Arabic

information and privacy commission new south wales

نشرة معلومات

تشرين الثاني/نوفمبر 2023

أسئلة شائعة عن برنامج MNDB

لمن هذه المعلومات؟	لأفراد الجمهور في نيو ساوث ويلز الذين يبحثون عن معلومات عن 'برنامج الإخطار الإلزامي لحوادث خرق البيانات'.
ما الذي يجعل هذه المعلومات مهمة لهم؟	ستساعد نشرة المعلومات هذه أفراد الجمهور على فهم المزيد عن البرنامج وما هي حقوقهم عند حدوث خرق للبيانات يتعلق بمعلوماتهم الشخصية.

ما هو نظام الإخطار الإلزامي لحوادث خرق البيانات؟

برنامج الإخطار الإلزامي لحوادث خرق البيانات (برنامج MNDB) هو شرط إلزامي للإخطار بموجب *قانون حماية الخصوصية والمعلومات الشخصية لعام 1998* (قانون PPIP) لوكالات القطاع العام في نيو ساوث ويلز في حالة حدوث 'خرق بيانات مؤهلة'.

متى بدأ برنامج MNDB؟

بدأ برنامج MNDB في 28 تشرين الثاني/نوفمبر 2023.

على من ينطبق برنامج MNDB؟

ينطبق برنامج MNDB على وكالات القطاع العام في نيو ساوث ويلز والوزراء والجامعات ومجالس البلدية والشركات التي تملكها الولاية ولا يغطيها تشريع الخصوصية التابع للكومنولث.

ما هي سياسة خرق البيانات؟

سياسة خرق البيانات (أوDBP) هي سياسة أو خطة موثقة تحدد كيفية استجابة الوكالة لحدوث خرق للبيانات. بموجب التشريع، يتعين وجود خطة DBP لدى الوكالات. ويجب أن تحدد DBP أدوار ومسؤوليات موظفي الوكالة فيما يتعلق بإدارة أي خرق والخطوات التي ستتبعها الوكالة عند حدوث خرق.

وعلى الوكالات التأكد من إمكانية وصول عموم الناس إلى خطة DBP الخاصة بها بسهولة، مما يعني أنه ينبغي على الوكالات نشر DBP الخاصة بها على موقعها الإلكتروني.

ما هو 'خرق البيانات المؤهلة'؟

بموجب برنامج MNDB، يجب على الوكالة إخطار الأفراد المتأثرين ومفوض الخصوصية عندما يكون هناك خرق لبيانات مؤهلة.

يحدث 'خرق البيانات المؤهلة' عندما يكون هناك:

- وصول غير مصرح به إلى أو إفصاح غير مصرح به عن المعلومات الشخصية التي تحتفظ بها الوكالة يُحتمل أن يؤدي إلى **ضرر خطير** للفرد الذي تتعلق به المعلومات
- فقدان للمعلومات الشخصية التي تحتفظ بها الوكالة في ظروف يُمحتمل أن يحدث فيها وصول أو كشف غير مصرح به يُحتمل أن يؤدي إلى **ضرر خطير** للفرد الذي تتعلق به المعلومات.

ما هو الضرر الخطير؟

يمكن أن يشمل الضرر الخطير ضررًا جسديًا أو ماليًا أو ماديًا، أو أذى عاطفيًا أو نفسيًا، أو الإضرار بسمعة الفرد. ويمكن أن يختلف تأثير الضرر من شخص لآخر، ولكنه قد يشمل ما يلي:

- خسارة مالية عن طريق الاحتيال
- خطر محتمل للتعرض للأذى الجسدي أو النفسي، على سبيل المثال من قبل شريك سابق يمارس الإساءة
- سرقة الهوية والتي يمكن أن تؤثر على أموالك و/أو سجلك الائتماني
- الإضرار الخطير بسمعة الفرد.

كيف يمكن أن يحدث خرق البيانات؟

على العموم، يمكن أن يحدث خرق البيانات بسبب خطأ بشري أو فشل الأنظمة أو نتيجة خرق خبيث أو سيبراني.

ما هي الأمثلة على خرق البيانات؟

بعض الأمثلة على خرق البيانات هي:

الخطأ البشري:

- إرسال رسالة بالبريد العادي أو الإلكتروني إلى شخص عن طريق الخطأ.
- إعطاء شخص ما القدرة على الدخول إلى النظام عن طريق الخطأ دون تصريح أو عدم وجود حماية كافية لكلمات المرور.
- فقدان أشياء مادية تحتوي على معلومات شخصية و/أو وضعها في غير مكانها، على سبيل المثال، السجلات وجهاز الكمبيوتر المحمول وUSB وجهاز الهاتف.

فشل النظام:

- خطأ في الترميز يسمح بالوصول إلى النظام دون مصادقة، أو إنشاء إشعارات تلقائيًا
- عدم صيانة الأنظمة من خلال تطبيق التصحيحات المعروفة والمدعومة.

الهجوم الخبيث أو الإجرامي:

- الحوادث السيبرانية، على سبيل المثال، برامج الفدية، والبرامج الضارة، والقرصنة، والتصيّد الاحتيالي، ومحاولات الوصول بالقوة الغاشمة.
- الهندسة الاجتماعية/انتحال الشخصية، ومعنى ذلك الإفصاح غير المناسب عن المعلومات الشخصية.

مفوضية المعلومات والخصوصية في نيو ساوث ويلز
(www.ipc.nsw.gov.au | 1800 IPC NSW (1800 472 679

- التهديدات الداخلية (من جانب الموظفين) باستخدام بيانات اعتماد صالحة للوصول إلى/الإفصاح عن المعلومات الشخصية خارج نطاق واجباتهم أو تصاريحهم.

هل تحتاج الوكالة إلى إخطار مفوض الخصوصية؟

عندما يتم تقييم خرق البيانات على أنه خرق لبيانات مؤهلة، يجب على الوكالات إخطار مفوض الخصوصية على الفور، باستخدام الإستمارة الموجودة على موقع IPC الإلكتروني.

هل سيتم إعلامي إذا تأثرتُ بخرق بيانات مؤهلة؟

إذا قررت إحدى الوكالات أن هناك خرقًا لبيانات مؤهلة يتعلق بمعلوماتك الشخصية، يجب عليها إخطارك في أقرب وقت ممكن عمليًا بهذا الخرق. وهذا يعني أنه يجب على الوكالة إخطارك كتابيًا وإعطاءك معلومات عن خرق البيانات المؤهلة، بما في ذلك ما يلي:

- الإجراءات التي اتخذتها الوكالة أو تخطط لاتخاذها للتحكّم بالضرر الذي لحق بك أو تخفيفه
- الخطوات التي ينبغي أن تفكر في اتخاذها بعد حدوث خرق لبيانات مؤهلة
- معلومات عن كيفية طلب إجراء مراجعة داخلية لسلوك الوكالة أو كيفية تقديم شكوى تتعلق بالخصوصية إلى مفوض الخصوصية.

ما هي المدة التي يمكنني أن أتوقع أن يتم إخطاري فيها بعد حدوث خرق للبيانات؟

عندما يكون لدى الوكالة أسباب معقولة للاشتباه في احتمال حدوث خرق لبيانات مؤهلة، يجب عليها اتخاذ عدد من الخطوات:

- بذل كافة الجهود المعقولة لاحتواء الخرق.
- تقييم ما إذا كان هناك وصول أو إفصاح غير مصرح به أو فقدان معلومات شخصية تحتفظ بها الوكالة في غضون 30 يومًا.
- تقييم ما إذا كان هناك احتمال لحدوث ضرر خطير لأي فرد متأثر في غضون 30 يومًا.
- بذل كافة المحاولات المعقولة للتخفيف من الضرر الناجم عن الخرق المشتبه به.

إذا قررت إحدى الوكالات، بعد اتخاذها الخطوات المذكورة أعلاه، أنه قد حدث خرق لبيانات مؤهلة يتعلق بمعلوماتك الشخصية، يجب عليها إخطارك في أقرب وقت ممكن عمليًا بهذا الخرق.

ماذا لو لم يعد لدى الوكالة تفاصيل الاتصال بي لإخطاري بشأن خرق البيانات؟

لدى الوكالات صلاحيات لتبادل المعلومات بموجب نظام MNDB وذلك لتمكينها من طلب المعلومات الشخصية ذات الصلة من وكالة أخرى في القطاع العام. تقتصر المعلومات التي يمكن أن تطلبها وكالة ما على المعلومات الضرورية بشكل معقول لتأكيد الاسم وتفاصيل الاتصال الخاصة بالفرد المتأثر بخرق البيانات.

إلّا أنه إذا لم تتمكن الوكالة من إخطارك مباشرة، فيجب عليها نشر إخطار على موقعها الإلكتروني واتخاذ خطوات معقولة لنشر الإخطار. ويجب أن يظل الإخطار على سجل الإخطارات العامة للوكالة لمدة 12 شهرًا على الأقل.

هل هناك أسباب لعدم قيام الوكالة بإخطاري؟

نعم. هناك استثناءات معينة لشرط قيام الوكالات بإخطار الأفراد المتأثرين بخرق البيانات. على سبيل المثال، إذا تصرفت إحدى الوكالات بسرعة للتخفيف من تأثير خرق البيانات وأصبح من غير المرجح، نتيجة لهذا الإجراء، أن يؤدي خرق البيانات إلى ضرر خطير، فلا يكون هناك أي التزام بإخطار أي أفراد متأثرين.

هل ستقدم لي الوكالة أي مساعدة بعد الإخطار؟

يعتمد نوع المساعدة أو الدعم الذي قد تقدمه الوكالة بعد الإخطار على الظروف المحددة لخرق البيانات. قد تشمل الأمثلة ما يلي:

- المساعدة في إبدال وثائق الهوية أو الأوراق الثبوتية الصادرة عن الحكومة والتي تم خرقها - مثل رخصة القيادة
- نصائح حول كيفية حماية معلوماتك الشخصية
- توفير روابط لخدمات الدعم والمشورة الإضافية.

ماذا يجب أن أفعل إذا تلقيت إخطارًا؟

هناك خطوات عملية يمكنك اتخاذها لحماية معلوماتك الشخصية وتقليل مخاطر تعرضك للضرر بسبب خرق البيانات. تعتمد أنواع الإجراءات التي يمكنك اتخاذها على ظروف خرق البيانات ونوع المعلومات المعنية. يجب أن يوصي الإخطار الذي تتلقاه بالإجراءات التي يمكنك اتخاذها كاستجابة لنوع الخرق المحدد في الإخطار.

إذا كنت تريد المزيد من المعلومات حول خرق البيانات أو كيفية حماية معلوماتك الشخصية، ينبغي عليك الاتصال بالوكالة التي أرسلت إليك الإخطار.

أين يمكنني العثور على مزيد من المعلومات؟

لدى مفوضية المعلومات والخصوصية (IPC) المزيد من المعلومات والموارد الإضافية المتاحة على موقعها الإلكتروني. وبدلاً من ذلك، يمكنك الاتصال بـ IPC باستخدام تفاصيل الاتصال أدناه.

للمزيد من المعلومات

اتصل بمفوضية المعلومات والخصوصية في نيو ساوث ويلز:

مكالمة مجانية: 1800 472 679

البريد الإلكتروني: ipcinfo@ipc.nsw.gov.au

الموقع الإلكتروني: www.ipc.nsw.gov.au

ملاحظة: ينبغي استخدام المعلومات الواردة في نشرة المعلومات هذه كدليل فقط. وينبغي طلب المشورة القانونية فيما يتعلق بالظروف الفردية.