Le immagini sono generate attraverso l'utilizzo dell'Intelligenza Artificiale.

Data Breach: come gestire una violazione di dati personali

Riconoscere gli errori per tutelare la sicurezza

Care/i Colleghe/i,

Nella presente Newsletter, analizziamo il tema del **Data Breach,** così come descritto ai sensi dell'art. 4, n. 12 del GDPR. È fondamentale sapere **come gestire un incidente di sicurezza**, non solo per gli obblighi in capo al Titolare del trattamento, ma soprattutto **per evitare conseguenze ai danni del nostro Ente e dei dati personali dei soggetti interessati**.

Il **Data Breach** è una violazione di sicurezza che si verifica quando i dati personali, riservati o protetti, vengono esposti, sottratti, modificati o distrutti senza autorizzazione. Questo può avvenire **accidentalmente**, a causa di errori umani o vulnerabilità nei sistemi, oppure in **modo illecito**, a seguito di attacchi informatici da parte di hacker o insider malintenzionati. Questo tipo di incidente può compromettere la **riservatezza**, l'**integrità** o la **disponibilità** dei dati personali, esponendo gli interessati a rischi significativi. Di seguito si espone cosa accade quando viene compromesso almeno uno dei **tre principi fondamentali** della sicurezza delle informazioni:

1. **Violazione della riservatezza**: **i dati vengono resi accessibili a persone non autorizzate**, mettendo a rischio dati personali o informazioni strategiche riservate.
2. **Violazione dell'integrità**: **le informazioni vengono alterate o modificate senza autorizzazione**, compromettendo la loro affidabilità e accuratezza.
3. **Violazione della disponibilità**: **i dati o i sistemi che li gestiscono diventano inaccessibili** agli utenti legittimi, causando interruzioni nei servizi e potenziali danni operativi.

Il **Data Breach** può avere conseguenze gravi, tra cui **danni reputazionali**, **sanzioni pecuniarie significative e controversie legali**. È quindi fondamentale **adottare misure di prevenzione** e risposte rapide per proteggere le informazioni e minimizzare i rischi.

I comportamenti interni scorretti: tra le cause più comuni di Data Breach

Le **cause di un Data Breach** possono essere **molteplici** e **dipendono da diversi fattori**, tra cui elementi umani, tecnologici e organizzativi. La violazione dei dati può avvenire sia a causa di attacchi esterni che per errori o negligenze interne. Sebbene si tenda a pensare che un Data Breach sia spesso il risultato di un'azione esterna, come un attacco hacker, un malware o il furto di dispositivi contenenti dati sensibili, **nella maggior parte dei casi la violazione è riconducibile a comportamenti interni** all'Ente.

Le principali **cause interne** che comportano una violazione di sicurezza sono:

Errori umani accidentali: comportamenti tipici possono essere, **l'invio di dati riservati al destinatario sbagliato**, la **pubblicazione** accidentale di **informazioni riservate** su piattaforme pubbliche o interne, il **deposito di file in luoghi non sicuri e/o non protetti**, come servizi di cloud non autorizzati o **dispositivi USB**, la **condivisione di link a documenti riservati su canali non sicuri**, l'accesso a sistemi critici **tramite reti pubbliche non protette**, la **registrazione su portali esterni utilizzando la mail regionale** ecc.

Smarrimento o furto di dati su dispositivi elettronici e cartacei: è il caso dei dispositivi quali, **PC, smartphone** (senza dimenticare ovviamente anche i supporti cartacei) **contenenti dati riservati,** che comporta la **perdita fisica** degli stessi**.** Non si tratta di un'eventualità rara, poiché il dispositivo può essere portato al di fuori dei locali protetti dell'Ente in varie occasioni, come ad esempio nelle situazioni di lavoro da remoto. Altra possibile causa di perdita di dati può configurarsi in caso di distruzione di un dispositivo; infatti, i guasti fisici possono derivare non solo da malfunzionamenti hardware, ma anche da un **uso improprio o da una gestione inadeguata dei dispositivi**.

Mancata applicazione delle procedure di sicurezza: ad esempio la mancata cifratura dei dati, l'assenza di aggiornamenti nei sistemi di protezione o l'uso di **password deboli**. In particolare, per quest'ultimo caso, il **riutilizzo di una stessa password** per accedere a diversi account, la **condivisione** o la **conservazione** delle password su **supporti inadatti** (quali foglietti, post-it, file salvati sul proprio desktop ecc.) sono alcuni *comportamenti assolutamente da evitare!*

Accessi non autorizzati da parte di dipendenti o collaboratori: si verificano ogni qualvolta dei soggetti non autorizzati possano accidentalmente o intenzionalmente accedere a informazioni riservate. In particolare, il sabotaggio interno, ovvero gli **atti deliberati di distruzione o furto di dati** da parte di dipendenti o collaboratori, può costituire una minaccia considerevole.

Le conseguenze di un Data Breach sui soggetti interessati

Quando si verifica un **Data Breach**, le conseguenze non ricadono esclusivamente sull'Ente coinvolto, ma anche sui **soggetti i cui dati personali sono stati violati** (es. cittadini). Dalle violazioni di informazioni anagrafiche fino a quelle sulle categorie particolari di dati personali, un **Data Breach** può portare a:

Danni economici: i dati di contatto (come l'e-mail personale) o altre informazioni personali (ad esempio, il nome e il cognome e/o il codice fiscale) possono essere utilizzati per truffe, phishing, frodi finanziarie o altre attività illecite che possono comportare perdite economiche per la vittima.

Danni reputazionali e discriminazione: la diffusione non autorizzata di informazioni personali o professionali può ledere l'immagine e la credibilità della persona coinvolta, con possibili ripercussioni sul piano sociale e lavorativo. In alcuni casi, dati sensibili relativi a salute, orientamento sessuale o convinzioni religiose potrebbero essere utilizzati in modo discriminatorio.

Furto di identità: i dati personali sottratti possono essere utilizzati per impersonare la vittima e compiere azioni fraudolente, come aprire conti bancari, richiedere prestiti o stipulare contratti a suo nome, con conseguenze potenzialmente gravi e difficili da risolvere.

Perdita di controllo sui propri dati: una volta che le informazioni personali vengono esposte, possono essere condivise, vendute nel dark web o riutilizzate senza il consenso del proprietario, rendendo molto difficile la loro eliminazione e aumentando il rischio di ulteriori abusi in futuro.

Come gestire un Data Breach in Regione Calabria - dal rilevamento alla notifica al Garante

Il nostro Ente si dota di un **processo di gestione di Data Breach** (approvato con DGR 2349/2021) [Clicca qui per consultare il "Processo di Gestione Data Breach (Incidenti di sicurezza dati di Regione Calabria)] nel quale è riportato il flusso operativo per comprendere le modalità di approccio nei casi in cui si rilevi il rischio di una violazione dei dati personali in Regione Calabria. A ciò fa fede anche quanto definito dall'**European Data Protection Board** che [Clicca qui per consultare le Linee Guida 9/2022 dell'EDPB sulla notifica delle violazioni dei dati personali ai sensi del regolamento generale sulla protezione dei dati (GDPR)] che riporta alcuni casi pratici che identificano situazioni di violazioni di dati personali.

Di seguito, **gli step operativi** da considerare per la corretta **gestione di un Data Breach**, alla luce anche di quanto stabilito nel processo regolato nel nostro Ente:

Segnalazione: È la fase da cui si parte. Nel caso di situazioni sospette o anomale, che possono essere rilevate sia da soggetti interni che esterni è necessario **segnalare tempestivamente l'evento alle funzioni preposte** alla loro gestione. Nel contesto di Regione Calabria, tali eventi devono essere prontamente segnalati al **Settore Referente Informatico**.

Identificazione: Nella fase successiva bisogna inquadrare in modo corretto l'evento e distinguere tra un **vero incidente**, che ha conseguenze reali, e un *c.d. falso positivo*. Inoltre, possono verificarsi generici **incidenti tecnici** che comportano **malfunzionamenti di sistemi senza impatti sui dati personali**, oppure un **incidente con dati personali**, che implica una violazione della privacy. Analizzare l'evento con precisione permette di adottare le giuste misure di mitigazione.

Valutazione: È la fase in cui si svolge la **valutazione della gravità dell'incidente** e per la quale è necessario utilizzare una metodologia certa e misurabile. In particolare, il Settore Referente Informatico informa dell'avvenimento il DPO, il Delegato del Titolare direttamente coinvolto nell'attività e l'Ufficio Privacy. In questa fase, **si determinano le misure di contenimento** da adottare per contrastare la violazione. Ai fini della valutazione si ricorda di considerare altresì lo **strumento di autovalutazione messo a disposizione dal Garante** per individuare le azioni da intraprendere a seguito di una violazione che aiuta a determinare **se ed in quale caso inviare una notifica di violazione dei dati personali**. [clicca qui per consultare lo strumento di autovalutazione del GPDP]

Notifica e/o Comunicazione: A valle del calcolo della gravità della violazione, se dalle analisi effettuate emerge il bisogno di procedere alla **notifica al Garante** (**senza ingiustificato ritardo** e, ove possibile, entro **72 ore** dal momento in cui ne è venuto a conoscenza) e/o **alla comunicazione degli interessati coinvolti (senza ingiustificato ritardo)**, l'invio spetterà al **Delegato del Titolare**, previa collaborazione dell'Ufficio Privacy e del DPO per la predisposizione della notifica/comunicazione.

Documentazione: È la fase nella quale va documentato in un apposito **registro** ciascun incidente avvenuto e le azioni intraprese per la sua gestione. Per la **registrazione** – presente sulla piattaforma per la gestione degli adempimenti privacy di Regione Calabria - provvede il **Settore Referente Informatico** e avviene sia in caso di accertamento positivo che negativo della violazione. Il **registro degli incidenti** ha l'obiettivo di raccogliere tutte le informazioni necessaria e deve essere **messo a disposizione dell'Autorità Garante su richiesta**.

Apprendimento: L'ultima fase è quella nella quale fare tesoro delle *lezioni apprese* allo **scopo di migliorare la prevenzione e rafforzare la comunicazione** all'interno dell'Ente. Dopo aver gestito l'incidente, è **essenziale analizzarlo in profondità per individuare le cause**, i punti critici e le eventuali inefficienze nella risposta. Questo permette di migliorare le strategie di prevenzione, affinando le procedure di sicurezza e adottando misure proattive per ridurre il rischio di eventi simili in futuro.

La protezione dei dati personali è un pilastro fondamentale per la sicurezza e l'integrità delle informazioni gestite dal nostro Ente. Prevenire i Data Breach non significa solo evitare **sanzioni o conseguenze legali, ma anche preservare la fiducia dei cittadini e garantire la trasparenza operativa**. Ogni dipendente ha un ruolo cruciale nella corretta gestione dei dati, adottando pratiche responsabili e strategie di prevenzione efficaci. Solo attraverso un impegno costante nella sicurezza possiamo proteggere le informazioni sensibili e rafforzare la resilienza dell'Ente di fronte alle *sfide del progresso tecnologico*.

Come sempre, vi ricordiamo di **segnalare** al Settore "Infrastrutture Digitali e Sicurezza", al Responsabile Protezione Dati e all'Ufficio Privacy eventuali comportamenti scorretti in materia di privacy, invitando i colleghi a adottare comportamenti conformi al quadro normativo. Il rispetto delle regole tutela l'istituzione, i dipendenti e i cittadini: la sicurezza dei dati è responsabilità di tutti.

Saluti,
Settore "Infrastrutture Digitali e Sicurezza",
Responsabile Protezione Dati,
Ufficio Privacy Regione Calabria.