Spanish

information and privacy commission new south wales

Hoja informativa **Noviembre de 2023**

Preguntas frecuentes sobre el plan MNDB

¿A quién va dirigida esta información?	Miembros del público de NSW que buscan información sobre el Plan de Notificación Obligatoria de Transgresión de Datos (MNDB, por sus siglas en inglés).
¿Por qué es importante para ellos esta información?	Esta hoja informativa ayudará al público a comprender mejor el programa y cuáles son sus derechos cuando se produce una transgresión de datos (data breach) que involucra su información personal.

¿Qué es el Plan de Notificación Obligatoria de Transgresión de Datos?

El Plan de Notificación Obligatoria de Transgresión de Datos (Plan MNDB) es un requisito de notificación obligatoria en virtud de la *Ley de Protección de Privacidad e Información Personal de 1998* (Ley PPIP) para las agencias del sector público de NSW en caso de una "transgresión de datos elegible (eligible data breach)."

¿Cuándo comenzó el Plan MNDB?

El Plan MNDB comenzó el 28 de noviembre de 2023.

¿A quién se aplica el Plan MNDB?

El Plan MNDB se aplica a las agencias del sector público, ministros, universidades, consejos municipales y corporaciones estatales de NSW que no están cubiertas por la legislación de privacidad de la Commonwealth.

¿Qué es la política de transgresión de datos?

La política de transgresión de datos (Data Breach Policy / DBP) es una política o plan documentado que establece cómo una agencia responderá a una transgresión de datos. Las agencias están obligadas a tener una DBP según la legislación. Una DBP debe establecer las funciones y responsabilidades del personal de la agencia en relación con la gestión de una infracción, y los pasos que seguirá la agencia cuando se produzca.

Las agencias deben asegurarse de que su DBP sea de acceso público, lo que significa que las agencias deben publicar la DBP en su sitio web.

¿Qué es una "transgresión de datos elegible"?

En virtud del Plan MNDB, una agencia debe notificar a las personas afectadas y al Comisionado de Privacidad cuando se haya producido una transgresión de datos elegible.

Una "transgresión de datos elegible" (eligible data breach)" se produce cuando:

- Hay un acceso no autorizado a la información personal en poder de una agencia o la divulgación no autorizada de la misma que pueda causar un **daño grave** a la persona a la que la información se refiere
- La pérdida de información personal en poder de una agencia en circunstancias en las que es probable que se produzca un acceso o divulgación no autorizados, y que probablemente resultaría en un **daño grave** a la persona a la que la información se refiere.

¿Qué es un daño grave?

Los daños graves (serious harm) pueden incluir daños físicos, financieros o materiales, daños emocionales o psicológicos, o daños a la reputación. El impacto del daño puede variar de una persona a otra, pero puede incluir:

- Pérdida financiera por fraude
- Un riesgo probable de daño físico o psicológico, como por ejemplo por parte de una expareja abusiva
- Robo de identidad, que puede afectar sus finanzas y/o historial crediticio
- Daño grave a la reputación de una persona.

¿Cómo podría ocurrir una transgresión de datos?

En términos generales, una transgresión de datos puede ocurrir debido a un error humano, falla del sistema o transgresión cibernética maliciosa.

¿Cuáles son ejemplos de transgresión de datos?

Algunos ejemplos de transgresión de datos son:

Falla humana:

- Se envía una carta o correo electrónico al destinatario incorrecto.

- Se concede incorrectamente acceso al sistema a alguien sin autorización, o no hay una protección adecuada con contraseña.
- Se pierden o extravían activos físicos con información personal, por ejemplo, registros, laptop, USB, teléfono.

Falla del sistema:

- Un error de codificación que permite el acceso al sistema sin autenticación o la generación automática de avisos.
- Los sistemas no se mantienen mediante la aplicación de parches conocidos y compatibles.

Ataque malicioso o delictivo:

- Incidentes cibernéticos, por ejemplo, ransomware, malware, piratería (hacking), phishing, intentos de acceso por fuerza bruta.
- Ingeniería social/suplantación de identidad, es decir, divulgación inapropiada de información personal.
- Amenazas internas (empleados) que utilizan credenciales válidas para acceder/divulgar información personal fuera del alcance de sus tareas o permisos.

¿Es necesario que la agencia notifique al Comisionado de Privacidad?

Cuando una transgresión de datos se evalúe como transgresión de datos elegible, las agencias deben notificar al Comisionado de Privacidad de inmediato, utilizando el formulario en el sitio web de la IPC.

¿Se me notificará si me veo afectado por una transgresión de datos elegible?

Si una agencia decide que ha habido una transgresión de datos elegible en relación con su información personal, debe notificarle tan pronto como sea posible. Esto significa que la agencia debe notificarle por escrito y darle información sobre la transgresión de datos elegible, lo que incluye:

- Acciones que la agencia ha tomado o planea tomar para controlar o mitigar el daño que se le ha causado
- Medidas que usted debe considerar tomar después de una transgresión de datos elegible
- información sobre cómo solicitar una revisión interna de la conducta de la agencia o cómo presentar una queja de privacidad ante el Comisionado de Privacidad.

¿Cuánto tiempo después de una transgresión de datos se me notificará?

Cuando una agencia tiene motivos razonables para sospechar que puede haber ocurrido una transgresión de datos elegible, las agencias deben tomar una serie de medidas:

- Hacer todos los esfuerzos razonables para contener la transgresión.
- Evaluar si ha habido acceso no autorizado, divulgación o pérdida de información personal en poder de una agencia en un plazo de 30 días.
- Evaluar si existe la probabilidad de daño grave a cualquier persona afectada dentro de los 30 días.
- Hacer todo intento razonable para mitigar el daño causado por la presunta transgresión.

Si, después de llevar a cabo los pasos anteriores, una agencia decide que ha habido una transgresión de datos elegible en relación con su información personal, debe notificarle lo antes posible sobre la misma.

¿Qué pasa si la agencia ya no tiene mis datos para notificarme sobre una transgresión de datos?

Las agencias tienen facultades de intercambio de información en virtud del Plan MNDB para permitirles solicitar información personal pertinente de otra agencia del sector público. La información que una agencia puede solicitar se limita a la información que es razonablemente necesaria para confirmar nombre y datos de contacto de una persona afectada por una transgresión de datos.

Sin embargo, si la agencia no puede notificarle directamente, debe publicar una notificación en su sitio web y tomar medidas razonables para publicitar la notificación. La notificación debe permanecer en el registro de notificaciones públicas de la agencia durante al menos 12 meses.

¿Hay razones por las que una agencia podría no notificarme?

Sí. Existen ciertas excepciones al requisito de que las agencias notifiquen a las personas afectadas de una transgresión de datos. Por ejemplo, si una agencia actúa rápidamente para mitigar una transgresión de datos y, debido a esta acción, no sea probable que la transgresión de datos provoque daños graves, no es necesario notificar a las personas afectadas.

¿La agencia me proporcionará alguna ayuda después de una notificación?

El tipo de asistencia o apoyo que una agencia puede proporcionar después de una notificación dependerá de las circunstancias específicas de la transgresión de datos. Algunos ejemplos pueden ser:

- Asistencia para reemplazar documentos de identidad o credenciales gubernamentales comprometidos, como una licencia de conducir
- Consejos sobre cómo proteger su información personal
- Proporcionar enlaces a servicios adicionales de apoyo y asesoramiento.

¿Qué debo hacer si recibo una notificación?

Hay medidas prácticas que puede tomar para proteger su información personal y reducir el riesgo de que se vea perjudicado por una transgresión de datos. Los tipos de acciones que puede tomar dependerán de las circunstancias de la transgresión y del tipo de información involucrada. La notificación que reciba debe recomendar acciones que puede tomar en respuesta al tipo de transgresión identificado en la notificación.

Si desea obtener más información sobre la transgresión de datos o cómo proteger su información personal, debe ponerse en contacto con la agencia que le envió la notificación.

¿Dónde puedo encontrar más información?

La Comisión de Información y Privacidad (IPC) tiene más información y recursos adicionales disponibles en su sitio web. Alternativamente, puede ponerse en contacto con la IPC utilizando los datos de contacto que figuran a continuación.

Para más información

Póngase en contacto con la Comisión de Información y Privacidad de NSW (IPC):

Llamada gratuita: 1800 472 679

Correo electrónico: ipcinfo@ipc.nsw.gov.au

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

NOTA: *La información de esta hoja informativa debe usarse únicamente como guía. Se debe buscar asesoramiento legal en relación con las circunstancias individuales.*