi per i diritti e le libertà fondamentali delle persone fisiche interessate dai trattamenti svolti da EKLETTA Srl definendo i requisiti ed i criteri per garantire una tempestiva identificazione degli eventi di "data breach", indirizzare le azioni correttive e determinare la necessità e la modalità di notifica di tali eventi all'Autorità Garante ed ai soggetti interessati.
La presente procedura si applica nel caso in cui vi sia violazione del dato personale di qualsiasi interessato che risieda negli Stati Membri dell'Unione Europea (UE) e nelle nazioni membri dello Spazio Economico Europeo (SEE).

Inoltre, l'oggetto del presente documento s'individua nel dato personale trattato all'interno dell'Azienda, indipendentemente dal Paese di residenza dell'Interessato al quale il dato violato si riferisce.

3. DOCUMENTAZIONE DI RIFERIMENTO

- "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 (General Data Protection Regulation, di seguito GDPR)";
- "Guidelines on Personal data breach notification under Regulation 2016/679", - Article 29 Data Protection Working Party, WP250 adottate il 3 Ottobre 2017;
- Codice Privacy (D.Lgs. 196 del 2003 come novellato dal D.Lgs. 101 del 2018);
- FAQ pubblicate dal Garante per la Protezione dei Dati Personali (Garante Privacy);
- Guidelines 01/2021 on Examples regarding Data Breach Notification Adopted on 14 January 2021 Version 1.0, European Data Protection Board (EDPB);
- Provvedimento del Garante per la Protezione dei Dati Personali del 27 maggio 2021 - Procedura telematica per la notifica di violazioni di dati personali (data breach), Registro dei provvedimenti n. 209 del 27 maggio 2021.

4. DEFINIZIONI

Le seguenti definizioni sono tratte dall'articolo 4 del Regolamento Generale sulla Protezione dei Dati dell'Unione europea (o GDPR):

"**Dato Personale**": qualsiasi informazione riguardante una persona fisica identificata o identificabile («Interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento 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, genetica, psichica, economica, culturale o sociale;

"**Dato relativo alla Salute**": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rilevano informazioni relative al suo stato di salute;

"**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.

"**Responsabile del trattamento**": una persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.

"**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.

"**Violazione dei Dati Personali**": 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.

"**Autorità di Controllo**": l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR dell'UE;

"**Autorizzato per designazione":** persona fisica che opera sotto l'autorità del Titolare del Trattamento, espressamente designata dallo stesso alla quale vengono attribuiti specifici compiti e funzioni connessi al trattamento dei dati personali. La seguente definizione è tratta dall'Art. 2quaterdecies del D. Lgs. 196/2003 come novellato dal D.Lgs. 101/2018.

5. GOVERNANCE E TEAM DATA BREACH PER LA VERIFICA DELLA VIOLAZIONE DEI DATI

Di seguito sono riportati i ruoli e le responsabilità dei soggetti coinvolti nel processo di gestione dei "data breach".

Il Team privacy per la verifica della violazione dei dati (di seguito "TEAM DATA BREACH" è costituito da persone esperte e competenti con le figure apicali della società:

- Referente privacy interno;
- Società nominata Amministratore di sistema;
- Data Protection Officer (DPO).

Il **referente privacy interno quando** viene a conoscenza di potenziali eventi di "data breach" convoca il team privacy al fine di procedere alla valutazione degli impatti sui diritti e le libertà dei soggetti interessati dell'evento negativo segnalato e determina, di concerto con il **Titolare del trattamento**, la necessità di notificare tale incidente all'Autorità Garante ed ai soggetti interessati.

Se necessario il Team potrà avvalersi di esperti esterni quali ad esempio del consulente per i progetti IT quale esperto in materia si sicurezza delle informazioni al fine di fornire supporto al team privacy nell'analisi di

dettaglio degli eventi di "data breach", nell'individuazione della causa scatenante dell'evento e nell'analisi dei possibili impatti per i diritti e le libertà dei soggetti interessati.

5.1 ACQUISIZIONE DELLA NOTIZIA

Chiunque ossia dipendente, collaboratore o terzo che lavora ovvero agisce per conto di EKLETTA Srl appena è notiziato di una presunta ovvero effettiva violazione dei dati personali deve comunicarla al referente privacy interno.

Ogni soggetto che lavora o agisce per conto di EKLETTA Srl è tenuto a comunicare al referente privacy interno la notizia di una presunta o effettiva violazione dei dati personali mediante la compilazione del "modulo di segnalazione di un potenziale data breach" allegato al presente documento (DOC. 1).

6. TASSONOMIA DEGLI EVENTI DI DATA BREACH

Una violazione può essere considerata come un evento inaspettato che potrebbe compromettere la confidenzialità, la disponibilità o l'integrità dei dati:

- *violazione della confidenzialità* in caso di diffusione o accesso non autorizzato al dato personale;
- *perdita di disponibilità* in caso di alterazione non autorizzata o accidentale del dato personale;
- *violazione dell'integrità* in caso di perdita permanente, indisponibilità estesa o distruzione del dato personale.

Una violazione può interessare una o più delle tipologie sopra indicate (ad esempio potrebbe verificarsi allo stesso tempo una violazione di confidenzialità e una violazione dell'integrità).
Nella seguente tabella è sintetizzata una tassonomia degli eventi di "data breach":

Evento	*Descrizione*	*Principio di sicurezza violato*
Distruzione o cancellazione dei dati personali	Indisponibilità irreversibile o di lunga durata dei dati personali gestiti Tale violazione potrebbe essere causata da un'eliminazione non autorizzata sul database logico (es. cancellazione di dati) o dalla distruzione fisica (es. rottura hardware) a cui si aggiunge l'impossibilità di recuperare l'informazione.	Disponibilità
Indisponibilità dei dati personali	L'indisponibilità irreversibile o temporanea dei mezzi e degli strumenti necessari per effettuare il trattamento dei dati da parte degli interessati o della società Titolare del trattamento per l'erogazione di servizi richiesti o per conto dell'interessato. L'indisponibilità non implica necessariamente la distruzione dei dati personali.	Disponibilità
Perdita o furto di dati personali	Perdita del controllo sugli asset di storage fisico, come la privazione, sottrazione, perdita degli strumenti, o documenti cartacei. La perdita di un supporto fisico di memorizzazione dei dati non implica che si sia verificata anche un'altra violazione quale distruzione, alterazione, diffusione o accesso non autorizzato. Una violazione può non sussistere dove è possibile escludere con ragionevole sicurezza il verificarsi di accessi non autorizzati al dato e se la perdita dello storage fisico non comporta una perdita permanente del dato personale.	Disponibilità Confidenzialità
Alterazione o modifiche non autorizzate ai dati personali	Alterazione, o modifica, del dato non autorizzata o inappropriata, né rilevata né corretta da processi interni, che causa trattamenti non corretti o diffusione del dato personale.	Integrità

	Un'alterazione impropria può occorrere nelle ordinarie operazioni di trattamento svolte da personale autorizzato o in caso di modifica fraudolenta eseguita da soggetti non autorizzati.	
Diffusione di dati personali	Diffusione non autorizzata o accidentale di dati personali a terze parti indefinite (persone fisiche o legali, gruppi, pubblico). Una violazione può non sussistere dove è possibile escludere con ragionevole sicurezza il verificarsi di accessi non autorizzati al dato e se la perdita dello storage fisico non comporta una perdita permanente del dato personale.	Confidenzialità
Accesso non autorizzato o illecito ai dati	Accesso alle informazioni personali trattate da parte di soggetti non autorizzati.	Confidenzialità

6.1 ESEMPI DI DATA BREACH

A titolo esemplificativo e non esaustivo, si riportano alcuni eventi capaci di causare una violazione di dati personali:

- aggirare i controlli di sicurezza di un sistema informatico per avere accesso ai dati personali senza autorizzazione;
- la perdita di un dispositivo di memorizzazione elettronica (ad es. CD, DVD, laptop, hard disk, tablet) contenente dati personali non crittografati;
- e-mail di phishing aperte o utilizzate da un dipendente che hanno generato una perdita o un accesso non autorizzato ai dati personali o che hanno permesso l'installazione di un malware che sottrae dati personali;
- e-mail contenente dati personali inviata involontariamente al mittente sbagliato;
- difetti di protezione dei software che possono aver provocato un accesso non autorizzato ai sistemi o ai dati personali;
- la modifica o cancellazione impropria di dati personali.

7. PROCESSO DI GESTIONE DI DATA BREACH

Il processo di gestione degli eventi rilevati che configurano un "data breach" è strutturato secondo le seguenti fasi:

- Analisi e classificazione dell'evento;
- Valutazione degli impatti;
- Notifica dell'evento di "data breach";
- Tracciamento dell'evento di "data breach".

7.1 ANALISI E CLASSIFICAZIONE DELL'EVENTO

L'**Amministratore di sistema** deve raccogliere le informazioni necessarie all'analisi del "data breach".
In particolare, in fase di analisi devono essere raccolte almeno le seguenti informazioni:

- data e ora di rilevazione dell'evento;
- modalità di rilevazione dell'evento;
- dove si è verificato il "data breach";
- tipologia di evento, secondo la tassonomia sopra riportata;
- asset, archivi e sistemi IT coinvolti;
- natura e volume dei dati coinvolti;
- categoria e volume di soggetti cui si riferiscono i dati;
- contromisure adottate per contenere l'impatto della violazione.

Anche nel caso in cui le analisi accertino che l'evento in oggetto non costituisca una violazione di dati personali, è necessario il tracciamento delle analisi svolte e delle motivazioni che hanno portato a non classificare l'evento come "data breach".

È importante sottolineare che, anche nel caso in cui dall'analisi preliminare dell'evento emerga che la segnalazione non ha i caratteri del Data Breach, è necessario comunque annotarla Registro delle Violazioni in possesso dell'Amministratore di sistema.

7.2 VALUTAZIONE DEGLI IMPATTI

Il **titolare del trattamento**, in coordinamento con il team Data Breach, valuta i possibili impatti della violazione occorsa sui soggetti interessati, con particolare riferimento ai relativi diritti e libertà, tenendo in considerazione i seguenti aspetti:

- tipo di violazione;
- natura e sensibilità dei dati personali violati;
- volume dei dati personali violati ed estensione geografica dell'evento;
- facilità di identificazione dei soggetti a cui si riferiscono i dati;
- gravità delle conseguenze per i soggetti a cui si riferiscono i dati violati;
- eventuali contromisure da implementare o già implementate per ridurre l'impatto della violazione.

Tale valutazione avviene sulla base delle informazioni raccolte in fase di analisi e si svolge nelle seguenti fasi necessarie per il calcolo della *severity* complessiva di un evento di "data breach":

a) valutazione della natura dei dati violati;
b) valutazione del livello di identificabilità dell'interessato;
c) valutazione delle circostanze della violazione.

a) La **valutazione della natura dei dati violati**, secondo le metriche definite nella seguente tabella:

Natura dati violati	Impatto
Dati biometrici: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.	**Alto**
Dati sensibili e relativi alla salute: dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.	**Alto**
Dati Giudiziari: dati relativi a casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reato e relativi carichi pendenti, o che rivelino la qualità di imputato o di indagato.	**Alto**
Dati di localizzazione: dati che consentono la rilevazione dell'ubicazione sul territorio o in determinate aree geografiche in un determinato intervallo temporale.	**Alto**
Dati di profilazione: dati che consentono la valutazione determinati aspetti personali relativi a una persona fisica e, in particolare, di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di una persona fisica.	**Medio Alto**
Dati finanziari: dati personali identificativi associati ad una valorizzazione economico/patrimoniale (importo transazione, saldo rapporto, ...)	**Medio**
Registrazioni audio video: Dati relativi a registrazioni audio e video (es. videosorveglianza, telefonate, …)	**Medio**
Dati personali comuni: qualsiasi informazione riguardante una persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento 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, genetica, psichica, economica, culturale o sociale (nome, cognome, domicilio, residenza, CF, Partita Iva, …)	**Medio**
Dati personali provenienti da fonti pubbliche: dati personali provenienti da pubblici archivi o resi manifesti dall'interessato.	**Medio basso**
Dati non personali: dati che non consentono l'identificazione diretta o indiretta di una persona fisica.	**Basso**

b) Il **livello di identificabilità dell'interessato** stima quanto può essere agevole, per chi entra in possesso dei dati violati, associarli inequivocabilmente a determinati interessati. La tabella da tenere in considerazione è la seguente:

Livello di identificabilità	Impatto
Certo: dati che consentono di identificare direttamente e univocamente un soggetto interessato anche se decontestualizzati.	**alto**
Altamente probabile: dati che, con alta probabilità, sono sufficienti ad identificare univocamente un soggetto interessato	**Medio alto**
Improbabile: dati che, se decontestualizzati, non consentono di identificare univocamente un soggetto interessato.	**Medio**
Impossibile: dati che non consentono né direttamente né indirettamente l'identificazione di un soggetto interessato.	**Medio basso**

c) Le **circostanze della violazione** sono valutate coerentemente con la tassonomia degli eventi di "data breach" definita nei capitoli precedenti.

Circostanze della violazione	Impatto
Grave perdita di riservatezza, integrità o disponibilità, dovuta ad eventi accidentali o dolosi	**alto**
Rilevante perdita di riservatezza, integrità o disponibilità dovuta a eventi accidentali o dolosi	**medio**
Minima perdita di integrità o disponibilità dovuta a eventi accidentali	**basso**

Tenuto conto delle tabelle sopra esposte, sarà valutata la *severity* complessiva dell'evento di "data breach" come "molto alta", "alta", "media" o "bassa".

7.3 COMUNICAZIONI

Qualora venga accertato un Data Breach con severity "molto alta", "alta" o "bassa" ovvero venga ravvisato un potenziale evento di tale portata, riguardante i trattamenti di Dati personali per i quali il Titolare del trattamento è Responsabile del Trattamento dati, se ne dovrà dare conoscenza per iscritto al rispettivo Titolare del trattamento mediante i canali di comunicazione da questi indicati nel relativo DPA, senza giustificato ritardo e, comunque, non oltre 24 (ventiquattro) ore dal momento dell'avvenuta conoscenza dell'evento predetto.

7.4 NOTIFICA DI VIOLAZIONE ALL'AUTORITÀ GARANTE

Il Titolare del trattamento è tenuto a notificare la violazione al Garante per la protezione dei dati personali entro 72 ore dal momento in cui il titolare ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio sui diritti e le libertà delle persone fisiche.
Il **Titolare del trattamento**, provvede a notificare le violazioni con *severity* molto alta, alta o media all'Autorità Garante, a meno che:

- sia improbabile che l'evento di "data breach" presenti un rischio per i diritti e le libertà delle persone fisiche;
- le misure di sicurezza adottate consentano di attenuare efficacemente eventuali rischi.

La notifica deve essere effettuata entro e non oltre 72 ore dal momento in cui la violazione è stata rilevata o segnalata e deve specificare almeno:

- la descrizione della natura della violazione dei dati personali, delle categorie e il numero approssimativo di interessati in questione nonché le categorie dei dati personali;

- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure già implementate o di cui si propone l'adozione da parte del titolare per porre rimedio o ridurre l'impatto della violazione dei dati personali.

7.5 COME INVIARE LA NOTIFICA AL GARANTE?

A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ (VEDI: Provvedimento del 27 maggio 2021).

Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante.

Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha ideato e messo disposizione un apposito strumento di autovalutazione consultabile sul sito del garante al seguente indirizzo: https://servizi.gpdp.it/databreach/s/self-assessment che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

7.6 COMUNICAZIONE DELLE VIOLAZIONI AI SOGGETTI INTERESSATI

Gli eventi di "data breach" con *severity* "alta" o "molto alta" devono essere altresì notificati ai soggetti interessati, a meno che i dati oggetto di violazione fossero cifrati o non intellegibili o i provvedimenti adottati dalla Società per porre rimedio alla violazione consentissero di mitigare efficacemente i possibili rischi per i diritti e le libertà degli interessati.
Con rischio elevato per i diritti e le libertà degli interessati si intendono i casi in cui la violazione dei dati personali può causare un danno materiale o immateriale per gli individui.
Qualora sia necessario comunicare l'evento agli interessati, il Titolare del trattamento predispone la documentazione necessaria, in particolare:

- la descrizione della natura della violazione, della tipologia, del numero di soggetti coinvolti e, laddove possibile, della numerosità dei dati personali coinvolti;
- la descrizione delle probabili conseguenze della violazione dei dati;
- la descrizione delle misure già implementate o di cui si propone l'adozione da parte del titolare per porre rimedio o ridurre l'impatto della violazione dei dati personali.

Tale comunicazione deve avvenire tempestivamente tramite il canale più adeguato, definito in funzione dei risultati della fase di valutazione, e può includere:

- comunicazione individuale tramite i recapiti forniti;
- comunicazione pubblica sul sito web istituzionale che informi sulle misure di sicurezza implementate dalla società o che debbano essere intraprese dagli interessati, aggiornamenti sullo stato della violazione, FAQ e strumenti per valutare se i propri dati sono stati oggetto di violazione;
- assistenza tramite call center o live chat sul sito istituzionale;
- comunicati stampa.

8. RESPONSABILITÀ

Qualsiasi individuo violi questa Procedura è soggetto a misure disciplinari interne (che possono arrivare alla risoluzione del rapporto di lavoro); inoltre, qualora le sue azioni violino la legge, potrebbe incorrere in responsabilità civile o penale.

9. VALIDITÀ E GESTIONE

Il presente documento è valido dal 3 marzo 2022.

Il monitoraggio della presente procedura è previsto con frequenza almeno annuale al fine di controllare e, se necessario, aggiornare il presente documento.

Fanno parte integrante della presente procedura i seguenti documenti

- Modulo di segnalazione di un potenziale data breach - DOC. 1