PO 01 – PROCEDURA DATA BREACH

Il Titolare del Trattamento		**Data**	**Firma**

REV	**Data**	**Oggetto della Revisione**
1	**27/09/2018**	**Elaborazione Registro segnalazioni**

1. Premessa

Una violazione dei dati personali (c.d. data breach) può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

2. Scopo del documento e ambito di applicazione

Il presente documento si prefigge lo scopo di indicare le opportune modalità di gestione del data breach, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016.

In questo documento si sintetizzano le regole per garantire il rispetto dei principi esposti e la realizzabilità tecnica e la sostenibilità organizzativa, nella gestione del data breach, sotto i diversi aspetti relativi a:

- modalità e profili di segnalazione al Titolare
- modalità e profili di segnalazione all'Autorità Garante
- valutazione dell'evento accaduto
- eventuale comunicazione agli interessati

3. 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 (art. 4, punto 1).
"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 (art. 4, punto 2).
"Archivio": qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, punto 6).
"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 (art. 4, punto 7)..
"Data Protection Officer": la persona fisica o giuridica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39).
"Autorizzato al trattamento": la persona fisica, espressamente designata, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali (art. 4, punto 10).
"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 (art. 4, punto 8).
"***Violazione dei dati personali (c.d. 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, punto 12)

4. Normativa e documenti di riferimentoDatore di lavoro

- Regolamento UE 679/2016, considerando n. 85, 86, 87, 88 artt. 33, 34
- Guidelines on Personal data breach notification under Regulation 2016/679 – article 29 data protection working party (Adopted on 3 October 2017 – as last Revised and Adopted on 6 February 2018)

5. Gestione del data breach interno alla struttura

5.1 Modalità e profili di notifica all'Autorità Garante Privacy

Ogni operatore autorizzato a trattare dati, qualora venga a conoscenza di un potenziale caso di data breach, avvisa tempestivamente il titolare del trattamento. Quest'ultimo, valutato l'evento, se confermate le valutazioni di potenziale data breach, utilizzando il modulo allegato (All. 1), ed eventualmente avvalendosi del DPO per eventuali funzioni consulenziali, predispone l'eventuale comunicazione all'Autorità Garante, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali. Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo. È comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi).

Successivamente la violazione sarà riportata nel Registro delle Violazioni.

6. Gestione del data breach esterno alla struttura

6.1 Premesse

Ogniqualvolta il titolare del trattamento si trovi ad affidare il trattamento di dati ad un soggetto terzo/responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di data breach sia inclusa nel suddetto contratto. Ciò al fine di obbligare il responsabile ad informare il titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di data breach[1].

Ad ogni responsabile del trattamento deve essere comunicato il contatto del titolare del trattamento.

6.2 Modalità e profili di notifica all'Autorità Garante Privacy

Ogni responsabile del trattamento, qualora venga a conoscenza di un potenziale data breach che riguardi dati di cui l'Ente sia titolare, ne dà avviso senza ingiustificato ritardo al titolare del trattamento. Per "ingiustificato ritardo" si considera la notizia pervenuta al titolare al più tardi entro 12 ore dalla presa di conoscenza iniziale da parte del responsabile. Il titolare del trattamento effettua una valutazione dell'evento avvalendosi del DPO per eventuali funzioni consulenziali. Pertanto, sulla scorta delle determinazioni raggiunte, il titolare del trattamento predispone l'eventuale comunicazione all'Autorità Garante,, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali. Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo. È comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi). La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del referente privacy.

Successivamente la violazione sarà riportata nel Registro delle Violazioni.

7. Modalità di comunicazione agli interessati

[1] NB: Rimane salva la possibilità che sia il responsabile del trattamento ad effettuare una notifica per conto del titolare del trattamento, se il titolare del trattamento ha rilasciato specifica autorizzazione al responsabile, all'interno del suddetto contratto. Tale notifica deve essere fatta in conformità con gli articoli 33 e 34 del GDPR. La responsabilità legale della notifica rimane in capo al titolare del trattamento. In questa procedura si esamina solamente il caso d'uso ordinario in cui la notifica venga effettuata dal titolare del trattamento.

Nel caso in cui dal data breach possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione. Il titolare del trattamento, o suo delegato, predispone l'eventuale comunicazione all'interessato/agli interessati, a firma del titolare, da inviarsi nei tempi e nei modi che lo stesso, anche attraverso la funzione consulenziale del DPO, individuerà come più opportuna come specificato nell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.

8. Schema di valutazione scenari – data breach

Un data breach non è solo un attacco informatico, ma può consistere anche in un accesso abusivo, un incidente (es. un incendio o una calamità naturale), nella semplice perdita di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno), nella sottrazione di documenti con dati personali (es. furto di un notebook di un dipendente).

La comunicazione involontaria di documenti, o in generale di dati, che non abbiano vero senso compiuto/riconducibilità verso l'interessato non è considerato data breach, ma è considerato un normale errore procedurale.

9. Registro delle violazioni

Il titolare del trattamento, o suo delegato, cura l'aggiornamento del registro delle violazioni, ai sensi dell'art. 33, comma 5 del GDPR, e come definito nella presente procedura.