State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

إخطارات اختراق البيانات الشخصية

PDPPL-02050217A

المبادئ التوجيهية للمخاطبين بأحكام القانون

شؤون الحوكمة والضمان السيبراني الوطني

الإصدار: ٢,٠

تاريخ الإصدار الأولي: نوفمبر ٢٠٢٠

تاريخ التحديث الأخير: سبتمبر ٢٠٢٢

تصنيف الوثيقة: عامّ

تحديثات الوثيقة

رقم الإصدار	الوصف	تاريخ التحديث
١,٠	الوثيقة المنشورة ذات الاصدار ١,٠	نوفمبر ٢٠٢٠
٢,٠	الوثيقة المنشورة ذات الإصدار ٢,٠	سبتمبر ٢٠٢٢

الوثائق ذات صلة

الرقم المرجعي للوثيقة	اسم الوثيقة
PDPPL-02050208A	المبادئ التوجيهية لأسس حماية خصوصية البيانات الموجهة للمخاطبين بأحكام القانون
PDPPL-02050206A	المبادئ التوجيهية لتحليل تأثير حماية خصوصية البيانات الموجهة للمخاطبين بأحكام القانون
PDPPL-02040403A	نموذج إخطار اختراقات البيانات الشخصية

تنويه \ الحقوق القانونية

تم إعداد هذه المبادئ التوجيهية للمراقبين/المعالجين الذين يعالجون البيانات الشخصية إلكترونيًا أو الذين يجمعون البيانات الشخصية أو يتلقونها أو يقومون باستخراجها تحسبًا لمعالجتها إلكترونيًا أو الذين يعالجون البيانات الشخصية من خلال مجموعة من تقنيات المعالجة الإلكترونية والتقليدية. كما أن هذه المبادئ التوجيهية تعمل على تقديم المعلومات للأفراد والأطراف المعنية الأخرى حول كيفية امتثال المؤسسات لقانون حماية خصوصية البيانات الشخصية Personal Data Privacy Protection (Law) - PDPPL.

لا تعد الوكالة الوطنية للأمن السيبراني (National cyber Security Agency) و / شؤون الحوكمة والضمان السيبراني (National Cyber Governance and Assurance Affairs)) مسؤولة عن أي أضرار تنشأ عن استخدام أو عدم القدرة على استخدام هذه المبادئ التوجيهية أو أي مادة واردة فيها، أو من أي إجراء أو قرار تم اتخاذه نتيجة لاستخدامها. قد يرغب أي فرد أو مؤسسة في طلب استشارة من المستشار القانوني و / أو المهني للحصول على مشورة قانونية أو غيرها فيما يتعلق بهذه المبادئ التوجيهية.

بغض النظر عن وسائل نسخ الوثيقة، أي نسخ لهذه الوثيقة سواء بشكل جزئي أو كلّي يجب أن تقر شؤون الحوكمة والضمان السيبراني والوكالة الوطنية للأمن السيبراني كمصدر للوثيقة ومالك لوثيقة "المبادئ التوجيهية للاتصال الالكتروني لغرض التسويق المباشر الموجهة للمخاطبين بأحكام القانون".

سيتطلب أي نسخ يتعلق بهذه الوثيقة لأي غرضٍ كان إذنًا خطّيّاً من شؤون الحوكمة والضمان السيبراني والوكالة الوطنية للأمن السيبراني. تحتفظ شؤون الحوكمة والضمان السيبراني والوكالة الوطنية للأمن السيبراني بالحق في تقييم الجانب الوظيفي والتطبيقي لهذا النسخ من هذه الوثيقة المعدة لغرض تجاري.

لا يعتبر الإذن المقدم من شؤون الحوكمة والضمان السيبراني والوكالة الوطنية للأمن السيبراني أنه موافقة على الوثيقة المنسوخة التي تم إعدادها ولا يجوز للجهة الناسخة للوثيقة نشرها أو إساءة استخدامها من خلال وسائل الإعلام أو المحادثات أو الاجتماعات العامّة. كما يجب أن لا تنسب ملكية الوثيقة المنسوخة الى الجهة الناسخة، وإنما تبقى ملكيتها تابعة للوكالة الوطنية للأمن السيبراني.

التوصيات القانونية

بناءً على القرار الأميري رقم (1) لسنة 2021، فإن شؤون الحوكمة والضمان السيبراني مفوضة من قبل الوكالة الوطنية للأمن السيبراني باعتبارها الإدارة المختصة بتطبيق القانون رقم (١٣) لسنة ٢٠١٦ بخصوص قانون حماية خصوصية البيانات الشخصية (PDPPL).

تنص المادة ٢٧ من القانون رقم (١٣) لسنة ٢٠١٦ من شؤون الحوكمة والضمان السيبراني اتخاذ جميع الإجراءات اللازمة لأغراض تنفيذ قانون حماية خصوصية البيانات الشخصية (PDPPL).

تم إعداد هذه المبادئ التوجيهية للأخذ في الاعتبار القوانين المعمول بها في دولة قطر. إذا نشأ تعارض بين هذه الوثيقة وقوانين أخرى في دولة قطر، تكون للقوانين الأولوية. وفي هذه الحالة يتم حذف أي مصطلح متعارض من هذه الوثيقة، وتبقى الوثيقة قائمة دون التأثير على الأحكام الأخرى على أن يتم تحديث الوثيقة لضمان الامتثال للقوانين ذات الصلة المعمول بها في دولة قطر.

المعلومات الواردة في هذه المبادئ التوجيهية ليست شاملة ويجب قراءتها بالاقتران مع قانون حماية خصوصية البيانات الشخصية (PDPPL)، والمبادئ التوجيهية الصادرة عن شؤون الحوكمة والضمان السيبراني وأي قرارات وزارية ذات صلة.

قائمة المحتويات

١ - النقاط الرئيسية

- اختراق البيانات الشخصية هو فقدان البيانات أو تعديلها أو إتلافها أو إفشائها. يمكن أن تحدث الاختراقات لأسباب متعمدة أو عن طريق الخطأ. عندما يتعلق الأمر بالبيانات الشخصية، يعد ذلك اختراقاً للبيانات الشخصية.
- يمكن أن تتسبب اختراقات البيانات الشخصية أضرار جسيمة للأفراد، سواء كانت جسدية أو معنوية أو مادية يتم استخدامها، على سبيل المثال، لتمكين السرقة أو التمييز أو التسبب في إزعاج للأفراد.
- يجب على المراقب وضع الاحتياطات المناسبة لمنع اختراقات البيانات الشخصية. بالإضافة الى ذلك، يجب أن يكون المراقب قادر على الكشف عن الاختراقات، إجراء أنشطة تصنيف وتحديد الأولويات في إطار زمني مناسب، وتقييم ما إذا كان الاختراق قد يتسبب في أضرار جسيمة للأفراد.
- يجب على المراقب إجراء تمارين الاستجابة لاختراقات البيانات الشخصية بشكل مستمر. كما يجب أن يكون هذا جزءًا من إطار أمن المعلومات الخاص بالمراقب.
- يجب أن يقوم المراقب بإخطار شؤون الحوكمة والضمان السيبراني والأفراد باختراق البيانات الشخصية في غضون ٧٢ ساعة من إدراكه للاختراق، حيث يمكن أن يتسبب الاختراق في خطر جسيم للأفراد.
- قد يؤدي عدم إخطار شؤون الحوكمة والضمان السيبراني أو الأفراد عن اختراق البيانات الشخصية كما هو مطلوب إلى عقوبة تصل إلى ١,٠٠٠,٠٠٠ ريال قطري لكل مخالفة بموجب المادة ٢٣ من قانون حماية خصوصية البيانات الشخصية (PDPPL).
- قد يؤدي عدم اتخاذ الاحتياطات المناسبة التي تتناسب مع طبيعة وأهمية البيانات الشخصية إلى عقوبة تصل إلى ٥,٠٠٠,٠٠٠ ريال قطري لكل مخالفة بموجب المادة ٢٤ من قانون حماية خصوصية البيانات الشخصية (PDPPL).
- عدم قيام المعالج بإخبار المراقب باختراق البيانات الشخصية الذي قد يتسبب بحدوث خطر ما قد يؤدي إلى عقوبة مترتبة على المراقب تصل إلى ٥,٠٠٠,٠٠٠ ريال قطري لكل مخالفة بموجب المادة ٢٤ من قانون حماية خصوصية البيانات الشخصية (PDPPL).
- إذا كان المراقب يعمل ضمن نطاق قوانين أو لوائح البيانات الشخصية الدولية الأخرى (مثل اللائحة العامة لحماية البيانات في الاتحاد الأوروبي)، فيجب عليه مراعاة متطلبات الإبلاغ عن اختراقات البيانات الشخصية بموجب هذه القوانين وكذلك بموجب قانون حماية خصوصية البيانات الشخصية (PDPPL).

٢ - المقدمة

يتطلب قانون حماية خصوصية البيانات الشخصية (PDPPL) من المراقب إخطار الأفراد شؤون الحوكمة والضمان السيبراني بأي اختراق "قد يتسبب في أضرار جسيمة" لخصوصية الفرد أو حماية خصوصية بياناته الشخصية. قد يكون هذا اختراقاً للأمن، على سبيل المثال سرقة البيانات الشخصية، أو اختراقاً لاحتياطات حماية خصوصية البيانات الشخصية، على سبيل المثال عندما لا يقوم الموظفون باتّباع الاحتياطات الإدارية مثل السياسات والإجراءات أو وجود احتياطات فنية مثل التشفير غير فعّالة.

تم إعداد هذه المبادئ التوجيهية من قبل شؤون الحوكمة والضمان السيبراني لتزويد المراقبين بمعلومات عن الإجراءات الاحترازية التي يمكنهم اتخاذها لتقليل احتمالية حدوث اختراق للبيانات الشخصية. بالإضافة إلى ذلك، توفر هذه المبادئ التوجيهية معلومات حول التزامات المراقبين بالاستجابة للاختراقات في حالة حدوثها ومتطلبات الإبلاغ عن مثل هذا الاختراقات إلى شؤون الحوكمة والضمان السيبراني اعتمادًا على طبيعة الاختراق.

يمكن الاطّلاع على متطلبات منع الاختراقات وإدارتها والإبلاغ عنها في المواد (٥) ١١و ١٣ و ١٤، ويتم شرحها بمزيد من التفاصيل أدناه.

٣ - ما هو اختراق البيانات الشخصية؟

يعني اختراق البيانات الشخصية اختراقاً للأمن يؤدي إلى التدمير الغير مقصود أو غير القانوني أو الضياع أو التغيير أو الكشف غير المصرح به أو الوصول إلى البيانات الشخصية. وهذا يشمل كل من الاختراقات الغير مقصودة وغير متعمدة.

فيما يلي بعض الأمثلة على اختراقات البيانات الشخصية:

- سرقة أو فقدان معدات تكنولوجيا المعلومات التي تحتوي على بيانات شخصية أو تجارية ذات طبيعة خاصّة؛
- الوصول بشكل غير صحيح إلى البيانات العملاء / الموظفين الشخصية؛
- ترك الملفات السرية / الحساسة دون مراقبة؛
- التخلص غير الدقيق من المواد السرية؛
- الكشف غير المصرح به عن بيانات العملاء؛
- استخدام بيانات العملاء لتحقيق مكاسب شخصية.

غالبًا ما ينتج عن اختراقات البيانات الشخصية تأثيرات سلبية على الأفراد أو المؤسسات و / أو المجتمعات، مثل:

- مخاطر متعلقة بالسلامة شخصية أو حماية خصوصية البيانات الشخصية؛
- عبء الالتزامات القانونية الإضافية أو العقوبات التنظيمية؛
- الخسارة المالية / الضرر التجاري؛
- تعطل الأعمال أو أضرار السمعة؛
- عدم قدرة الأفراد على الوصول إلى بياناتهم أو ممارسة الحقوق بموجب قوانين حماية الخصوصية.

الأمثلة المذكورة أعلاه ليست حصرية ولكنها تشير إلى أنواع الخروقات والعواقب التي يجب أن يضع المراقب الاحتياطات اللازمة لمنع حدوثها والتخفيف من أثرها.

٤ - ما الذي ينص عليه قانون حماية خصوصية البيانات الشخصية (PDPPL) فيما يخص اختراق البيانات الشخصية؟

تنص المادة (٥)١١ من قانون حماية خصوصية البيانات الشخصية (PDPPL) على ما يلي:

*"على المراقب اتخاذ الإجراءات التالية: وضع نظم داخلية للإدارة الفعالة للبيانات الشخصية، **والإبلاغ عن أي تجاوز للإجراءات** التي تهدف إلى حمايتها ".*

تنص المادة ١٣ من قانون حماية خصوصية البيانات الشخصية (PDPPL) على ما يلي :

*" يجب على كل من المراقب والمعالج **اتخاذ الاحتياطات اللازمة لحماية البيانات الشخصية** من الضياع أو التلف أو التعديل أو الإفشاء، أو الوصول إليها أو استخدامها بشكل عارض أو غير مشروع.*

ويجب أن تكون تلك الاحتياطات متناسبة مع طبيعة وأهمية البيانات الشخصية المراد حمايتها.

*وعلى **المعالج أن يخطر المراقب بوجود أي إخلال بالاحتياطات** المشار إليها، أو عند حدوث أي **خطر يهدد البيانات الشخصية للأفراد بأي وجه، فور علمه بذلك".***

تنص المادة ١٤ من قانون حماية خصوصية البيانات الشخصية (PDPPL) على ما يلي :

*يجب على **المراقب إعلام الفرد والإدارة المختصة، بحدوث أي إخلال بالاحتياطات** المنصوص عليها في المادة السابقة، **إذا كان من شأن ذلك إحداث ضرر جسيم** بالبيانات الشخصية أو بخصوصية الفرد.*

بشكل موجز، ينص قانون حماية خصوصية البيانات الشخصية (PDPPL) على ما يلي فيما يخص اختراقات البيانات الشخصية:

- يجب على المراقب اتخاذ الاحتياطات المناسبة لمنع وتقليل احتمالية وتأثير الاختراقات.
- يجب أن يكون المراقب قادر على الكشف عن الاختراق في حال حدوثه وأن يقيّم على الفور احتمال حدوث ضرر جسيم للأفراد.
- يجب على المراقب الإبلاغ عن اختراق البيانات الشخصية إلى شؤون الحوكمة والضمان السيبراني دون تأخير وخلال ٧٢ ساعة من إدراكه، إذا كان اختراق البيانات الشخصية قد يتسبب في تلف البيانات الشخصية أو خصوصية للأفراد.
- يجب أن يقوم المراقب بإخطار الأفراد باختراق البيانات الشخصية دون تأخير وفي غضون ٧٢ ساعة من إدراك ذلك إذا كان اختراق البيانات الشخصية يمكن أن يتسبب في أضرار جسيمة لبيانات الأفراد الشخصية أو خصوصية الأفراد.

٥ - ما الاحتياطات التي يمكن أن يتخذها المراقب لتقليل احتمالية حدوث اختراق للبيانات الشخصية؟

هناك العديد من الاحتياطات التي يمكن أن يقوم المراقب بتطبيقها لتقليل احتمالية حدوث اختراقات للبيانات الشخصية، مع التأكد من إعداد وتطبيق احتياطات جديدة بشكل منتظم. يجب على المراقب اتخاذ الاحتياطات الإدارية والتقنية والمالية لحماية خصوصية البيانات الشخصية وخصوصية الأفراد. يمكن الاطّلاع على معلومات شاملة حول هذه الاحتياطات ضمن المبادئ التوجيهية لحماية خصوصية البيانات الشخصية المتضمنة بالتصميم والمتضمنة افتراضياً للمخاطبين بأحكام القانون.

فيما يلي أمثلة على الاحتياطات التي يمكن أن يطبقها المراقب، خاصّةً فيما يتعلق بمنع اختراقات البيانات الشخصية:

تطبيق إطار قوي لأمن المعلومات

يجب أن يقوم المراقب بتطبيق إطارًا قويًا لأمن المعلومات، حيث يتم تصنيف البيانات (بما في ذلك البيانات الشخصية) والحفاظ عليها آمنة باستخدام إجراءات الأمن التي تتناسب مع خطر الضرر الذي قد يسببه الاختراق لخصوصية الأفراد أو حماية خصوصية البيانات الشخصية.

إعداد إطار استجابة لاختراقات البيانات الشخصية

يجب على المراقب الاستعداد للاختراقات المحتملة من خلال تطبيق إطار استجابة لاختراقات البيانات الشخصية. يجب أن يخصص هذا الإطار الأدوار والمسؤوليات التي يجب على الموظفين الوفاء بها في حالة حدوث اختراق (انظر البند التالي) وتوفير الأدوات والتوجيهات اللازمة لهم للاستجابة بفعالية لاختراقات البيانات الشخصية. تزداد قدرة المراقب على الاستجابة للاختراق بكفاءة وفعالية تماشيًا مع مستوى الاستعدادات التي يتم العمل بها. يجب أن يشتمل إطار الاستجابة لاختراقات البيانات الشخصية على التوجيه المناسب للنقاط التالية:

١ - معرفة وإدراك اختراقات البيانات الشخصية؛

٢ - إخطار الأشخاص المعنيين في المؤسسة؛

٣ - التواصل مع الموظفين بشأن خرق البيانات الشخصية مع مراعاة تعليمات السرية؛

٤ - القيام بأنشطة تصنيف وتحديد الأولويات المتعلقة باختراقات البيانات؛

٥ - تشكيل فريق الاستجابة للاختراقات؛

٦ - تحديد مدى اختراق البيانات الشخصية؛

٧ - إجراء تقييم للضرر الجسيم الذي يلحق بالأشخاص؛

٨ - تقييم متطلبات الإخطار والقيام بإخطار شؤون الحوكمة والضمان السيبراني والأفراد المعنيين؛

٩ – إغلاق ملف الاختراق البيانات الشخصية؛

١٠- توثيق الانتهاك والدروس المستفادة للحد من تكرار اختراقات البيانات الشخصية.

تحديد الأدوار والمسؤوليات للاستجابة لاختراقات البيانات الشخصية

يجب أن يقوم المراقب بتحديد من هو المسؤول عن إجراء أنشطة تصنيف وتحديد الأولويات المتعلقة باختراقات البيانات بعد اكتشاف الاختراق، وتقييم الضرر المحتمل على الأفراد، والتواصل مع شؤون الحوكمة والضمان السيبراني والأفراد المتضررين، وأداء الأنشطة لإدارة وإغلاق ملف الاختراق.

إجراء تحليل تأثير حماية خصوصية البيانات (DPIA) لأنشطة المعالجة المعنية

يجب أن يقوم المراقب بإجراء تحليل تأثير حماية خصوصية البيانات (DPIA) قبل إجراء أنشطة معالجة جديدة. تتمثل أهمية هذا الإجراء بإمكانية تسبب معالجة البيانات الشخصية بضررًا جسيماً على الأفراد الذين تتعلق بهم البيانات الشخصية. من المخاطر التي يجب تحديدها عند إجراء تحليل تأثير حماية خصوصية البيانات (DPIA) هو خطر اختراق البيانات الشخصية. كما يجب تحديد إجراءات لمنع أو الاستجابة لاختراق البيانات الشخصية، بما في ذلك أي إجراءات محددة يلزم اتخاذها لنشاط المعالجة المحدد.

تدريب الموظفين على الكشف عن اختراقات البيانات الشخصية والإخطارات المتعلقة بالاختراقات

يجب أن يقوم المراقب بترتيب جلسات تدريب وتوعية منتظمة فيما يخص حماية خصوصية البيانات والتي يجب أن تغطي اختراقات البيانات الشخصية والإجراءات المناسبة التي يجب اتباعها عند اكتشاف الاختراق. كما يجب أن يكون الموظفين على دراية حول كيفية تحديد اختراق البيانات الشخصية، وعند القيام بذلك، معرفة من هم الأشخاص الذين يجب إبلاغهم داخل مؤسسة المراقب.

يعد التدريب على اختراقات البيانات الشخصية وحماية الخصوصية ضابط إداري أساسي لحماية خصوصية البيانات الشخصية. إذا لم يكن الموظفون على دراية بكيفية التعرف على اختراقات البيانات الشخصية، فقد لا يكون من الممكن الكشف عن هذه الاختراقات.

تحديد مسؤوليات المراقب والمعالج في حالة الإخلال بالعقود

عندما يقوم المراقب بتعيين معالج لمعالجة البيانات الشخصية نيابة عنه، يجب أن يضمن المراقب أنه قد قام بتحديد بوضوح في عقود واتفاقيات معالجة البيانات الشخصية التزامات كل طرف في حالة حدوث اختراقات البيانات الشخصية.

على سبيل المثال، إذا تعرّض المعالج لاختراق للبيانات الشخصية، فيجب على المعالج إبلاغ المراقب على الفور إذا كانت البيانات التي تم اختراقها تتكون من البيانات الشخصية التي عهد بها المراقب إلى المعالج للمعالجة بما يتماشى مع المادة ١٣ من قانون حماية خصوصية البيانات الشخصية (PDPPL).

إجراء تمارين الاستجابة للاختراقات والتدريبات بانتظام لاختبار خطط الاستجابة للاختراقات

تعد خطط الاستجابة للاختراقات أمرًا بالغ الأهمية لتمكين القدرة على الاستجابة بشكل فعّال لاختراقات البيانات الشخصية عند حدوثها. يجب على المراقب التفكير في إجراء تمارين استجابة للاختراقات "تجارب عملية" لممارسة واختبار وتحسين خطط الاستجابة للاختراقات بشكل دوري.

٦ - متى يجب على المراقب إخطار شؤون الحوكمة والضمان السيبراني وحماية البيانات والأفراد بحدوث اختراق للبيانات الشخصية؟

تتطلب المادة ١٤ بموجب قانون حماية خصوصية البيانات الشخصية (PDPPL) من المراقب إخطار شؤون الحوكمة والضمان السيبراني والأفراد بحدوث اختراق إذا كان الاختراق قد يتسبب في ضرر لخصوصية الأفراد أو حماية خصوصية بياناتهم الشخصية.

يجب على المراقب إخطار شؤون الحوكمة والضمان السيبراني والأفراد باختراقات البيانات الشخصية في غضون ٧٢ ساعة من علمه بها.

المراقب هو المسؤول عن تقييم ما إذا كان الاختراق قد يتسبب في ضرر جسيم لخصوصية الأفراد أو حماية خصوصية البيانات الشخصية. عندما يصبح المراقب على دراية باختراق البيانات الشخصية، يجب أن يعمل على احتواء الاختراق بالتوازي مع تقييم تأثيره المحتمل على الأفراد.

ماذا لو كان المراقب على علم باختراق البيانات الشخصية ولكن ليس لديه جميع المعلومات ذات الصلة؟

لن يكون من الممكن دائمًا التحقيق في اختراق البيانات الشخصية بالكامل في غضون ٧٢ ساعة لفهم طبيعة وظروف الاختراق أو تحديد الإجراءات المطلوبة لحماية الأفراد من الضرر الخطير لخصوصية الأفراد أو حماية خصوصية بياناتهم الشخصية. ماذا لو لم تتوفر لدينا جميع المعلومات المطلوبة حتى الآن؟

يجب على المراقب إخطار شؤون الحوكمة والضمان السيبراني بالمعلومات المتاحة لديهم خلال ٧٢ ساعة إذا تبيّن له أنه من المحتمل أن يتسبب في أضرار للأفراد. كما يجب على المراقب تضمين أسباب عدم قدرته على تقديم جميع المعلومات المطلوبة في غضون ٧٢ ساعة وتحديد كيف ومتى سيتمكن من تقديم المزيد من المعلومات.

يجب على المراقب بذل كل الجهود المناسبة لتسريع التحقيق في الاختراق كضمان توفير الموارد المطلوبة لفريق التحقيق.

كيف يقيّم المراقب ما إذا كان اختراق البيانات الشخصية يمكن أن يتسبب في أضرار جسيمة للأفراد؟

في تقييم الضرر الناجم عن اختراق البيانات الشخصية، يجب على المراقب أن يولي اهتماماً خاصاً للعواقب السلبية على الأفراد المتضررين من الاختراق. يمكن أن يكون للاختراق مجموعة من الآثار السلبية على الأفراد، بما في ذلك الاضطراب المعنوى والأضرار المادية والجسدية. أمثلة على المعالجة التي، عندما تتأثر بالاختراق، يمكن أن تزيد من شدة الضرر الذي يلحق بالأفراد:

- معالجة أي بيانات شخصية ذات طبيعة خاصة؛
- استخدام تقنية مبتكرة جديدة أو تقنية مستخدمة بطريقة جديدة؛
- تطبيق عملية صنع قرار آلية تؤدي إلى قرار يقيد وصول الفرد إلى منتج أو خدمة أو فرصة أو فائدة، أي القرارات التي يتخذها الكمبيوتر أو النظام التقني دون تدخل بشري؛
- جمع البيانات الشخصية عبر أطراف ثالثة بدلاً من الأفراد مباشرة؛
- تتبع الأفراد أو مراقبة سلوكهم (مثل كاميرات المراقبة CCTV ، وأنماط التصفح عبر الإنترنت ، وأنظمة تحديد المواقع GPS)؛
- إجراء نقل البيانات الشخصية عبر الحدود، أي نقل البيانات الشخصية خارج دولة قطر؛
- استخدام البيانات الشخصية لاستهداف التسويق الموجه للأفراد؛

- تسويق أو توفير السلع أو الخدمات للأطفال (مثل إرسال رسائل بريد إلكتروني ترويجية للأطفال) دون موافقة الوالدين؛
- إجراء نشاط جديد لمعالجة البيانات الشخصية للقطاع الذي يعمل به المراقب.

من الضروري أن يكون لدى المراقب أنشطة قائمة لإجراء تقييم للضرر الناجم عن اختراق البيانات الشخصية على الأفراد في الوقت المناسب وبشكل متين وفعّال. إذا قام المراقب بالامتثال للمادتين (١) ١١ و ١٣ من قانون حماية خصوصية البيانات الشخصية (PDPPL) من خلال إجراء عمليات تحليل تأثير حماية خصوصية البيانات (DPIA) على أنشطة المعالجة الخاصة به، فبالتالي سيكون لديه تقييمات للأضرار المحتملة التي يمكن أن يسببها الاختراق على مستوى نشاط المعالجة. يعد هذا الإجراء بمثابة مساهمة قيمة لأي تقييم لاختراقات البيانات الشخصية.

لمزيد من المعلومات حول ما قد يتسبب في أضرار جسيمة للأفراد، يرجى الاطّلاع إلى المبادئ التوجيهية فيما يخص تحليل تأثير حماية خصوصية البيانات (DPIAs) للمخاطبين بأحكام القانون.

يتحكم المراقب في اتخاذ القرار ويجب أن يقوم بتوثيق الأساس المنطقي لقراره بشأن ما إذا كان يجب الإبلاغ عن الاختراقات إلى شؤون الحوكمة والضمان السيبراني والأفراد أم لا. هذا مهم بشكل خاص إذا قرر المراقب عدم الإبلاغ عن الاختراق.

إذا قام المراقب باتخاذ القرار بشكل غير صحيح على أن الاختراق لا يمكن أن يسبب ضررًا جسيماً بحيث يكون هناك احتمالية لحدوث ذلك الخطر وبعد ذلك يقرر المراقب عدم إبلاغ شؤون الحوكمة والضمان السيبراني أو الأفراد في الوقت المناسب، فقد يتبين أن المراقب لم يمتثل لقانون حماية خصوصية البيانات الشخصية (PDPPL).

إذا وجد أن المراقب في حالة عدم امتثال لمتطلبات الإبلاغ عن الاختراقات بموجب المادة ١٤، فقد يترتب على المراقب عقوبة بموجب المادة ٢٣ من قانون حماية خصوصية البيانات الشخصية (PDPPL).

٧ - كيف يجب على المراقب إخطار شؤون الحوكمة والضمان السيبراني؟

يجب أن يقوم المراقب بإخطار شؤون الحوكمة والضمان السيبراني عبر صفحة إخطار الاختراقات على الموقع الالكتروني لشؤون الحوكمة والضمان السيبراني باستخدام نموذج إخطار الاختراقات.

يجب أن يشمل إخطار الاختراقات النقاط التالية:

- وصف طبيعة اختراق البيانات الشخصية، بما في ذلك، حيثما أمكن، الفئات والأعداد التقريبية للأفراد المعنيين والفئات والعدد التقريبي لسجلات البيانات الشخصية المعنية؛
- توفير معلومات حول اسم وبيانات الاتصال بجهة الاتصال الرئيسية للشركة فيما يخص المسائل المتعلقة بحماية خصوصية البيانات الشخصية أو جهة اتصال أخرى حيث يمكن الحصول على مزيد من المعلومات؛
- وصف العواقب والآثار المحتملة لاختراق البيانات الشخصية؛
- وصف الإجراءات المتخذة أو المقترح اتخاذها من قبل المراقب لمعالجة اختراق البيانات الشخصية، بما في ذلك، عند الاقتضاء، إجراءات للتخفيف من آثار الاختراق السلبية المحتملة.

إذا لم يقم المراقب بإبلاغ شؤون الحوكمة والضمان السيبراني عن اختراق البيانات الشخصية وأصبحت شؤون الحوكمة والضمان السيبراني في وقت لاحق على علم بالاختراق من خلال مصدر آخر ، فمن المحتمل أن يؤدي هذا إلى إجراء تحقيق من قبل شؤون الحوكمة والضمان السيبراني.

٨ - كيف يجب على المراقب إخطار الأفراد؟

يجب أن يتم الاتصال بالفرد بشكل مباشر وأن يتم وصف الحالة بلغة واضحة وصريحة عن طبيعة اختراق البيانات الشخصية حيث يجب أن يتضمن الاتصال المعلومات التالية كحد أدنى:

- اسم وبيانات الاتصال بمسؤول حماية خصوصية البيانات أو جهة اتصال أخرى لدى المراقب حيث يمكن الحصول على مزيد من المعلومات حول اختراق البيانات الشخصية؛
- وصف العواقب والآثار المحتملة لاختراق البيانات الشخصية؛
- وصف الإجراءات المتخذة أو المقترح اتخاذها من قبل المراقب لمعالجة اختراق البيانات الشخصية، بما في ذلك، عند الاقتضاء، إجراءات للتخفيف من آثار الاختراق السلبية المحتملة.

يكون إخطار الأفراد المتضررين مهمًا بشكل خاص عندما يمكن أن يتسبب الاختراق في إلحاق ضرر جسيم بخصوصية الأفراد المتضررين أو حماية خصوصية بياناتهم الشخصية.

يتحكم المراقب في اتخاذ القرارات ويجب عليه توثيق الأساس المنطقي لقراره بشأن ما إذا كان يجب إبلاغ الأفراد المتأثرين بالاختراق يتعلق ببياناتهم الشخصية أم لا. هذا مهم بشكل خاص إذا قرر المراقب عدم الإبلاغ عن الاختراق.

قد يرغب المراقب في العمل مع شؤون الحوكمة والضمان السيبراني قبل إخطار الأفراد باختراق البيانات الشخصية للتشاور حول طريقة ومحتوى التواصل.

٩ - ما الذي سيتم إجراؤه من قبل شؤون الحوكمة والضمان السيبراني بعد قيام المراقب بإخطارها باختراق للبيانات الشخصية؟

بمجرد أن يقوم المراقب بإخطار شؤون الحوكمة والضمان السيبراني ، قد تقوم شؤون الحوكمة والضمان السيبراني بإجراء أي من النقاط التالية أو جميعها:

تحديد وقائع مختلفة مرتبطة بالاختراق

قد يشمل ذلك تحديد التالي:

- كيف حدث اختراق البيانات الشخصية؛
- متى حدث اختراق البيانات الشخصية؛
- متى أصبح المراقب على علم بالاختراق؛
- متى احتوى المراقب الخرق؛
- ما هي أقسام العمل التي تأثرت بالاختراق.

تحديد طبيعة البيانات المعرضة للخطر

قد تتضمن تفاصيل البيانات المعرضة للخطر التالي:

- فئات أو طبيعة البيانات الشخصية المخترقة؛
- مدى البيانات الشخصية المخترقة؛
- موقع البيانات الشخصية المخترقة؛
- الفئات وعدد الأفراد المتضررين؛
- تفاصيل عن أي تأثير سلبي على الأفراد.

تحديد وتقييم الاحتياطات التي قام المراقب بوضعها لمنع الاختراقات

أمثلة على أدلة الاحتياطات التي تتوقع شؤون الحوكمة والضمان السيبراني تطبيقها تشمل ولا تقتصر على:

- سياسة لحماية خصوصية البيانات الشخصية؛
- سياسة أمن المعلومات؛
- تفاصيل الاحتياطات الفنية لمنع الخرق مثل التشفير وجدار الحماية (Firewall) وما إلى ذلك؛
- دليل على تدريب الموظفين الإلزامي الدوري حول مواضيع حماية خصوصية البيانات ومنع الاختراقات.

التحقيق في مشاركة أطراف ثالثة خارجية إن أمكن

قد يشمل ذلك تقييم التالي:

- الاتفاقية التعاقدية القائمة بين المراقب والأطراف الثالثة الخارجية ذات الصلة؛
- مدى تحقق المراقب من احتياطات المعالج وامتثال المعالج لتعليمات المراقب؛
- ما إذا كان المراقب يدرك كيفية حفظ البيانات ومعالجتها؛
- نهج المراقب في الإجراءات الاستقصائية فيما يتعلق بالمعالج وأي معالج من الباطن؟

مراجعة أنشطة الإصلاح والإخطار الخاصة بالمراقب

قد يشمل ذلك تقييم التالي:

- الخطوات التي اتخذها المراقب لاحتواء الاختراق والتخفيف من أي خطر على خصوصية الأفراد أو حماية خصوصية بياناتهم الشخصية؛
- توقيت ومدى فعالية أي تقييمات للضرر الذي يلحق بالأفراد بسبب الاختراق؛
- توقيت وطبيعة الإخطار الموجه إلى شؤون الحوكمة والضمان السيبراني ؛
- توقيت وطبيعة أي إخطارات للأفراد؛
- تفاصيل أي شكاوى مقدمة من الأفراد المتضررين.

١٠ - ما الذي يجب أن يفعله المراقب بعد إخطار شؤون الحوكمة والضمان السيبراني و / أو الأفراد باختراق البيانات الشخصية؟

يجب أن يستمر المراقب في العمل من أجل احتواء وحل اختراق البيانات الشخصية وفقًا لإجراءاته الداخلية. وفي نفس الوقت، يجب على المراقب التأكد من توثيق الاختراق بشكل فعّال والاستعداد لأي نشاط متزايد محتمل للتعامل مع الطلبات والشكاوى المقدمة من الأفراد.

توثيق تفاصيل الاختراق والدروس المستفادة

يجب توثيق التفاصيل الكاملة لاختراق البيانات الشخصية وأي دروس مستفادة بشكل كامل بهدف تقليل احتمالية حدوث اختراق مماثل مرة أخرى في المستقبل. يتضمن هذا جمع كل وقائع الاختراق، وتقييم أي ضعف في الضوابط قد يتسبب في استمرار الاختراق أو حدوثه مرة أخرى، وتحديد أي حلول مطلوبة وتوثيق تفاصيل اختراق البيانات الشخصية من نقطة تحديده حتى الإغلاق. كما يجب أن يستمر المراقب في تقديم المعلومات إلى شؤون الحوكمة والضمان السيبراني والأفراد حسب الضرورة.

الاستعداد لزيادة الطلبات والشكاوى المتعلقة بحقوق الأفراد

كنتيجة لاختراقات البيانات الشخصية، قد تواجه المؤسسات حجمًا أكبر من الطلبات أو الشكاوى المتعلقة بحماية خصوصية البيانات الشخصية، خاصة فيما يتعلق بطلبات الوصول والمحو. يجب أن يكون لدى المراقب خطة طوارئ للتعامل مع إمكانية حدوث ذلك. من المهم أن يستمر المراقب في التعامل مع تلك الطلبات والشكاوى، إلى جانب أي عمل آخر تم إنشاؤه كمطلب لمعالجة الاختراق. كما يجب على المراقب أيضًا التفكير في كيفية إدارة التأثير على الأفراد، بما في ذلك شرح كيفية ملاحقتهم للتعويض إذا كان الموقف يتطلب ذلك.

١١ - ما الذي يجب أن يأخذه المراقب في الاعتبار فيما يتعلق باختراقات البيانات الشخصية؟

١١,١ - أن يكون المراقب على علم بمتطلبات إعداد التقارير في ولايات القضائية أخرى غير الولاية القضائية التي يعمل فيها

إذا كان المراقب يعمل ضمن نطاق قوانين أو لوائح البيانات الشخصية الدولية الأخرى (مثل اللائحة العامة لحماية البيانات في الاتحاد الأوروبي)، فيجب عليه مراعاة متطلبات الإبلاغ عن اختراقات البيانات الشخصية بموجب هذه القوانين وكذلك بموجب قانون حماية خصوصية البيانات الشخصية (PDPPL).

قد يرغب المراقب في العمل مع شؤون الحوكمة والضمان السيبراني قبل إخطار منظمات حماية خصوصية البيانات الدولية باختراق البيانات الشخصية للتشاور حول طريقة ومحتوى التواصل.

١١,٢ - أن يكون المراقب على دراية بالغرامات المحتملة التي قد يخضع لها المراقب ومعالج البيانات الذي يعمل معه

يحدد قانون حماية خصوصية البيانات الشخصية (PDPPL) الغرامات التي قد يتحملها المراقبون والمعالجين لدفعها إذا لم يلتزموا بالمتطلبات المتعلقة باختراقات البيانات الشخصية. يتم تحديد الغرامات المحتملة أدناه:

- قد يؤدي عدم إخطار شؤون الحوكمة والضمان السيبراني أو الأفراد عن اختراق البيانات الشخصية كما هو مطلوب إلى عقوبة تصل إلى ١,٠٠٠,٠٠٠ ريال قطري لكل مخالفة بموجب المادة ٢٣ من قانون حماية خصوصية البيانات الشخصية (PDPPL).
- قد يؤدي عدم اتخاذ الاحتياطات المناسبة التي تتناسب مع طبيعة وأهمية البيانات الشخصية إلى عقوبة تصل إلى ٥,٠٠٠,٠٠٠ ريال قطري لكل مخالفة بموجب المادة ٢٤ من قانون حماية خصوصية البيانات الشخصية (PDPPL).
- عدم قيام المعالج بإخبار المراقب باختراق البيانات الشخصية الذي قد يتسبب بحدوث خطر ما قد يؤدي إلى عقوبة مترتبة على المراقب تصل إلى ٥,٠٠٠,٠٠٠ ريال قطري لكل مخالفة بموجب المادة ٢٤ من قانون حماية خصوصية البيانات الشخصية (PDPPL).

نهاية الوثيقة