State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

تحليل تأثير حماية خصوصية البيانات - DPIA

PDPPL-02050206A

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: عام

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-02050203A	قائمة المراجعة لنظام إدارة حماية البيانات الموجهة للمخاطبين بأحكام القانون
PDPPL-02050208A	المبادئ التوجيهية لحماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً الموجهة للمخاطبين بأحكام القانون
PDPPL-02050204A	المبادئ التوجيهية للأسباب التي تسمح بمعالجة البيانات الشخصية الموجهة للمخاطبين بأحكام القانون
PDPPL-02050201A	المبادئ التوجيهية لأسس حماية خصوصية البيانات الموجهة للمخاطبين بأحكام القانون
PDPPL-02050502A	نموذج تحليل تأثير حماية خصوصية البيانات الموجه للمخاطبين بأحكام القانون

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 الوطني (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 الوطني والوكالة الوطنية للأمن السيبراني كمصدر للوثيقة ومالك لوثيقة " المبادئ التوجيهية لتحليل تأثير حماية خصوصية البيانات الموجهة للمخاطبين بأحكام القانون".

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

لا يعتبر الإذن المقدم من قبل شؤون الحوكمة والضمان السيبراني الوطني 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 لاتنسب 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 الوطني مخولة من قبل الوكالة الوطنية للأمن السيبراني باعتبارها هي 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 الوطني 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 الوطني وأي قرارات وزارية ذات صلة.

قائمة المحتويات

١ – النقاط الرئيسية

- الغرض من هذا الدليل هو شرح متطلبات المراقب لإجراء تحليلات تأثير حماية خصوصية البيانات (DPIA) قبل معالجة البيانات الشخصية بموجب المادة ١١,١ من قانون حماية خصوصية البيانات الشخصية (PDPPL).
- تحليل تأثير حماية خصوصية البيانات هي عملية تقييم لتحديد مخاطر معالجة البيانات الشخصية للأفراد وتخفيف مخاطر معالجة البيانات الشخصية إلى مستوى مقبول.
- يعد تحليل تأثير حماية خصوصية البيانات (DPIA) عنصراً رئيسياً لنظام إدارة البيانات الشخصية (PDMS) ويساعد على إظهار حماية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً.
- يجب على مراقب البيانات تنفيذ عملية لإدارة تحليل تأثير حماية خصوصية البيانات (DPIA) وتقديم التدريب للموظفين حول كيفية إجرائها.
- يجب على مراقب البيانات إجراء تحليل تأثير حماية خصوصية البيانات قبل القيام بمعالجة البيانات الشخصية بطرق جديدة أو قبل إجراء تغيير جذري على نشاط المعالجة الحالي. كما يجب على مراقب البيانات تضمين أي إجراءات للتخفيف من المخاطر في خطة المشروع للمبادرة للتأكد من تطبيق هذه الإجراءات.
- بموجب قانون حماية خصوصية البيانات الشخصية (PDPPL)، المراقب هو الجهة المسؤولة عن كيفية معالجة البيانات الشخصية وتقليل المخاطر على الأفراد وبياناتهم. يُعد الاحتفاظ بسجل لإجراءات تحليل تأثير حماية خصوصية البيانات (DPIAs) طريقة مهمة لإثبات الامتثال.

٢ - المقدمة

يتطلب قانون حماية خصوصية البيانات الشخصية (PDPPL) من مراقب البيانات عمل تقييماً لإجراءات حماية خصوصية البيانات قبل البدء في عملية معالجة بيانات شخصية جديدة. يُعرف هذا التقييم باسم تحليل تأثير حماية خصوصية البيانات (DPIA). تشكل معالجة البيانات الشخصية مخاطر على الأفراد وبياناتهم الشخصية حيث تمكّنكم عملية تحليل تأثير حماية خصوصية البيانات من تحديد هذه المخاطر وتنفيذ خطة للتخفيف منها. يعتبر إجراء تحليل تأثير حماية خصوصية البيانات (DPIA) عنصراً رئيسيًا لنظام إدارة البيانات الشخصية. للمزيد من المعلومات حول نظام إدارة البيانات الشخصية، يرجى الاطّلاع على وثيقة نظام إدارة حماية البيانات - قائمة المراجعة للمخاطبين بأحكام القانون.

يمكن الاطّلاع على متطلبات مراجعة تدابير حماية الخصوصية قبل المعالجة في المادة ١١ من قانون حماية خصوصية البيانات الشخصية (PDPPL) ويمكن العثور على متطلبات تنفيذ تدابير للتخفيف من مخاطر المعالجة في المادة ١٣.

٣ - ماذا ينص قانون حماية خصوصية البيانات الشخصية عن تحليل تأثير حماية خصوصية البيانات (DPIA)؟

تنص المادة ١١,١ من قانون حماية خصوصية البيانات الشخصية (PDPPL) على ما يلي:

"يجب على المراقب مراجعة إجراءات حماية الخصوصية قبل إدراج عمليات معالجة جديدة".

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

قبل معالجة البيانات الشخصية، يجب على مراقب البيانات إجراء النقاط التالي:

- تحديد المخاطر التي يتعرض لها الأفراد من خلال نشاط معالجة البيانات الشخصية المقترح؛
- مراجعة التدابير المعمول بها لحماية البيانات الشخصية؛
- تقييم التأثير المحتمل على الأفراد لأي نشاط معالجة بيانات شخصية جديد.

يجب على مراقب البيانات وضع تدابير إدارية وفنية ومالية للحفاظ على أمان البيانات الشخصية وخصوصيتها والتأكد من أن معالجة البيانات ستكون متماثلة مع أحكام قانون حماية البيانات الشخصية (PDPPL) التي تتناسب مع طبيعة وأهمية البيانات الشخصية الجاري معالجتها والمخاطر المرتبطة بها.

يُظهر إجراء تحليل تأثير حماية خصوصية البيانات (DPIA) فعّال الامتثال لقانون حماية خصوصية البيانات الشخصية (PDPPL)، مما يوفر دليلاً بأن مراقب البيانات قد قام بإجراء المراجعة المطلوبة بموجب المادة ١١,١ وحدد الاحتياطات المناسبة التي سيتم وضعها بموجب المادة (٣) ٨ و١٣.

٤ - ما هو تحليل تأثير حماية خصوصية البيانات (DPIA)؟

تحليل تأثير حماية خصوصية البيانات (DPIA) هو تقييم لتحديد مخاطر معالجة البيانات الشخصية للأفراد وتقليل مخاطر المعالجة إلى مستوى مقبول. يعتبر تحليل تأثير حماية خصوصية البيانات مشابه لتقييم المخاطر، ويجب أن يتم إجراءه باستمرار بطريقة موحدة عبر مؤسستكم.

٤,١ - ما الذي يتضمنه تحليل تأثير حماية خصوصية البيانات (DPIA)؟

تحليل تأثير حماية خصوصية البيانات (DPIA):

- يحدد تفاصيل نشاط المعالجة بما في ذلك:
  - كيفية معالجة البيانات الشخصية؛
  - لماذا تتم معالجة البيانات الشخصية؛
  - من هو المسؤول داخل منظمتكم.
- يحدد مخاطر المعالجة للأفراد واحتمالية عدم الامتثال على المنظمة؛
- يحدد مخفّفات للمخاطر المحددة؛
- يصيغ قرارًا بشأن إجراءات الحد التي تتناسب مع المخاطر المطروحة ومبررًا لأي إجراءات يتم تحديدها ولكن لم يتم تنفيذها؛
- يحدد الحاجة إلى التشاور مع شؤون الحوكمة والضمان السيبراني الوطني إذا لم يكن بالإمكان تخفيف المخاطر بشكل مناسب؛
- الحصول على الموافقة من الشخص/ أو الأشخاص المسؤولين المعنيين على تقييم تحليل تأثير حماية خصوصية البيانات وخطة تنفيذ إجراءات التخفيف المحددة.

٤,٢ - ما هي أهم مخرجات تحليل تأثير حماية خصوصية البيانات (DPIA)؟

المخرجات الرئيسية لتحليل تأثير حماية خصوصية البيانات:

- يوجد لدى مراقب البيانات خطة إجراءات قابلة للتطبيق لتقليل خطر الضرر الجسيم الذي قد يسببه إجراء معالجة البيانات الشخصية (DPIA) إلى مستوى مناسب. هذه الاحتياطات ليست حصرية بشكل متبادل ويمكن أن تكون:
  - **إدارية:** على سبيل المثال سياسة أو عملية أو تدريب أو حوكمة و / أو فصل اختصاصات جديدة أو محدثة.

- **التقنية:** على سبيل المثال، التشفير، إخفاء الهوية، الاسم المستعار و / أو ضوابط الوصول.
- **المالية:** على سبيل المثال الاستثمار في خدمة أو تكنولوجيا و / أو تأمين.

- لدى مراقب البيانات تأكيد موثّق على وجود تدابير مناسبة لحماية البيانات الشخصية التي تتم معالجتها ويمكن أن يبرر إجراء تحليلاته بأن مثل هذه الإجراءات تقلل بدرجة كافية من خطر حدوث ضرر جسيم.
- يمكن لمراقب البيانات تقييم احتمال حدوث ضرر جسيم بشكل سريع في حالة اختراق البيانات الشخصية لأن لدى مراقب البيانات سجل إجراء تحليل تأثير حماية خصوصية البيانات (DPIA).
- يوجد لدى مراقب البيانات سجل لصنع القرار الخاص به لإثبات الامتثال للمادتين ١١ و١٣ تماشياً مع مبدأ المساءلة.
- يوجد لدى مراقب البيانات المعلومات المطلوبة للتشاور مع شؤون الحوكمة والضمان السيبراني الوطني إذا لم يتمكن من التخفيف من مخاطر المعالجة بشكل كاف.

٥ - متى يجب على مراقب البيانات إجراء تحليل تأثير حماية خصوصية البيانات (DPIA)؟

يجب على مراقب البيانات القيام بإجراء تحليل تأثير حماية خصوصية البيانات (DPIA) قبل بدء أي نشاط جديد يتضمن معالجة البيانات الشخصية أو قبل إجراء تغييرات كبيرة على نشاط موجود. من الجيد مراجعة تحليلات تأثير حماية خصوصية البيانات (DPIAs) بشكل دوري للتأكد من أنها محدثة.

تعتبر تحليلات تأثير حماية البيانات (DPIAs) مهمة بشكل خاص عند تنفيذ نشاط معالجة قد يسبب ضررًا جسيماً للأفراد الذين تتم معالجة بياناتهم الشخصية. هذا يعني أنه على الرغم من أن مراقب البيانات لم يقم بعد بتقييم مستوى المخاطر بالتفصيل، إلا أنه بحاجة إلى فحص العوامل التي تشير إلى احتمال وجود تأثير واسع النطاق أو جسيم على الأفراد.

أمثلة على الأنشطة التي قد تؤدي إلى إجراء تحليل تأثير حماية خصوصية البيانات (DPIA) هي:

- تطبيق أو تحديث التكنولوجيا.
- التغييرات على العمليات القائمة.
- التغييرات على المنتجات أو الخدمات.

يتم توفير المزيد من الأمثلة في الملحق.

يجب على مراقب البيانات أخذ القرار فيما إذا كان تحليل تأثير حماية خصوصية البيانات (DPIA) مطلوب بما يتماشى مع مبدأ المساءلة. إذا لم يقم بإجراء تحليل تأثير حماية خصوصية البيانات (DPIA) حيث يُطلب منه القيام بذلك بوضوح، فقد يكون مراقب البيانات مسؤول عن دفع غرامة قدرها ١,٠٠٠,٠٠٠ ريال قطري بموجب المادة ٢٣ من قانون حماية خصوصية البيانات الشخصية (PDPPL).

يمكن أن يغطي تحليل تأثير حماية خصوصية البيانات (DPIA) عملية معالجة واحدة أو مجموعة من عمليات المعالجة المماثلة. قد يتمكن المراقب حتى من الاعتماد على تحليل تأثير حماية خصوصية البيانات (DPIA) الحالي إذا كان يغطي عملية معالجة مماثلة بمخاطر مماثلة. مراقب البيانات هو المسؤول عن تبرير مدى تشابه أنشطة المعالجة وما إذا كان الاعتماد على تحليل تأثير حماية خصوصية البيانات (DPIA) الحالي مناسبًا.

عند قيام مراقب البيانات باستخدام معالجًا للبيانات كطرفاً ثالثاً، قد يتمكن من استخدام تحليل تأثير حماية خصوصية البيانات (DPIA) التي قام الطرف الثالث بإجرائه لتزويد تحليل تأثير حماية خصوصية البيانات (DPIA) الخاص بمراقب البيانات بالمعلومات. على سبيل المثال، مراقب بيانات يشرك مقدم خدمات لتقديم طلب تطبيق بريد مباشر يطلب نسخة من تحليل تأثير حماية خصوصية البيانات (DPIA) التي أجراها مزود الخدمات عند إعداد التطبيق لتوفير معلومات عن المخاطر وإجراءات التخفيف المحتملة التي يمكن أن يضعها مراقب البيانات.

٥,١ - ما المقصود ب "احتمال حدوث ضرر جسيم؟

لا يحدد قانون حماية خصوصية البيانات الشخصية (PDPPL) ما تعنيه عبارة "قد تسبب ضررًا جسيمًا". قبل معالجة البيانات الشخصية، يجب على مراقب البيانات تقييم ما إذا كان يمكن أن يحدث ضرراً جسيماً لخصوصية الأفراد أو بياناتهم الشخصية. ينص قانون حماية خصوصية البيانات الشخصية (PDPPL) بشكل واضح على طريقتين محددتين للمعالجة قد تتسببان في أضرار جسيمة. الطريقتين هم:

- نقل البيانات الشخصية خارج دولة قطر، المعروفة باسم نقل البيانات عبر الحدود؛
- معالجة البيانات الشخصية ذات الطبيعة الخاصة، وفئات معينة من البيانات الشخصية تُعرف أيضًا باسم البيانات الشخصية ذات الطبيعة الخاصة.

يجب على مراقب البيانات الأخذ في الاعتبار التأثير المحتمل على الأفراد والضرر الذي قد تسببه معالجة البيانات الشخصية - سواء كان جسديًا أو عاطفيًا أو ماديًا. على وجه الخصوص، يمكن أن تكون أمثلة مخاطر الضرر التي يمكن لمعالجة البيانات الشخصية المساهمة بحدوثها:

- عدم القدرة على ممارسة حقوق الأفراد؛
- عدم القدرة على الوصول إلى الخدمات أو الفرص؛
- فقدان السيطرة على استخدام البيانات الشخصية؛
- التمييز؛
- سرقة الهوية والاحتيال؛
- الخسائر المالية؛
- إلحاق الضرر بالسمعة؛
- أذى جسدي؛
- فقدان السرية؛
- إعادة تحديد البيانات المستعارة؛
- أي ضرر أو تأثير اقتصادي أو اجتماعي جسيم آخر.

الضرر الجسيم لا يقتصر على الضرر الذي يحدث في حالة حدوث خرق. يمكن أن يكون مرتبطًا بمعالجة البيانات الشخصية بشكل غير عادل مما قد يؤدي إلى اتخاذ قرارات بشأن الأفراد التي لا تتماشى مع مبادئ المعالجة وتؤثر سلبًا على حقوق الأفراد.

٥,٢ - كيف يمكن أن يفيد تحليل تأثير حماية خصوصية البيانات في حالة حدوث اختراق للبيانات الشخصية؟

يتطلب قانون حماية خصوصية البيانات الشخصية (PDPPL) أيضًا من مراقب البيانات إخطار الأفراد و شؤون الحوكمة والضمان السيبراني الوطني بأي اختراق "قد يتسبب في أضرار جسيمة" لخصوصية الأفراد أو بياناتهم الشخصية. يمكن أن يكون هذا الاختراق امنياً، على سبيل المثال، سرقة البيانات الشخصية ولكنه قد يكون أيضًا خرقًا للمبادئ، على سبيل المثال، عدم معالجة البيانات الشخصية بشفافية من خلال عدم تقديم إشعار خصوصية مناسب.

في حالة حدوث اختراق للبيانات الشخصية، ستمكّن قاعدة بيانات تحليلات تأثير حماية خصوصية البيانات (DPIA) مراقب البيانات من تحديد ما إذا كان من المحتمل أن يكون الاختراق قد تسبب في أضرار جسيمة للأفراد مساندة عملية اتخاذ القرارات المتعلقة بالاستجابة لخروقات البيانات الشخصية، بما في ذلك ما إذا كانت الإخطارات مطلوبة. على هذا النحو، يعتبر تحليل تأثير حماية خصوصية البيانات الشخصية (DPIA) جزءًا أساسيًا من الاستعداد لخروقات البيانات الشخصية لدى مراقب البيانات الشخصية.

٥,٣ - كيف يمكن لمراقب البيانات تقييم ما إذا كان نشاط المعالجة "قد يتسبب في حدوث أضرار جسيمة"؟

يجب إجراء تحليل تأثير حماية خصوصية البيانات (DPIA) لأي نشاط معالجة جديد. بالنسبة لأنشطة المعالجة الحالية، من الممارسات الجيدة إجراء تحليل تأثير حماية خصوصية البيانات (DPIA) لتقييم أي مخاطر جسيمة تحتاج للتخفيف قد تطرأ على خصوصية الأفراد وبياناتهم الشخصية. يجب على مراقب البيانات القيام بإجراء تحليل تأثير حماية خصوصية البيانات (DPIA) لأي نشاط معالجة "قد يتسبب في أضرار جسيمة".

من أجل تحديد ما إذا كان تحليل تأثير حماية خصوصية البيانات (DPIA) ضروري أم لا، يجب على مراقب البيانات إصدار حكم عالي المستوى لتحديد ما إذا كانت هناك خصائص تشير إلى احتمال حدوث ضرر جسيم. كما يجب على مراقب البيانات أيضاً متابعة أي مؤشرات تدل على أنه بحاجة إلى القيام بإجراء تحليل تأثير حماية خصوصية البيانات (DPIA) للنظر في الخطر (بما في ذلك احتمال وشدة الضرر المحتمل) بمزيد من التفصيل.

لتحديد ما إذا كانت المعالجة الخاصة بمراقب البيانات "قد تسبب ضررًا جسيماً" وستتطلب تحليل تأثير حماية خصوصية البيانات (DPIA)، يجب الأخذ في الاعتبار ما إذا كان نشاط المعالجة الخاص به يتضمن واحدًا أو أكثر من النقاط التالية:

- معالجة أي بيانات شخصية ذات طبيعة خاصة.
- استخدام تقنية مبتكرة جديدة أو تقنية موجودة بطريقة جديدة.
- تنفيذ عملية صنع قرار آلية مؤتمتة إلى قرار يقيد وصول الفرد إلى منتج أو خدمة أو فرصة أو فائدة ، أي القرارات التي يتخذها الحاسب الآلي دون تدخل بشري.
- جمع البيانات الشخصية عبر أطراف ثالثة بدلاً من الأفراد مباشرة.

- تتبع الأفراد أو مراقبة سلوكهم (مثل CCTV، وأنماط التصفح عبر الإنترنت، وتتبع موقع GPS).
- القيام بنقل البيانات الشخصية عبر الحدود، أي نقل البيانات الشخصية خارج دولة قطر.
- معالجة البيانات الشخصية للموظفين.
- استخدام البيانات الشخصية لاستهداف التسويق المباشر للأفراد.
- تسويق أو توفير السلع أو الخدمات للأطفال (مثل إرسال رسائل بريد إلكتروني ترويجية للأطفال) دون موافقة الوالدين.
- تنفيذ نشاط معالجة جديد في مجالكم أو قطاعكم.

بالارتكاز إلى أفضل الممارسات، يجب على مراقب البيانات مراجعة تحليل تأثير حماية خصوصية البيانات (DPIA) بشكل مستمر وإعادة تقييمه بانتظام. لذلك، من المتوقع أن يقرر مراقب البيانات إجراء تحليلات تأثير حماية خصوصية البيانات (DPIA) على أنشطة المعالجة الحالية الخاصة به، بناءً على المعايير المذكورة أعلاه، كجزء من التزاماته بما يتماشى مع مبدأ المساءلة.

في النهاية، يرجع الأمر إلى مراقب البيانات في تحديد ما إذا كانت المعالجة الخاصة به قد تسبب ضررًا جسيماً للأفراد، مع مراعاة البيانات الشخصية التي تمت معالجتها وطبيعة المعالجة. إذا كان لدى المراقب أي شك، فيجب إجراء تحليل تأثير حماية خصوصية البيانات لضمان الامتثال وإثبات أفضل الممارسات.

بالنسبة للأنشطة التي قد لا تسبب "ضررًا جسيمًا"، يجب على مراقب البيانات توثيق الأدلة على أنه قد أخذتم في الاعتبار الحاجة إلى تحليل تأثير حماية خصوصية البيانات (DPIA). يعتبر توثيق هذا القرار بمثابة دليل على أن مخاطر الخصوصية يتم أخذها في الاعتبار قبل تنفيذ نشاط معالجة يتماشى مع حماية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً. يرجى الاطّلاع على المبادئ التوجيهية لحماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً للمخاطبين بأحكام القانون.

٦ - كيف يقوم مراقب البيانات بإجراء تحليل تأثير حماية خصوصية البيانات (DPIA)؟

على مستوى عالٍ، يجب على تحليل تأثير حماية خصوصية البيانات (DPIA) الخاصة بالمراقب تضمين التالي:

- وصف طبيعة وأهمية البيانات الشخصية الضرورية لنشاط المعالجة هذا، بما في ذلك على سبيل المثال لا الحصر الكمية وطبيعة البيانات الشخصية؛
- تحديد مخاطر التي قد تسبب أضرار جسيمة للأفراد؛
- وصف حجم ونطاق عمليات المراقب والوسائل المالية مؤسسة المراقب؛
- تقييم ما إذا كان الغرض من المعالجة يمكن تحقيقه باستخدام أي وسيلة أخرى تتضمن معالجة بيانات شخصية أقل؛
- النظر في أحدث الوظائف والعمليات والضوابط والأنظمة والإجراءات وغيرها من التدابير الحالية لحماية البيانات الشخصية؛
- إصدار حكم بشأن التدابير لحماية البيانات الشخصية التي تتناسب مع طبيعة نشاط المعالجة والمخاطر التي قد تسبب أضرار جسيمة للأفراد وتخفيف المخاطر التي تتضمنها بشكل كاف.

يجب توثيق تحليلات تأثير حماية خصوصية البيانات (DPIA) الخاصة بمراقب البيانات بلغة واضحة وموجزة مع مراعاة الأشخاص الغير متخصصين، مع شرح أي مصطلحات فنية ومختصرات يتم استخدامها.

لقد قدمنا نموذجًا لتحليل تأثير حماية خصوصية البيانات (DPIA) يمكن لمراقب البيانات استخدامه لإجراء عمليات التحليل. يمكن لمراقب البيانات استخدام النموذج المقدم أو إعداد نموذجه الخاص. من المفترض أن يكون تحليل تأثير حماية خصوصية البيانات مرن وقابل للتطوير.

- إذا كانت مؤسسة مراقب البيانات ضمن فئات المؤسسات الصغيرة ذات أنشطة معالجة بسيطة نسبيًا، فمن المحتمل ألا تكون تفاصيل تقييم تأثير حماية البيانات متضمنة لتفاصيل كثيرة.
- إذا كانت شركة مراقب البيانات ضمن فئات الشركات التي تعمل على مستوى العالم التي تقوم بمعالجة البيانات الشخصية بطريقة معقدة باستخدام أحدث التقنيات، فمن المحتمل أن يحتاج المراقب إلى التفكير في تأثير هذه المعالجة بعمق ليتمكن من التأكد من أن تدابير حماية الخصوصية الخاصة به تتناسب مع خطر الضرر الجسيم.

٦,١ - من الذي يجب أن يشارك في استكمال إجراء تحليل تأثير حماية خصوصية البيانات (DPIA)؟

يجب استكمال تحليل تأثير حماية خصوصية البيانات (DPIA) بواسطة شخص أو مجموعة من الأشخاص لديهم ما يلي:

- معرفة تفصيلية كافية عن نشاط المعالجة المقترح، غالبًا ما يتم توفير ذلك من قبل مالك العملية.

- فهم كاف لمتطلبات قانون حماية خصوصية البيانات الشخصية (PDPPL) ومفاهيم وممارسات حماية البيانات، وغالبًا ما يتم توفيرها من قبل مسؤول حماية البيانات أو سفير من القسم المعني.
- سلطة كافية للتوقيع على القرار الصادر بشأن ما إذا كانت الاحتياطات المناسبة تتناسب مع طبيعة نشاط المعالجة.

٧ - ما هي الخطوات لاستكمال إجراء تحليل تأثير حماية خصوصية البيانات (DPIA)؟

غالبًا ما يكمل مالك العملية أو المشروع أو فريق المشروع استمارة تحليل تأثير حماية خصوصية البيانات (DPIA) بالتشاور مع موظف مدرب على موضوع حماية البيانات.

يجب عليهم التشاور مع جميع أصحاب المصلحة المعنيين، داخليًا وفي أي طرف ثالث، للتأكد من أنهم يرصدون جميع المخاطر ذات الصلة الناشئة بسبب نشاط المعالجة، ولا سيما تلك التي قد تسبب ضررًا جسيماً.

يجب الموافقة على تحليل تأثير حماية خصوصية البيانات (DPIA) من قبل شخص لديه السلطة المناسبة للقيام بذلك وشخص لديه معرفة كافية بحماية البيانات، على سبيل المثال، رئيس القسم الذي يمتلك نشاط المعالجة ورئيس حماية البيانات.

لقد حددنا المجالات التي يجب أن يغطيها تحليل تأثير حماية خصوصية البيانات (DPIA) أدناه مع توجيهات بشأن المعلومات التي يجب تقديمها. تتماشى هذه الإرشادات مع الخانات الموجودة في نموذج استمارة تحليل تأثير حماية خصوصية البيانات (DPIA) وينبغي قراءتهما معًا.

٧,١ - تقديم تفاصيل ملكية العملية

يجب على مراقب البيانات تحديد من مالك نشاط المعالجة هذا داخل مؤسستكم. يجب أن يكون عبارة عن موظف أو دور أو قسم أو فريق واحد مسؤول عن القرارات اليومية المطلوبة لتشغيل العملية.

إنهم مسؤولون عن المعالجة ولكنك، بصفتك المراقب، تكون مسؤولاً في النهاية عن حماية البيانات الشخصية التي تتم معالجتها.

٧,٢ - القيام بتوثيق القرار حول ما إذا كانوا مراقب البيانات سيقومون بتنفيذ تحليل تأثير حماية خصوصية البيانات (DPIA) أم لا؟

يجب الاحتفاظ بسجل لقرارات مراقب البيانات بشأن ما إذا كان سيقوم بتنفيذ تحليل تأثير حماية خصوصية البيانات (DPIA) ومبررات قراره بما يتماشى مع مبدأ المساءلة. هذا مهم بشكل خاص عندما يقرر أن تحليل تأثير حماية خصوصية البيانات ليس ضروري. إذا كان متاحًا، إرفاق مستندات أخرى ذات صلة يمكن أن تساعد في توفير مبرر مثل خطة المشروع.

٧,٣ - تقديم تفاصيل عن نشاط المعالجة

يجب على مراقب البيانات تقديم شرح للهدف المقصود من مشروعه وصيغ المعالجة المتبعة. يجب أن تتضمن هذه التفاصيل توضيحاً لما يلي:

- ما سيتم معالجته - البيانات الشخصية التي سيتم معالجتها، بما في ذلك أي بيانات شخصية ذات طبيعة خاصة.
- من ستتم معالجة بياناته - الأفراد الذين ستتم معالجة بياناتهم الشخصية.

- كيف ستتم المعالجة - طبيعة المعالجة، على سبيل المثال، عدد المرات، الأنظمة المستخدمة، موقع معالجة البيانات، إلخ.
- سبب إجراء هذه المعالجة - الغرض من المعالجة (بما في ذلك الأسباب التي تسمح بمعالجة البيانات الشخصية). لمزيد من التفاصيل فيما يخص الأسباب التي تسمح بمعالجة البيانات الشخصية، يرجى الاطّلاع على المبادئ التوجيهية لأسباب التي تسمح بمعالجة البيانات الشخصية للمخاطبين بأحكام القانون.

٧,٤ - تقييم الضرورة والتناسب

مراقب البيانات هو المسؤول عن معالجة البيانات الشخصية وفقًا لمبادئ قانون حماية خصوصية البيانات الشخصية (PDPPL) بما في ذلك تقليل البيانات والتأكد من محدودية التخزين.

يجب على مراقب البيانات تقييم ما إذا كانت البيانات الشخصية التي سيتم جمعها ضرورية للغاية لتحقيق غرضهم المقصود، وتقييم "الضرورة"، وما إذا كان يمكنه تحقيق غرضه بشكل مناسب للمعالجة بطريقة أخرى أقل تدخلاً أو مرتبطة بالمخاطر، وتقييم "التناسب".

يجب على مراقب البيانات تضمين تفاصيل حول كيفية ضمان الامتثال لحماية خصوصية البيانات، وهي مقياس جيد الضرورة والتناسب. على وجه الخصوص، يجب على مراقب البيانات تضمين التفاصيل ذات الصلة بشأن:

- الغرض المشروع للمعالجة؛
- كيف سيمنعون توسع نطاق الوظيفة؛
- كيف سيقومون بضمان جودة البيانات؛
- كيف سيقومون بضمان تقليل البيانات؛
- كيف سيقومون بتوفير معلومات الخصوصية للأفراد؛
- كيف سيقومون بتطبيق ودعم حقوق الأفراد؛
- تدابير لضمان امتثال معالجة البيانات الخاصة بالمراقب؛
- ضمانات للتحويلات الدولية.

٧,٥ - إجراء تقييم للمخاطر وتحديد إجراءات تخفيف المخاطر

مراقب البيانات هم مسؤولون عن حماية البيانات الشخصية، للقيام بذلك، يجب عليهم تحديد وتسجيل المخاطر التي يشكلها نشاط المعالجة واحتمال وتأثير الضرر على خصوصية الأفراد والبيانات الشخصية.

تشمل المخاطر التي يحددها مراقب البيانات تلك التي يشكلها اختراق أمني يؤثر على البيانات الشخصية ولكن أيضًا المخاطر المتعلقة بتحكم اصحاب البيانات في بياناتهم الشخصية وخصوصيتهم، على سبيل المثال، عدم الامتثال لمبادئ حماية البيانات مثل تقليل البيانات والتأكد من محدودية الغرض.

بمجرد قيام مراقب البيانات بتحديد المخاطر، يجب اتخاذ القرار حول التدابير المناسبة اللازمة للتخفيف من تلك المخاطر. بالاضافة الى تحديد أشخاص مسؤولين من التأكيد أن هذه التدابير تم تنفيذها. عند الاقتضاء، قد يتم تضمين هذه التدابير في خطط الاستجابة للمخاطر كجزء من إطار المخاطر والضوابط الحالي للمراقب البيانات.

كما يجب على مراقب البيانات تحديد المخاطر المتبقية التي ستبقى بعد تنفيذ تدابير التخفيف الخاصة به. إذا كان هناك خطر كبير من حدوث ضرر جسيم لا يزال يتبع الإجراءات التي حددوها، فيجب على مراقب البيانات طلب الاستشارة من شؤون الحوكمة والضمان السيبراني الوطني حول كيفية المضي قدمًا.

٧,٦ - تقييم احتمال حدوث ضرر جسيم ضد التدابير المحددة

يجب أن تكونوا واثقين من أن الإجراءات التي تم تحديدها لحماية البيانات الشخصية التي تتم معالجتها تتناسب مع خطر حدوث ضرر جسيم لخصوصية الفرد أو بياناته الشخصية.

يجب أن تحددوا كيفية اتخاذ قرار التوازن الصحيح بين تدابير الحماية المناسبة والمخاطر التي يتعرض لها الأفراد مع مراعاة:

- أفضل الممارسات بما في ذلك أحدث التقنيات.
- تكاليف تنفيذ إجراءات الحماية المختلفة المتاحة.
- طبيعة ونطاق وسياق وأغراض المعالجة ("ماذا" و "من" و "كيفية" و "سبب" المعالجة).
- خطر الضرر الجسيم للأفراد.

يتوفر إرشادات حول ما قد يسبب ضررًا جسيمًا في القسم ٣ "متى يجب إجراء تحليل تأثير حماية خصوصية البيانات (DPIA)؟" في الأعلى.

لمزيد من المعلومات حول الإجراءات الإدارية والتقنية والمالية المناسبة في إرشادات الخصوصية المتضمنة بالتصميم والمتضمنة افتراضياً، يرجى الاطّلاع على المبادئ التوجيهية لأساسيات حماية خصوصية البيانات للمخاطبين بأحكام القانون.

٧,٧ - تقييم كيفية إثبات الالتزام بمبادئ قانون حماية خصوصية البيانات الشخصية (PDPPL)؟

يجب أن يقوم مراقب البيانات بتسجيل كيفية توضيح كل مبدأ من مبادئ حماية البيانات من خلال القرارات التي تم اتخاذها في تحليل تأثير حماية خصوصية البيانات (DPIA) الخاص به. سيساعد هذا مراقب البيانات على التحقق مما إذا كان قد فاته أي شيء وتحديد بوضوح كيفية توافق المعالجة مع قانون حماية خصوصية البيانات (PDPPL).

لمزيد من المعلومات حول المبادئ الأساسية لحماية خصوصية البيانات الشخصية، يرجى الاطّلاع على المبادئ التوجيهية لأساسيات حماية خصوصية البيانات للمخاطبين بأحكام القانون.

٧,٨ - الموافقة والتوقيع

يجب التوقيع على استمارة إدارة الشؤون السياسية من قبل:

- الموظفين المسؤولين عن قيادة حماية البيانات،
- رئيس القسم أو الوظيفة التي تمتلك النشاط،
- الموظفين الذين ساهموا في إجراء تحليل تأثير حماية خصوصية البيانات (DPIA).

يجب تخزينه بحيث يمكن الوصول إليه بسرعة إذا لزم الأمر، على سبيل المثال، في حالة حدوث خرق.

٧,٩ - الإجراءات التي تتبع تحليل تأثير حماية خصوصية البيانات (DPIA)

يجب على مراقب البيانات التأكد من أن إجراءات التخفيف الخاصة به مدرجة في خطة المشروع ومراقبة تنفيذها الناجح.

إذا قرر مراقب البيانات أنه غير قادرين على تخفيف مخاطر معينة، سواء من الناحية الفنية أو بسبب قيود التكلفة، يجب عليه استشارة شؤون الحوكمة والضمان السيبراني الوطني

كما يجب على مراقب البيانات إبقاء تحليل تأثير حماية خصوصية البيانات (DPIA) قيد المراجعة المستمرة وتحديثه إذا تغير نطاق أو معلومات عن المعالجة باتباع عملية تحليل تأثير حماية خصوصية البيانات (DPIA) الكاملة.

٨ - الملحق أ - مشغلات تحليل تأثير حماية خصوصية البيانات (DPIA)

أمثلة على الأنشطة التي قد تؤدي إلى إجراء تحليل تأثير حماية خصوصية البيانات (DPIA) هي:

- تطبيقات وتحديثات التكنولوجيا، على سبيل المثال:
  - تطبيق نظام جديد لإدارة علاقات العملاء (CRM) أو ترقية النظام،
  - سحب أو تعديل نظام إدارة موارد المؤسسة القديم (ERM) الحالي،
  - استخدام مزوّد نظام (طرف ثالث) جديد مثل تغيير مزوّد جهاز الدفع ببطاقة الائتمان،
  - جمع البيانات الشخصية بطريقة جديدة،
  - تخزين البيانات الشخصية أو تأمينها بطريقة جديدة،
  - تغيير الأنظمة التي تستخدمها لجمع البيانات الشخصية بأي طريقة.
- التغييرات على العمليات القائمة
  - معالجة البيانات الشخصية لغرض استخدام جديد أو الكشف عنها لطرف ثالث جديد،
  - تغيير عملية قائمة تتضمن البيانات الشخصية،
  - مشاركة البيانات مع مراقب أو معالج بيانات شخصية،
  - قرار الاحتفاظ بالبيانات لفترة أطول من تلك المحددة في جدول الاحتفاظ أو كما تم الكشف عنه في إشعار الخصوصية.
- التغييرات على المنتجات أو الخدمات
  - تطوير منتج أو خدمات جديدة،
  - استخدام البيانات الشخصية الموجودة لتحسين منتج أو خدمة،
  - جمع بيانات شخصية إضافية لتحسين منتج أو خدمة،
  - مشاركة البيانات مع طرف ثالث جديد لدعم عرض منتج أو خدمة.

القائمة أعلاه ليست حصرية ولكنها تعمل على تقديم أمثلة عن متى يتطلب إجراء تحليل تأثير حماية خصوصية البيانات (DPIA).

نهاية الوثيقة