

Procedura in caso di Violazione dei dati (Data Breach)

(ai sensi dell'art. 33 e 34 Regolamento UE 679/2016)

TITOLARE DEL TRATTAMENTO:	STUDIO LEGALE ENRICO SBAFFI
Sede Legale:	Via Rinaldoni 16 – 60030 Serra de' Conti (AN)
Il sede	Via Sanzio 369/6 – 60019 Senigallia AN
P. Iva:	02545100428
Telefono / Fax:	333-5222092 / 0731/879170
Email / Pec:	info@enricosbaffi.com / enrico.sbaffi@legalmail.it

Procedura DATA BREACH	PROCEDURA DI RISPOSTA E COMUNICAZIONE AD UNA VIOLAZIONE DI DATI (DATA BREACH)
Scopo	La Procedura fornisce principi generali e un modello di approccio per rispondere, e mitigare, alla violazioni di dati personali subite (Data Breach) in una o in entrambe le seguenti situazioni: • Il dato personale identifica gli interessati che risiedono negli Stati Membri dell'Unione Europea (UE) e nelle nazioni all'interno dello Spazio Economico Europeo (SEE), indipendentemente da dove tali dati siano soggetti al trattamento a livello globale; • I dati personali sono soggetti a trattamento all'interno dell'UE e/o del SEE, indipendentemente dal paese di residenza dell'interessato. La Procedura definisce i principi e le azioni generali per gestire con successo la risposta a una violazione di dati ed adempiere agli obblighi relativi alla notifica alle Autorità di Controllo e ai singoli individui, come richiesto dal GDPR dell'UE.
Chi deve applicarla	Tutti i Dipendenti, Personale, Collaboratori e Terzi, anche a tempo determinato, che lavorano o agiscono per conto del Titolare del Trattamento, devono essere a conoscenza e seguire la presente Procedura in caso di violazione dei dati personali (Data Breach).
Responsabilità	Titolare: distribuire la procedura e sovrintendere le operazioni di gestione della violazione dei dati subita (Data Breach). DPO/RPD (se previsto): sensibilizzare il personale al tema della sicurezza, aiutare nella gestione del Data Breach e gestire gli eventuali contatti con l'Autorità di Controllo.
Riferimenti normativi	D.lgs. 196/2003 Codice in materia di protezione dei dati personali GDPR - Regolamento (UE) 2016/679 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) D.lgs 101/2018 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio Politica sulla Protezione dei Dati Personali
Termini e definizioni	«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

Procedura in caso di Violazione dei dati (Data Breach)

(ai sensi dell'art. 33 e 34 Regolamento UE 679/2016)

	«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; «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»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento; «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 Regolamento.
Background	Il Regolamento attribuisce alla notifica di Data Breach una funzione essenziale di tutela degli interessati ed estende tale obbligo alla generalità dei titolari di trattamento rispetto alle precedenti normative. Il criterio per valutare la necessità di avviare una procedura di notifica è la probabilità che la violazione possa porre a rischio (per la notifica all'Autorità di Controllo) o essere ad elevato rischio (per la comunicazione agli interessati), le libertà e i diritti degli individui a cui i dati personali appartengono. Appurato il rischio conseguente dalla violazione, gli artt. 33 e 34 del GDPR indicano ai Titolari del trattamento i termini, le modalità, i contenuti e le deroghe della notifica e comunicazione di Data Breach.
Modalità operative	Processo di Risposta alle Violazione dei Dati Il Processo di Risposta alle Violazione dei Dati viene avviato quando qualcuno si accorge che una sospetta / presunta o effettiva violazione dei dati personali, si è verificata all'interno dell'organizzazione e la comunica al Titolare, o, se predisposto, a qualsiasi membro del Gruppo di Risposta alle Violazioni dei Dati. Il Titolare del trattamento, o il Gruppo di Risposta, è responsabile di determinare se la violazione debba essere considerata una violazione dei dati personali o meno. Il Titolare del trattamento, o il Gruppo di Risposta, ha la responsabilità di documentare ogni decisione in merito alla violazione. Poiché questi documenti potrebbero essere esaminati dalla Autorità di Controllo, devono essere scritti in modo molto preciso e accurato per garantire la tracciabilità e la responsabilizzazione. Notifica di violazione dei dati personali: comportamento del Responsabile del trattamento nei confronti del Titolare del trattamento Qualora la violazione dei dati personali, o la sospetta violazione dei dati, riguardassero i dati personali che vengono elaborati per conto di terzi, il Responsabile del trattamento

Procedura in caso di Violazione dei dati (Data Breach)

(ai sensi dell'art. 33 e 34 Regolamento UE 679/2016)

deve segnalare qualsiasi violazione subita, al rispettivo Titolare del trattamento dei dati senza indebito ritardo.

Il Responsabile del trattamento invierà una notifica al Titolare del trattamento che includerà quanto segue:

- *Una descrizione della natura della violazione*
- *Le categorie dei dati personali in questione*
- *Il numero approssimativo degli interessati coinvolti*
- *Se previsto, il nome e le informazioni di contatto del Responsabile del Gruppo di Risposta alle Violazioni dei Dati / Responsabile della Protezione dei Dati*
- *Le conseguenze della violazione dei dati personali*
- *Le misure adottate per gestire la violazione dei dati personali*
- *Qualsiasi informazione relativa alla violazione dei dati*

Il Titolare del trattamento, o il RPD/DPO, registrerà la violazione dei dati (Data Breach) nel proprio **"REGISTRO DELLE VIOLAZIONI DEI DATI"**, avendo cura di compilarlo con la massima attenzione e corrispondenza ai fatti accaduti.

Notifica di violazione dei dati personali: comportamento del Titolare del trattamento nei confronti dell'Autorità di Controllo

Qualora la violazione dei dati personali, o sospetta violazione dei dati, riguardasse i dati personali trattati dall'organizzazione come Titolare del trattamento, si dovrà procedere con le seguenti azioni:

- 1) L'organizzazione deve stabilire se la violazione dei dati personali debba essere segnalata all'Autorità di Controllo, in base alla probabilità che la violazione subita possa porre a rischio le libertà e i diritti degli individui interessati a cui i dati personali appartengono.
- 2) Al fine di determinare il rischio per i diritti e le libertà dell'interessato in questione, il Titolare del trattamento deve eseguire una Valutazione d'Impatto sull'attività di trattamento interessata dalla violazione dei dati.
- 3) Se è improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà degli interessati, non è richiesta alcuna notifica. Tuttavia, la violazione dei dati dovrà essere comunque registrata nell'apposito registro.
- 4) Qualora questa violazione dei dati personali sia suscettibile di presentare un rischio per i diritti e le libertà degli interessati colpiti dalla violazione dei dati personali, l'Autorità di Controllo deve essere informata senza indebito ritardo, e comunque non oltre le 72 ore (oltre tale termine, la notifica di violazione deve essere corredata con le ragioni giustificative del ritardo).

Il Titolare invierà una Notifica all'Autorità di Controllo che includerà quanto segue:

- *Una descrizione della natura della violazione*
- *Le categorie dei dati personali in questione*
- *Il numero approssimativo degli interessati*
- *Se previsto, il nome e le informazioni di contatto del Responsabile del Gruppo di Risposta alle Violazioni dei Dati / Responsabile della Protezione dei Dati*
- *Le conseguenze della violazione dei dati personali*
- *Le misure adottate per gestire la violazione dei dati personali*
- *Qualsiasi informazione relativa alla violazione dei dati*

Procedura in caso di Violazione dei dati (Data Breach)

(ai sensi dell'art. 33 e 34 Regolamento UE 679/2016)

	Comunicazione di violazione dei dati personali: comportamento del Titolare del trattamento nei confronti dell'Interessato Il Titolare del trattamento deve valutare se la violazione dei dati personali può comportare un rischio elevato per i diritti e le libertà dell'interessato. In caso affermativo, il Titolare del trattamento, o, se previsto, il Responsabile della Protezione dei Dati dell'organizzazione, deve informare gli interessati senza indebito ritardo. La comunicazione agli interessati deve essere scritta in un linguaggio chiaro e semplice e deve contenere le stesse informazioni elencate nella presente procedura > Sezione Modalità Operative > Paragrafo <i>"Comportamento del Titolare del trattamento nei confronti dell'Autorità di Controllo"</i>. Se, a causa del numero di interessati, risulta <u>sproporzionatamente</u> difficile informare tutti i soggetti in questione, il Titolare del trattamento deve adottare le misure necessarie per garantire che le persone interessate siano informate utilizzando canali di massa appropriati e pubblicamente disponibili.		
Controlli e verifiche	Devono essere previsti i seguenti controlli periodici: 1) Personale formato e informato sulle procedure di Data Breach 2) Contenuti pubblicati sul sito web istituzionale / social network 3) Audit sulle password per verificarne la solidità, le procedure di gestione e la durata		
Allegati (modulistica)	• Registro delle Violazioni dei dati subite (Data Breach)		
Gestione delle Revisioni	MODELLO - 11_Procedura di DataBreach - REV 2018.05.16.docx Rev 29-08-2024		
Richieste	<table><tr><td>TITOLARE DEL TRATTAMENTO: Sede Legale: Il sede P. Iva: Telefono / Fax: Email / Pec:</td><td>STUDIO LEGALE ENRICO SBAFFI Via Rinaldoni 16 – 60030 Serra de' Conti (AN) Via Sanzio 369/6 – 60019 Senigallia AN 02545100428 333-5222092 / 0731/879170 info@enricosbaffi.com / enrico.sbaffi@legalmail.it</td></tr></table>	TITOLARE DEL TRATTAMENTO: Sede Legale: Il sede P. Iva: Telefono / Fax: Email / Pec:	STUDIO LEGALE ENRICO SBAFFI Via Rinaldoni 16 – 60030 Serra de' Conti (AN) Via Sanzio 369/6 – 60019 Senigallia AN 02545100428 333-5222092 / 0731/879170 info@enricosbaffi.com / enrico.sbaffi@legalmail.it
TITOLARE DEL TRATTAMENTO: Sede Legale: Il sede P. Iva: Telefono / Fax: Email / Pec:	STUDIO LEGALE ENRICO SBAFFI Via Rinaldoni 16 – 60030 Serra de' Conti (AN) Via Sanzio 369/6 – 60019 Senigallia AN 02545100428 333-5222092 / 0731/879170 info@enricosbaffi.com / enrico.sbaffi@legalmail.it		