AREUS
Azienda Regionale
Emergenza Urgenza
Sardegna

REGIONE AUTONOMA DELLA SARDEGNA

Procedura per la gestione di *Data Breach* ai sensi del Regolamento UE 2016/679

Sommario

1. Premessa

Con il termine *data breach*, il Regolamento UE 2016/679, definisce una "violazione della 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, memorizzati o comunque trattati. Lo stesso Regolamento ha introdotto l'obbligo, in capo al Titolare, di notificare all'Autorità di Controllo la violazione dei dati personali, 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 libertà delle persone fisiche cui i dati violati si riferiscono.

La notifica deve essere effettuata all'Autorità di controllo competente per l'esercizio dei compiti e dei poteri assegnatele sul territorio del proprio Stato membro, per l'Italia il Garante per la Protezione dei dati personali.

Il Titolare ha inoltre l'obbligo di comunicare la violazione senza ingiustificato ritardo anche agli interessati, nel caso in cui la suddetta violazione presenti rischi per i diritti e le libertà delle persone fisiche, in modo da consentir loro di attivarsi a tutela dei propri interessi.

Già il Gruppo di lavoro "Articolo 29" (WP29), sostituito dal 25/05/2018 con l'entrata in vigore del Regolamento UE 2016/679 dal Comitato europeo per la protezione dei dati (EDPB), spiegava come i Data Breaches possano essere categorizzati sulla base dei parametri di Sicurezza delle Informazioni compromessi. Pertanto, è possibile distinguere tra:

- "violazione della confidenzialità" - in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;

- "violazione della disponibilità" - in caso di perdita accidentale o non autorizzata di accesso o distruzione di dati personali;
- "violazione dell'integrità" - in caso di alterazione non autorizzata o accidentale dei dati personali.

In virtù di quanto sopra indicato, anche la temporanea perdita di disponibilità dei dati, se implica un impatto per i diritti e le libertà degli Interessati, è da ritenersi una violazione dei dati.

Le conseguenze potenziali di una violazione di dati sono molteplici e possono avere diversi effetti nei confronti dei soggetti colpiti. La violazione, infatti, se non affrontata in modo adeguato e tempestivo, può implicare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano, 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 ad Areus 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 princìpi e alle disposizioni contenute nel Regolamento UE 2016/679 (General Data Protection Regulation o GDPR).

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, par. 1, n. 1 del GDPR).

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, par. 1, n. 2 del GDPR).

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, par. 1, n. 6 del GDPR).

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, par. 1, n. 7 del GDPR). In questo contesto il Titolare del trattamento è AREUS, nella figura del proprio legale rappresentante *pro tempore*

Data Protection Officer: la persona fisica/giuridica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39 del GDPR).

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. 2-quaterdecies del D. Lgs. n. 196/2003).

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, par. 1, n.c8 del GDPR).

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, par. 1, n. 12 del GDPR).

4. Normativa e documenti di riferimento

- *Regolamento UE 2016/679, 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).*
- *Guidelines 01/2021 on Examples regarding Data Breach Notification.*
- *Provvedimento del Garante per la Protezione dei Dati Personali del 27 maggio 2021, doc. web n. 9667201.*

5. Gestione del *data breach* interno alla struttura

5.1 Premesse

È necessario che l'Ente dia notizia a tutti i soggetti autorizzati al trattamento in merito alla presente procedura mediante idonea delibera e circolare.

Il Titolare del Trattamento si serve della consulenza del Data Protection Officer, al fine di valutare l'entità del Data Breach e le misure tecniche ed organizzative da predisporre.

5.2 Gruppo di valutazione data breach

Ai fini della gestione tempestiva di qualsiasi violazione di dati personali, è istituito un Gruppo di Valutazione della Data Breach composto dalle seguenti funzioni:

- Data Protection Officer

- Referente aziendale Privacy

- Referente per le Centrali Operative 118

- Responsabile dell'area Sistemi Informativi Reti Tecnologiche

- Responsabile dell'area presso cui è avvenuto il Data Breach.

Il Comitato di valutazione della Data Breach è convocato con urgenza dal Referente aziendale Privacy delegato, nel caso in cui si verifichi un incidente di sicurezza che possa determinare una Data Breach.

Il Gruppo di Valutazione dovrà riunirsi, anche mediante teleconferenza o videoconferenza, entro 24 ore dalla convocazione, salvo, motivate, situazioni eccezionali per attivare tutte le necessarie azioni, raccogliere le informazioni e valutare se notificare la Data Breach al Garante e, se del caso, agli interessati.

Le attività di raccolta documentale ed informativa sono coordinate dal Referente Aziendale Privacy.

Le valutazioni effettuate dovranno essere comunicate tempestivamente al Titolare del trattamento per consentire di procedere all'eventuale notifica all'Autorità di Controllo e/o agli interessati nei termini di legge.

5.3 Modalità e profili di notifica al Garante Per la Protezione dei Dati Personali

Ogni soggetto autorizzato al trattamento di dati personali, qualora venga a conoscenza di un potenziale caso di *data breach,* avvisa tempestivamente il Titolare del Trattamento.

Questi *effettua una valutazione dell'evento avvalendosi della consulenza del Data* Protection Officer.

Ai fini di una corretta classificazione dell'episodio, sarà utilizzato lo schema di scenario di *data breach*, allegato alla presente procedura.

Pertanto, sulla scorta delle determinazioni raggiunte, sarà predisposta l'eventuale notifica all'Autorità Garante per la Protezione dei Dati Personali, a firma del legale rappresentante del Titolare del Trattamento, 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 al Garante per la Protezione dei Dati Personali 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 Titolare del Trattamento.

Il modulo da utilizzare per la notifica al Garante per la Protezione dei Dati Personali dell'avvenuta violazione dei dati è disponibile al seguente link: https://servizi.gpdp.it/databreach/s/ .

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, in qualità di Responsabile del trattamento, è tenuto 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 è necessario al fine di obbligare il Responsabile ad informare il titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di *data breach*.

Ad ogni Responsabile del trattamento devono essere comunicati i contatti del Titolare del Trattamento, a cui inviare la notizia di *data breach*.

7. Modalità di comunicazione agli interessati

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 predispone l'eventuale comunicazione all'interessato/agli interessati, 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 dal Garante per la Protezione dei Dati Personali.

8. Schema di valutazione scenari – *data breach*

Di seguito sono illustrati alcuni esempi, non esaustivi, di possibili violazioni di dati personali, allo scopo di supportare i soggetti coinvolti nella procedura, nella valutazione in merito alla necessità di effettuare o meno la notifica di *data breach* al Garante per la Protezione dei Dati Personali.

Tipo di Breach	Definizione	Estensione minima / Soglia di segnalazione	Esempi	Controesempi
Distruzione	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, né di altri. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.	Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	• Guasto non riparabile dell'hard disk contenente uno o più referti che, in violazione al regolamento, erano salvati localmente • Incendio di archivio cartaceo delle.	• Rottura di una chiavetta USB che non contiene dati personali originali (in unica copia) • Rottura di un PC che non contiene dati personali originali (in unica copia) • Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura nell'apposito applicativo
Perdita	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili Dati relativi a più soggetti, relativi a interi episodi o relativi a tipologie di dato la cui indisponibilità lede i diritti fondamenta li dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla perdita possa ledere i diritti fondamentali dell'interessato Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	• Smarrimento di chiavetta USB contenente dati originali • Smarrimento di fascicolo cartaceo personale dipendente	• Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa

Divulgazione non Autorizzata	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento del l'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Consegna di dati personali ad altra struttura senza autorizzazione • Divulgazione su web di dati personali da parte di soggetti terzi	• Attacco informatico che porta all'esfiltrazione di dati personali e divulgazione su web. • Infezione virale di un PC con un malware che dalla scheda tecnica non trasmette dati su internet. • Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.

Perdita	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili Dati relativi a più soggetti, relativi a interi episodi o relativi a tipologie di dato la cui indisponibilità lede i diritti fondamenta li dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla perdita possa ledere i diritti fondamenta li dell'interessato Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	• Smarrimento di chiavetta USB contenente dati originali • Smarrimento di fascicolo cartaceo personale dipendente	• Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa
Divulgazione non Autorizzata	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento del l'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Consegna di dati personali ad altra struttura senza autorizzazione • Divulgazione su web di dati personali da parte di soggetti terzi	• Attacco informatico che porta all'esfiltrazione di dati personali e divulgazione su web. • Infezione virale di un PC con un malware che dalla scheda tecnica non trasmette dati su internet. • Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.

Tipo di Breach	Definizione	Estensione minima / Soglia di segnalazione	Esempi	Controesempi
Accesso non Autorizzato	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche incaricati dal titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti del l'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi • Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema informatico.	• Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi. • Accesso non autorizzata di un documento non ancora validato dal proprio autore.
Indisponibilità temporanea del dato	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'interessato.	Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale	• Infezione da ransomware che comporta la temporanea perdita di disponibilità dei dati e questi non possono essere ripristinati dal backup • cancellazione accidentale dei dati da parte di una persona non autorizzata • perdita della chiave di decrittografia di dati crittografati in modo sicuro	• Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso

Tipo di Breach	Definizione	Estensione minima / Soglia di segnalazione	Esempi	Controesempi
Modifica	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.	Caratteristiche: • Modifiche sistematiche su più casi Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Guasto tecnico che altera parte dei contenuti di un sistema, compromettendo anche i backup • Azione involontaria, o fraudolente, di un utente che porta alla alterazione di dati personali in modo non tracciato e irreversibile	• Guasto tecnico che altera parte dei contenuti di un sistema informatico, rilevato e sanato tramite operazioni di recovery • Azione involontaria di un utente che porta alla alterazione di dati tracciata e reversibile • Modifica di un documento non ancora validato dal proprio autore.

Un *data breach*, quindi, 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).

I casi di *data breach* per le casistiche già descritte si estendono ai documenti cartacei o su supporti analogici.

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.

Questo poiché:

- chi riceve non può sapere a quale interessato è riferito il testo;
- l'interessato non è danneggiato poiché nessuno riferimento alla sua persona è stato diffuso.

9. Registro delle violazioni

Il Titolare del Trattamento, avvalendosi dei soggetti autorizzati al trattamento, degli eventuali Responsabili del Trattamento e della consulenza del DPO, cura l'aggiornamento del registro delle violazioni, ai sensi dell'art. 33, paragrafo 5 del GDPR.