ARAG

Tutela legale.
Vivi pienamente.

helvetia
La tua Assicurazione svizzera

# IL DATA BREACH: COME PROTEGGERSI E COME GESTIRNE AL MEGLIO LE CONSEGUENZE

Con il termine Data Breach si intende fare riferimento ad una qualsiasi violazione alla sicurezza informatica che comporta l'accesso, la perdita, la modifica o la divulgazione non autorizzata di dati personali o il furto di questi. In sostanza, è una violazione alla riservatezza, all'integrità e anche alla disponibilità di tali dati.

# INDICE

# COME PROTEGGERSI

**1.** Il primo passo è quello di dotarsi di una policy di sicurezza aziendale e di portarla a conoscenza di tutti i dipendenti, collaboratori ed ausiliari, che dovranno essere adeguatamente formati sul contenuto della stessa e sui comportamenti da seguire per evitare imprevisti e danni accidentali.

**2.** Non di rado, infatti, le violazioni hanno origine interna all'azienda e sono conseguenza di un errore umano dovuto a scarsa consapevolezza e formazione sul tema (recenti studi hanno calcolato in una percentuale del 23 % i data breach direttamente riconducibili ad errore umano).

**3.** Detta policy poi dovrà anche costituire oggetto di attento e costante monitoraggio e verificate anche a mezzo di simulazioni di incidenti cyber. Ciò consentirà, infatti, di poter concretamente verificare che le norme ivi stabilite rimangano efficaci nel tempo, anche alla luce dell'evoluzione del progresso tecnologico, e che siano effettivamente osservate e rispettate da coloro che sono chiamati ad applicarle.

**4.** Si devono sempre tenere sotto controllo dei file di ingresso al sistema (log) per rilevare tempestivamente ogni attività o intrusione sospetta.

**5.** La rete e il perimetro aziendale devono invece essere protetti grazie a soluzioni come antivirus, firewall e antimalware.

**6.** I dispositivi personali (c.d. end-point) vanno monitorati e messi in sicurezza, in quanto costituiscono un facile punto di aggressione i malintenzionati.

**7.** Occorre avere sempre a disposizione una copia aggiornata dei dati utilizzati e ricorrere regolarmente a sistemi di backup e recupero dei dati, capaci, in presenza di evento informatico avverso, di ristabilire in tempi ragionevolmente contenuti l'operatività aziendale di base.

**8.** Parimenti importante sarà l'effettuazione di test periodici di verifica del protocollo adottato per garantire che le procedure seguite dall'Azienda per prevenire e risolvere casi di data breach siano efficienti e condotte da personale formato adeguatamente per implementare il protocollo.

**9.** È fortemente consigliabile dotarsi di un'adeguata garanzia assicurativa per proteggersi dalle conseguenze patrimoniali negative di un episodio di violazione di dati. L'assicurazione, infatti, risarcisce i costi che l'Azienda deve sostenere per riparare le conseguenze della violazione e deve anche coprire le eventuali spese legali che l'Azienda dovrà affrontare.

# GESTIONE DELL'EVENTO

In caso di data breach, generalmente i passi da seguire sono:

**1.** Acquisire la notizia, segnalarla a chi di competenza in modo da poter attivare la procedura dedicata;

**2.** procedere ad un'analisi tecnica dell'evento: una volta verificato che l'evento segnalato si configuri effettivamente come un "Data Breach", sarà opportuno svolgere tutte le operazioni necessarie a raccogliere gli elementi per una valutazione dell'evento, anche ai fini della notifica al Garante della Privacy.

**a)** Anche nel caso in cui dall'Analisi Preliminare emerga che la segnalazione non ha i caratteri del Data Breach, è necessario registrarla nel Registro delle Violazioni.

**b)** Dovrà poi essere effettuato, in un tempo consigliabile non superiore a 8 – 10 ore, il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità) o altro evento;

**3.** identificare i dati violati/distrutti/compromessi e relativi trattamenti;

**4.** individuare gli interessati;

**5**. contenere e limitare il danno;

**6.** raccogliere delle evidenze forensi nel caso appaia configurabile una fattispecie di reato;

**7.** determinare delle azioni possibili di ripristino;

**8.** valutare eventuali vulnerabilità collegate con l'incidente;

**9.** individuare delle azioni di mitigazione delle vulnerabilità individuate;

**10.** valutare i tempi di ripristino;

**11.** gestire la comunicazione con i Clienti e con i media;

**12.** ripristinare dati, sistemi, infrastruttura e configurazioni;

**13.** verificare i sistemi recuperati;

**14**. in caso di evento di origine dolosa, presentare una denuncia all'Autorità Giudiziaria competente;

**15.** valutare la necessità di procedere alla notifica al Garante Privacy (al modello denominato "Notifica di Data Breach al Garante della Privacy" presente nell'Archivio Documenti di ARAG SE Italia, accessibile dall'area clienti del sito www.arag.it)

**16.** valutare la necessità di procedere ad una comunicazione nei confronti dell'interessato, nei termini di cui al prospetto riportato in calce;

**17.** verificare, successivamente, a seguito del progresso dell'istruttoria, se sia necessaria una seconda, più approfondita e dettagliata, notifica;

**18.** inserire l'evento nel Registro delle Violazioni, in ossequio all'art. 33 paragrafo n. 5 del GDPR, anche al fine di

Il tracciamento dei casi di violazione dei dati personali viene effettuato allo scopo di:

- individuare e tenere sotto controllo i fattori di rischio, ossia i fattori che determinano con più frequenza una violazione dei dati personali;
- misurare l'efficacia delle policy e delle procedure adottate;
- elaborare un piano di conformità che fissi gli obiettivi da raggiungere per essere "compliant" rispetto a leggi, best practices, e che aiuti a dimostrare la conformità in sede di audit di verifica/ispezioni/test;
- conservare materiale probatorio della violazione, nel caso occorresse ricorrevi per difendersi nell'ambito di un'eventuale azione giudiziaria.

consentire all'Autorità di controllo di verificare il rispetto della norma.

Poiché, come visto, al Titolare del trattamento viene riconosciuta la più ampia discrezionalità sui criteri con i quali compiere la valutazione relativa al rischio che la violazione può avere sui diritti e alle libertà degli interessati, si ritiene utile accennare a taluni indicatori elaborati dell'Enisa - l'agenzia europea per la sicurezza delle informazioni - che potranno

**Rischio Basso**
Gli individui possono sperimentare piccoli inconvenienti superabili senza alcun problema (ad esempio: tempo occorrente per inserire nuovamente le informazioni, fastidio, irritazione ecc.).

**Rischio Medio**
Gli individui possono incontrare inconvenienti significativi superabili con alcune difficoltà (ad esempio: costi supplementari, indisponibilità di accedere a servizi, paura, mancanza di comprensione, stress, disturbi fisici minori ecc.).

**Rischio Alto**
Gli individui possono incontrare conseguenze significative superabili con gravi difficoltà (ad esempio: appropriazione indebita di fondi, inserimento in black list, danni alla proprietà, perdita del lavoro, chiamata in giudizio, peggioramento dello stato di salute ecc.).

**Rischio Elevato**
Gli individui possono incontrare conseguenze significative o irreversibili, che potrebbero non essere in grado di superare (ad esempio: incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte ecc.).

essere presi a riferimento per la stima della severità del rischio connesso ad uno specifico episodio di data breach.
Si tenga comunque presente che sul sito dell'Autorità Garante per la Protezione dei Dati Personali (www.gpdp.it) è a disposizione di ciascun titolare del trattamento di dati personali, un utile strumento che consente di individuare le

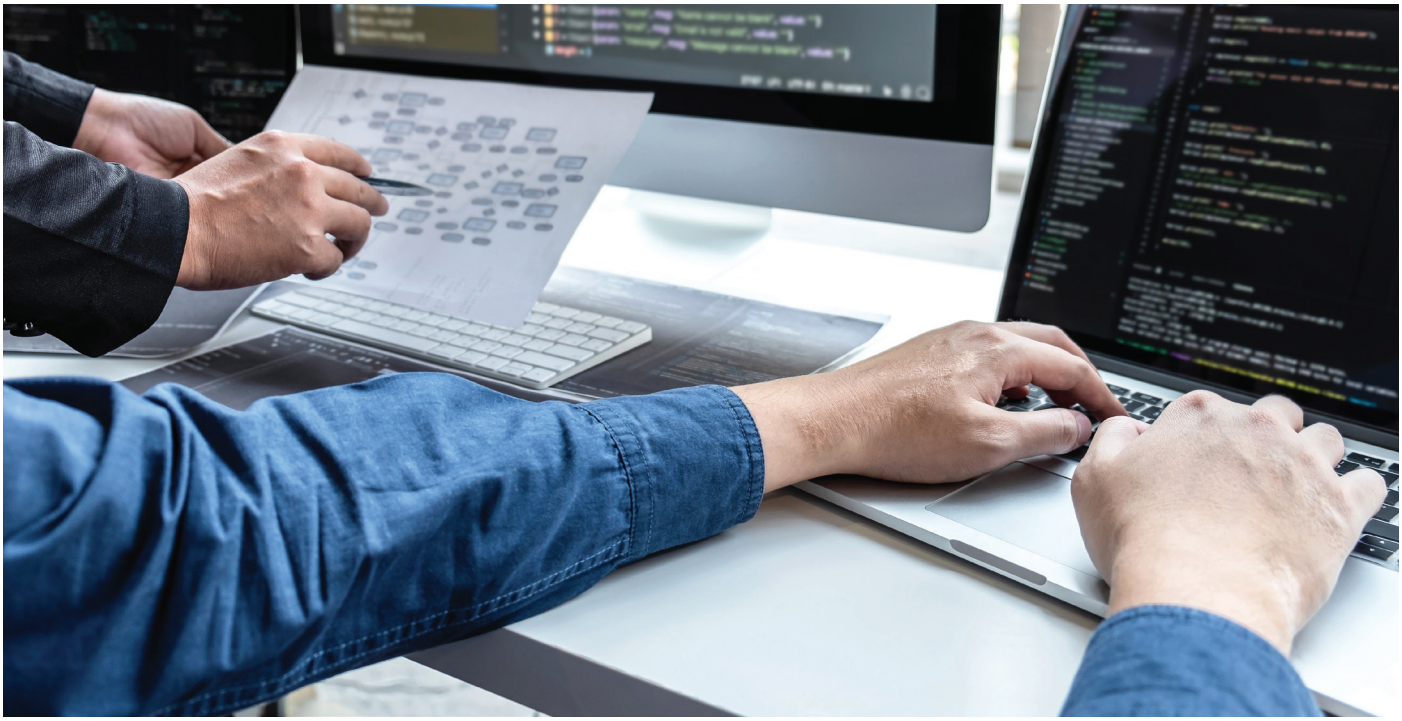
## COMUNICAZIONE AGLI INTERESSATI

azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.
In caso di **elevato rischio per la liberta e i diritti degli individui**, si deve provvedere ad informare gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio.

La **comunicazione agli interessati**, secondo quanto previsto dal paragrafo n. 3 dell'art. 34 del GDPR, **non e richiesta quando**:

- il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le liberta degli interessati di cui al paragrafo 1. In tale contesto assumono rilievo le misure di contenimento che gli stessi interessati possano mettere in atto per minimizzare i rischi;
- la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. Dovranno essere utilizzate le forme di comunicazione più comprensibili per gli interessati (mezzi, lingue, linguaggio) come indicato nelle Linee guida elaborate dal Gruppo Art. 29 in materia di trasparenza (WP 260), definite in base alle previsioni del Regolamento (UE) 2016/679.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità Garante può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che non ve ne sia bisogno in quanto una delle condizioni richieste dalla normativa sia da ritenere soddisfatta.



# ESEMPIO DI COMUNICAZIONE ALL'INTERESSATO

Si riporta, a mero titolo esemplificativo e non esaustivo, una possibile traccia di comunicazione di una violazione agli interessati.
Si consiglia, comunque, di consultare sempre un legale specializzato in materia per la predisposizione di una comunicazione da trasmettere agli interessati che tenga conto delle peculiarità del singolo data breach e dei profili di delicatezza al medesimo collegati.

MITTENTE
[Nome e indirizzo del mittente]

DESTINATARIO
Gent.ma Sig.ra/Egr. Sig.
[Nome e indirizzo dell'interessato]

Siamo venuti a conoscenza che una violazione dei nostri sistemi informatici ha comportato l'acquisizione di parte dei Suoi dati personali da parte di soggetti esterni a ciò non autorizzati.

In ossequio al regolamento europeo UE 2016/679 (General Data Protection Regulation) tale violazione è stata prontamente notificata al Garante Privacy.

Abbiamo incaricato esperti di sicurezza informatica ed esperti legali per ridurre ulteriormente l'esposizione dei Suoi dati a tale accesso non autorizzato ai nostri sistemi.

Cosa è accaduto:
- [elencare in modo oggettivo la cronologia degli eventi]

Sono stati coinvolti i seguenti dati personali:
- [elencare i tipi di dati personali oggetto del data breach. Ad esempio, Nome, Cognome, ecc.]

Cosa significa questo per Lei:
Considerando la natura della violazione e i tipi di dati personali coinvolti, riteniamo che le conseguenze per lei siano:
- [elencare le azioni che l'interessato dovrà approntare]

Come eviteremo in futuro tale problematica
Al fine di evitare che tale violazione si verifichi nuovamente e di ridurre al minimo l'impatto sui nostri clienti abbiamo attivato le seguenti iniziative:
- [elencare le azioni intraprese per garantire che questa violazione non venga ripetuta]

Scusandoci per il contrattempo, Le assicuriamo che stiamo facendo tutto ciò che è in nostro potere per contenere gli effetti dell'inconveniente occorso.

Per ulteriori informazioni si prega di contattare [.....]

Cordiali Saluti.
[.....]