Italian

information and privacy commission new south wales

Scheda informativa **Novembre 2023**

Domande più frequenti sul Sistema MNDB

A chi sono destinate queste informazioni?	Ai membri del pubblico del NSW che desiderano informazioni sul Sistema di notifica obbligatoria delle violazioni di dati (Mandatory Notification of Data Breach Scheme).
Perché queste informazioni sono importanti?	Questa scheda informativa fornisce informazioni sul Sistema e aiuta i membri del pubblico a comprendere i propri diritti in caso di violazione dei dati personali.

Che cos'è il Sistema di notifica obbligatoria delle violazioni di dati?

Il Sistema di notifica obbligatoria delle violazioni di dati (Sistema MNDB) prevede un obbligo di notifica ai sensi della legge sulla privacy e sulla protezione delle informazioni personali del 1998 *(Privacy and Personal Information Protection Act 1998* - PPIP Act) per gli enti pubblici del NSW in caso di "violazioni ammissibili dei dati".

Quando è entrato in vigore il Sistema MNDB?

Il Sistema MNDB è entrato in vigore il 28 novembre 2023.

Chi è soggetto al Sistema MNDB?

Il Sistema MNDB si applica agli enti pubblici del NSW, ai ministri, alle università, alle amministrazioni comunali e alle imprese di proprietà dello Stato che non sono soggette alla legislazione sulla privacy del Commonwealth.

Cos'è una politica sulla violazione dei dati?

Una Politica sulla violazione dei dati (Data Breach Policy - DBP) è una politica o un piano documentato che stabilisce come un ente deve rispondere ad una violazione dei dati. La legislazione impone agli enti di dotarsi di una DBP. Una DBP deve stabilire i ruoli e le responsabilità del personale dell'ente in relazione alla gestione delle violazioni e le fasi da seguire quando si verifica una violazione.

Gli enti sono tenuti a garantire che la loro DBP sia accessibile al pubblico; pertanto, devono pubblicare la DBP sul loro sito web.

Che cos'è una "violazione ammissibile dei dati"?

Ai sensi dello Schema MNDB, quando si verifica una violazione ammissibile di dati, l'ente deve informare i soggetti interessati e il Garante per la privacy.

Una violazione ammissibile di dati si verifica quando vi è:

- un accesso non autorizzato o la divulgazione non autorizzata di dati personali detenuti da un ente, che potrebbe causare un **grave danno** alla persona a cui si riferiscono i dati stessi;
- la perdita di dati personali detenuti da un ente in circostanze in cui è probabile che si sia verificato accesso o divulgazione non autorizzati, e che potrebbe causare un **grave danno** alla persona a cui si riferiscono i dati stessi.

Cosa si intende per danno grave?

Per danno grave si intendono danni fisici, economici o materiali, danni emotivi o psicologici o danni alla reputazione. L'impatto del danno può variare da persona a persona, ma può includere:

- perdite economiche a causa di una frode;
- un potenziale rischio di danno fisico o psicologico, ad esempio da parte di un ex partner violento;
- furto d'identità, che può avere ripercussioni sulle finanze e/o sulla situazione creditizia del soggetto;
- un grave danno alla reputazione di una persona.

Come si verifica una violazione dei dati?

In generale, una violazione di dati può verificarsi a causa di un errore umano, di un guasto ai sistemi o di una violazione dolosa o cibernetica.

Quali sono alcuni esempi di violazione dei dati?

Alcuni esempi di violazione dei dati sono:

Errore umano:

- Una lettera o un'e-mail che viene inviata al destinatario sbagliato.
- L'accesso al sistema viene concesso erroneamente a qualcuno senza autorizzazione, oppure la protezione della password è inadeguata.
- Perdita o smarrimento di beni fisici contenenti dati personali, ad esempio: registri, laptop, USB, telefoni.

Guasto ai sistemi:

- Un errore di codifica che consente l'accesso ai sistemi senza previa autenticazione o la generazione automatica di avvisi.
- I sistemi non vengono mantenuti attraverso l'applicazione di patch noti e supportati.

Attacco doloso o criminale:

- Incidenti informatici, ad esempio ransomware, malware, hacking, phishing, tentativi di accesso con forza bruta.
- Ingegneria sociale/impersonificazione, ovvero divulgazione inappropriata di dati personali.
- Minacce interne, da parte di dipendenti che utilizzano credenziali valide per accedere a o divulgare dati personali al di fuori dell'ambito delle loro mansioni o autorizzazioni.

L'ente è tenuto ad informare il Garante per la privacy?

Nel caso in cui una violazione dei dati sia ritenuta ammissibile, le agenzie devono informare immediatamente il Garante per la privacy, utilizzando il modulo presente sul sito web dell'IPC.

Sarò avvisato/a se sono colpito/a da una violazione ammissibile dei dati?

Se un ente ritiene che si sia verificata una violazione dei tuoi dati personali, dovrà comunicartelo non appena possibile. Ciò significa che l'ente deve avvisarti per iscritto e fornirti informazioni sulla violazione ammissibile dei dati, tra cui:

- le azioni che ha intrapreso o intende intraprendere per controllare o attenuare i danni che hai subito;
- le misure che dovresti prendere in considerazione a seguito di una violazione ammissibile dei dati;
- informazioni su come richiedere una revisione interna della condotta dell'ente o su come presentare un reclamo sulla privacy al Garante per la privacy.

Quanto tempo dopo una violazione dei dati posso aspettarmi di ricevere una notifica?

Quando un ente ha ragionevoli motivi per sospettare che si sia verificata una violazione ammissibile dei dati, deve adottare una serie di misure, tra cui:

- Compiere ogni ragionevole sforzo per contenere la violazione.
- Valutare, entro 30 giorni, se si è verificato un accesso non autorizzato, una divulgazione o una perdita di dati personali in possesso di un ente.
- Valutare, entro 30 giorni, se esiste la possibilità di un grave danno a carico di qualsiasi individuo interessato.
- Fare tutti i tentativi ragionevoli per mitigare il danno causato dalla sospetta violazione.

Se, dopo aver intrapreso i passi di cui sopra, un ente stabilisce che c'è stata una violazione ammissibile dei tuoi dati personali, deve informarti di tale violazione non appena possibile.

Cosa succede se l'ente non è più in possesso dei miei dati per informarmi di una violazione dei dati?

Gli enti hanno il potere di condividere dati nell'ambito del Sistema MNDB, che consente loro di richiedere informazioni personali pertinenti ad un altro ente pubblico. Le informazioni che un ente può richiedere sono limitate a quelle ragionevolmente necessarie per la conferma del nome e dei recapiti di una persona colpita da una violazione dei dati.

Tuttavia, se l'ente non è in grado di informarti direttamente, deve pubblicare una notifica sul proprio sito web e adottare misure ragionevoli per pubblicizzare tale notifica. Questa deve rimanere nel registro delle notifiche pubbliche dell'ente per almeno 12 mesi.

Ci sono ragioni per cui un ente potrebbe non avvisarmi?

Sì. Esistono alcune esenzioni all'obbligo di notifica di una violazione dei dati per gli enti. Ad esempio, se un ente agisce in modo rapido per mitigare una violazione dei dati e, grazie a questa azione, è improbabile che la violazione dei dati risulti in un danno grave, non vi è alcun obbligo di notifica agli individui interessati.

L'ente mi fornirà assistenza dopo la notifica?

Il tipo di assistenza o supporto che un ente può fornire a seguito di una notifica dipende dalle circostanze specifiche della violazione dei dati. Alcuni esempi includono:

- assistenza con la riemissione dei documenti d'identità o delle credenziali compromesse, come ad esempio la patente di guida;
- consigli su come proteggere i dati personali;
- connessione a ulteriori servizi di supporto e di counseling.

Cosa devo fare se ricevo una notifica?

Esistono misure pratiche che puoi adottare per proteggere i tuoi dati personali e ridurre il rischio di essere colpito/a da una violazione dei dati. I tipi di azioni che puoi intraprendere dipendono dalle circostanze della violazione dei dati e dal tipo di dati coinvolti. La notifica che ricevi dovrebbe offrire raccomandazioni sulle azioni da intraprendere in risposta al tipo di violazione individuato nella notifica stessa.

Se desideri ulteriori informazioni sulla violazione dei dati o su come proteggere i tuoi dati personali, puoi contattare l'ente che ti ha inviato la notifica.

Dove trovare maggiori informazioni?

La Commissione per l'informazione e la privacy (IPC) offre ulteriori informazioni e risorse aggiuntive sul sito web dell'IPC. In alternativa, è possibile contattare l'IPC utilizzando i recapiti riportati di seguito.

Per ulteriori informazioni

Contatta la Commissione del NSW per le informazioni e la privacy (Information and Privacy Commission NSW – IPC):

Chiamata gratuita: 1800 472 679

E-mail: ipcinfo@ipc.nsw.gov.au

Sito web: www.ipc.nsw.gov.au

N.B.: Le informazioni contenute in questa scheda informativa devono essere utilizzate solo come guida. Dovrai richiedere una consulenza legale in relazione a singole circostanze.