State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

حماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً

PDPPL-02050208A

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 الإصدار ١,٠	نوفمبر ٢٠٢٠
٢,٠	الوثيقة المنشورة ذات الإصدار ٢,٠	سبتمبر ٢٠٢٢

الوثائق ذات صلة

الرقم المرجعي للوثيقة	اسم الوثيقة
PDPPL-02050201A	المبادئ التوجيهية لأسس حماية خصوصية البيانات الموجهة للمخاطبين بأحكام القانون
PDPPL-02050205A	المبادئ التوجيهية لحقوق الأفراد الموجهة للمخاطبين بأحكام القانون
PDPPL-02050209A	المبادئ التوجيهية لمراقبي ومعالجي البيانات الشخصية الموجهة للمخاطبين بأحكام القانون
PDPPL-02050206A	المبادئ التوجيهية لتحليل تأثير حماية خصوصية البيانات الموجهة 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 لحماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً 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 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 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 6

٢ - المقدمة 7

٣ - ماذا الذي عليه ينص قانون حماية خصوصية البيانات الشخصية (PDPPL) حول خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً (DPbDD)؟ 8

٤ - ما هي المفاهيم الرئيسية لحماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً (DPbDD) وكيفية امتثال المراقب لها؟ 10

٥ - ما هي المبادئ الأساسية لحماية خصوصية البيانات المتضمنة بالتصميم؟ 12

٦ - ما هي الاحتياطات الرئيسية التي يتطلبها قانون حماية خصوصية البيانات الشخصية (PDPPL) من المراقب لتنفيذها؟ 14

٧ - كيف يمكن للمراقب تطبيق حماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً (DPbDD) في مؤسسته؟ 16

٧,١ - كيف يجب أن تبدو الاحتياطات من المنظور العملي؟ 17

١ - النقاط الرئيسية

- عندما يقوم المراقب بجمع البيانات الشخصية أو تخزينها أو استخدامها، فإن الأفراد الذين تتم معالجة بياناتهم الشخصية قد يتعرضون للمخاطر. من المهم أن يتخذ المراقب خطوات لضمان معالجة البيانات الشخصية بشكل قانوني وآمن وفعال من أجل تقديم أفضل رعاية ممكنة.
- يتطلب قانون حماية خصوصية البيانات الشخصية (PDPPL) من المراقب وضع "احتياطات إدارية وفنية ومالية مناسبة" لتطبيق مبادئ خصوصية البيانات، حماية حقوق الأفراد وحماية بياناتهم الشخصية. يجب أن تكون هذه الاحتياطات متناسبة مع خطر الضرر البالغ لخصوصية الأفراد أو بياناتهم الشخصية. يُعرف هذا باسم حماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً (DPbDD).
- تعني حماية خصوصية البيانات المتضمنة بالتصميم أنه يجب على المراقب وضع اعتبارات خصوصية البيانات في صميم عملية صنع القرار خلال كل من مرحلة تصميم المشاريع ودورة حياة المشاريع الكاملة.
- تعني حماية خصوصية البيانات المتضمنة افتراضياً أنه يجب على المراقب تقليل البيانات الشخصية التي يعالجها بشكل افتراضي، بالإضافة الى جمعها، معالجتها، تخزينها وإتاحتها إلى الحد الضروري لتحقيق الأغراض المحدودة التي تتم المعالجة من أجلها.
- يجب على المراقب التفكير في تطبيق إجراء لإنشاء سجل لأنشطة المعالجة وتحديد العمليات التي قد تشكل خطرًا على الأفراد والتي تتطلب وضع واتخاذ الإجراءات المناسبة.
- تقع على عاتق المراقب مسؤولية تحديد الاحتياطات المناسبة للأخطار التي قد تسبب في حدوث أضرار جسيمة، كما يجب على المراقب استخدام تحليل تأثير حماية خصوصية البيانات (DPIAs) للقيام بذلك. يجب على المراقب أيضًا الأخذ في الاعتبار عناصر إضافية مثل تحليل المخاطر، السياسات التنظيمية والاحتياطات المادية والفنية.
- يجب على المراقب أيضًا أن يأخذ في الاعتبار المتطلبات الإضافية حول أمان معالجة البيانات الشخصية حيث تنطبق هذه المتطلبات أيضًا على المعالج. كما يجب أن تضمن إجراءات المراقب "السرية والنزاهة والتوافر" لأنظمتها وخدماتها والبيانات الشخصية التي يقوم المراقب بمعالجتها.
- يحتاج المراقب أيضًا إلى التأكد من أن لديه عمليات مناسبة لاختبار فعالية التدابير وإجراء أي تحسينات مطلوبة. يكون المراقب هو المسؤول عن مستوى الحماية الذي يقرر تطبيقه. في حالة حدوث اختراق أو شكوى، قد يُطلب من المراقب إخطار الأفراد وشؤون الحوكمة والضمان السيبراني الوطني بخطر الضرر الجسيم بسبب القرارات التي اتخذها المراقب.

٢ - المقدمة

يتطلب قانون حماية خصوصية البيانات الشخصية (PDPPL) من المراقب تنفيذ الاحتياطات الإدارية والتقنية والمالية المناسبة لحماية البيانات الشخصية. يجب أن تكون هذه الاحتياطات متناسبة مع خطر حدوث ضرر جسيم للأفراد حيث يُعرف هذا باسم حماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً (DPbDD).

يجب على المراقب دمج حماية خصوصية البيانات في أنشطة المعالجة وممارسات الأعمال الخاصة به، حيث يجب أن تتطبق من مرحلة التصميم وحتى دورة الحياة الكاملة للأنشطة والعمليات. يجب أن يتم هذا مع اتباع نهج "الأولوية لحماية خصوصية البيانات" مع أي إعدادات افتراضية للأنظمة والتطبيقات، على سبيل المثال تتطلب من الأفراد الموافقة الاختيارية أو الانسحاب الاختاري .

تعتبر تحليل تأثير حماية خصوصية البيانات الشخصية (DPIAs) وسجل معالجة البيانات الشخصية جزءًا لا يتجزأ من حماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً (DPbDD)، والتي بدورها تشكل عنصراً رئيسيًا لأي نظام إدارة البيانات الشخصية (PDMS).

توفر هذه المبادئ التوجيهية معلومات حول متطلبات حماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً (DPbDD)، كيفية تنفيذها من قبل المراقب، بالإضافة الى أمثلة على الإجراءات التي يمكن اتخاذها لحماية خصوصية البيانات الشخصية مع كيفية تحديد الاحتياطات المناسبة المرتبطة بمخاطر المعالجة من قبل المراقب.

يمكن الإطّلاع على متطلبات حماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً (DPbDD) في المواد ٣، ٨ و١٣ وهي موضحة بمزيد من التفصيل أدناه.

٣ - ماذا الذي عليه ينص قانون حماية خصوصية البيانات الشخصية (PDPPL) حول خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً (DPbDD)؟

ماذا الذي ينص عليه قانون حماية خصوصية البيانات الشخصية عن الحق في حماية خصوصية البيانات الشخصية؟

تنص المادة ٣ من قانون حماية خصوصية البيانات الشخصية (PDPPL) على ما يلي:

"لكل فرد **الحق في حماية خصوصية** بياناته الشخصية....."

ما الذي تعنيه هذه المادة؟

هذا يمنح الأفراد الحق في حماية بياناتهم الشخصية. يكون المراقب مسؤول عن حماية البيانات الشخصية للأفراد حين يقوم المراقب بمعالجتها أو التي تتم معالجتها بالنيابة عنه، بالإضافة الى التأكد من معالجة تلك البيانات الشخصية وفقًا لأحكام ومبادئ قانون حماية خصوصية البيانات الشخصية (PDPPL). تعني حماية خصوصية البيانات الشخصية التالي:

- معالجة البيانات وفقا لأحكام ومبادئ قانون حماية خصوصية البيانات الشخصية (PDPPL)؛
- التأكد من الاحتفاظ بالبيانات بشكل آمن بحيث لا يتم مشاركتها عن قصد أو عن غير قصد، مع أي شخص أو مؤسسة؛
- تزويد الأفراد بالقدرة على التحكم ببياناتهم الشخصية من خلال تمكينهم من ممارسة حقوقهم بموجب قانون حماية خصوصية البيانات الشخصية (PDPPL).

لمزيد من المعلومات حول حقوق الأفراد، يرجى الإطّلاع على المبادئ التوجيهية لحقوق الأفراد.

ماذا الذي ينص عليه قانون حماية خصوصية البيانات الشخصية (PDPPL) حول الاحتياطات الإدارية والتقنية والمالية المناسبة؟

تنص المادة (٣) ٨ من قانون حماية خصوصية البيانات الشخصية (PDPPL) على ما يلي:

"يتعين على المراقب الالتزام بما يلي: **اتخاذ الاحتياطات الإدارية والفنية والمادية المناسبة** لحماية البيانات الشخصية، وفقاً لما تحدده الإدارة المختصة".

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".

ما الذي تعنيه هذه المواد؟

يكون المراقب مطالب بموجب المادتين ٨ و١٣ باتخاذ جميع الاحتياطات المناسبة اللازمة لحماية البيانات الشخصية. يجب أن تكون هذه الاحتياطات متناسبة مع طبيعة وأهمية البيانات الشخصية الجاري معالجتها. وهذا يعني أن إجراءات المراقب لحماية البيانات الشخصية يجب أن تكون متوازنة مع خطر تلف خصوصية الأفراد أو بياناتهم الشخصية.

٤ - ما هي المفاهيم الرئيسية لحماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً (DPbDD) وكيفية امتثال المراقب لها؟

ما هي حماية خصوصية البيانات المتضمنة بالتصميم؟

حماية خصوصية البيانات المتضمنة التصميم هي نهج لتطوير العمليات والمنتجات والأنظمة والخدمات الجديدة التي تتضمن على معالجة البيانات الشخصية. يتطلب هذا النهج من المراقب وضع اعتبارات حماية خصوصية البيانات في صميم عملية صنع القرار خلال كل من مرحلة تصميم المشاريع ثم طوال دورة حياة المشاريع. سيساعد ذلك على ضمان حماية أفضل وأكثر فعالية من حيث التكلفة لحماية خصوصية بيانات الأفراد الشخصية.

ما هي حماية خصوصية البيانات المتضمنة افتراضيًا؟

حماية خصوصية البيانات المتضمنة افتراضيًا هي نهج لمعالجة البيانات الشخصية يضمن معالجة البيانات بأعلى درجة من حماية خصوصية البيانات بشكل افتراضي. تتضمن حماية خصوصية البيانات المتضمنة افتراضيًا المبادئ التالي: محدودية الغرض، محدودية التخزين، وعلى وجه الخصوص تقليل البيانات.

يتطلب هذا النهج من المراقب ضمان حماية خصوصية البيانات الشخصية تلقائيًا في أي نظام تكنولوجيا معلومات، و/أو خدمة، و/أو منتج، و/أو ممارسة تجارية حتى لا يضطر الأفراد إلى اتخاذ إجراءات محددة لحماية خصوصية بياناتهم. يجب أن يكون الخيار الافتراضي لأي خيار يتم توفيره للأفراد مناسبًا لحماية خصوصية البيانات (على سبيل المثال، استخدام الموافقة الاختيارية وليس الانسحاب الاختياري أو المربعات المحددة مسبقًا).

يجب جمع البيانات الضرورية فقط لكل غرض معالجة بيانات شخصية محدد ما لم يسمح الأفراد للمراقب بجمع المزيد.

هل يعني هذا أن المراقب يجب أن يتوقف عن معالجة البيانات الشخصية؟

لا يعني هذا أن المراقب يجب أن يتوقف عن معالجة البيانات الشخصية لتحقيق أغراضه ولكن قد يحتاج المراقب إلى وضع احتياطات إضافية للتأكد من أنه لا يعالج سوى البيانات الشخصية الضرورية للغاية. بالاضافة الى ذلك يجب على المراقب التأكد من أن الأفراد على علم تام بالبيانات الشخصية التي يقوم المراقب بمعالجتها وكيفية معالجتها والأغراض التي تتم معالجة البيانات الشخصية من أجلها.

ما الذي يجب على المراقب القيام به من أجل الامتثال لمتطلبات حماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً DPbDD؟

يكون المراقب مطالب بوضع الاحتياطات الإدارية والتقنية والتنظيمية المناسبة لحماية خصوصية البيانات الشخصية التي يعالجها. يكون المراقب مسؤول عن تحديد الاحتياطات المناسبة ومتناسبة مع المخاطر التي قد يتسبب فيها المعالجة التي يقوم بها والتي قد تتسبب في ضرر جسيم لخصوصية الأفراد و/أو بياناتهم الشخصية. يجب على المراقب اتخاذ خطوات للتأكد من أن هذه الاحتياطات فعالة والتأكد من مراجعتها باستمرار.

يجب على المراقب تضمين حماية خصوصية البيانات في أنشطة المعالجة وممارسات الأعمال الخاصة به. كما يجب أن تكون تدابير حماية خصوصية البيانات في طليعة عملية اتخاذ القرار عند التخطيط لأنشطة المعالجة أو تصميمها ثم بعد ذلك طوال دورة حياتها.

ما الذي يجب على مراقب البيانات فعله تجاه معالج البيانات المستخدم من قبله؟

إذا كان المراقب يستخدم مؤسسة أخرى لمعالجة البيانات الشخصية بالنيابة عنه، فإن هذه المؤسسة هي معالج تحت قانون حماية خصوصية البيانات الشخصية (PDPPL). بالإضافة إلى ذلك معالج البيانات ملزم بالامتثال لمتطلبات حماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً (DPbDD).

تتطلب المادة (٨) ١١ من المراقب تأكيد أن معالج البيانات المستخدم:

- يمتثل لتعليمات التي يعطيها المراقب،
- يعتمد على الاحتياطات المناسبة لحماية خصوصية البيانات الشخصية،
- يحافظ باستمرار على الامتثال لهذه التعليمات واعتماد مثل هذه الاحتياطات.

لمزيد من المعلومات حول استخدام معالج البيانات، يرجى الاطلاع على المبادئ التوجيهية لمراقبي ومعالجي البيانات الشخصية.

٥ - ما هي المبادئ الأساسية لحماية خصوصية البيانات المتضمنة بالتصميم؟

حماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً (DPbDD) هو نهج معترف به دوليًا يستند إلى المبادئ الأساسية السبعة لحماية خصوصية البيانات المتضمنة بالتصميم الذي طوره مفوض المعلومات والخصوصية في ولاية أونتاريو.

تختلف مبادئ حماية خصوصية البيانات المتضمنة بالتصميم عن مبادئ خصوصية البيانات الشخصية المنصوص عليها في المبادئ التوجيهية لأسس حماية خصوصية البيانات. يرجى الاطّلاع على المبادئ التوجيهية لأسس حماية خصوصية البيانات لمزيد من التفاصيل. لا يُفترض أن تتداخل هاتان المجموعتان من المبادئ بل يجب تسيران جنبًا إلى جنب.

مبادئ حماية خصوصية البيانات المتضمنة بالتصميم هي:

١ - **النهج استباقي وليس رد الفعل، وقائي وليس علاجي:** يجب أن يكون نهج حماية خصوصية البيانات المتضمنة بالتصميم استباقيًا وليس رد فعل.

٢ - **الخصوصية كإعداد افتراضي:** تسعى حماية خصوصية البيانات المتضمنة بالتصميم إلى تقديم أقصى درجة من الحماية لخصوصية البيانات من خلال ضمان حماية البيانات الشخصية تلقائيًا في أي نظام تكنولوجيا معلومات أو ممارسة تجارية معينة. لا يتطلب اتخاذ أي إجراء من جانب الأفراد لحماية خصوصية بياناتهم فهو مدمج في النظام بشكل افتراضي.

٣ - **تضمين حماية خصوصية البيانات بالتصميم:** تكون حماية خصوصية البيانات متضمنة في داخل التصميم والهندسة هيكلية لأنظمة تكنولوجيا المعلومات والممارسات التجارية، هذا يعني أنها يجب أن تؤخذ في عين الاعتبار في المراحل الأولية لأي تصميم أو تخطيط.

٤ - **خاصية كاملة - نتائج إيجابية وليس سلبية:** تسعى حماية خصوصية البيانات المتضمنة بالتصميم إلى استيعاب وتحقيق جميع المصالح والأهداف المشروعة بطريقة تضمن تحقيق الإيجابية والفائدة للأعمال وحماية خصوصية البيانات وليس عن طريق النزاعات التي قد تسبب ضرراً لأي جهة.

٥ - **الأمان الشامل - حماية دورة الحياة الكاملة للبيانات:** تمتد حماية خصوصية البيانات المتضمنة بالتصميم بشكل آمن طوال دورة حياة البيانات المعنية حيث تعتبر الإجراءات الأمنية القوية ضرورية لحماية خصوصية البيانات. يتم الاحتفاظ بجميع البيانات بشكل آمن، ثم يتم إتلافها بشكل آمن في نهاية العملية في الوقت المناسب.

٦ - **الظهور والشفافية:** تؤكد حماية خصوصية البيانات الشخصية لجميع أصحاب المصلحة أن أنشطة معالجة البيانات الشخصية تعمل وفقًا للوعود والأهداف المعلنة. تظل الأنشطة والعمليات التابعة لمعالجة البيانات الشخصية ظاهرة وشفافة لكل من الأفراد ومزودي الخدمات على حد سواء.

٧ - **احترام خصوصية الأفراد:** تتطلب حماية خصوصية البيانات المتضمنة بالتصميم من مهندسي هيكلة تكنولوجيا المعلومات والمشغلين الحفاظ على مصالح الأفراد من خلال تقديم إجراءات مثل الافتراضات القوية لحماية خصوصية البيانات، إشعارات الخصوصية المناسبة، وتوفير خيارات سهلة الاستخدام لتمكين الأفراد.

إذا كان مراقب البيانات يستخدم معالج للبيانات فيجب عليه أن يؤكد أن المعالج يوضح امتثاله يأخذ في عين الاعتبار المبادئ لحماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً (DPbDD).

لمزيد من المعلومات حول استخدام معالج البيانات، يرجى الاطلاع على المبادئ التوجيهية لمراقبي ومعالجي البيانات.

٦ - ما هي الاحتياطات الرئيسية التي يتطلبها قانون حماية خصوصية البيانات الشخصية (PDPPL) من المراقب لتنفيذها؟

بموجب المادة ١١ قانون حماية خصوصية البيانات الشخصية، يجب على المراقب تنفيذ الاحتياطات التالية إلى حد مناسب متوازنة مع المخاطر ذات الأضرار الجسيمة الذي قد تسببه معالجة البيانات الشخصية لخصوصية الأفراد أو البيانات الشخصية.

- **نظام إدارة البيانات الشخصية (PDMS):** تتطلب المادة (٥) ١١ من المراقب وضع نظام إدارة البيانات الشخصية لإدارة عملية الامتثال لقانون حماية خصوصية البيانات الشخصية (PDPPL). يعد هذا النظام احتياط إداري رئيسي حيث يجب أن يتضمن القدرة على الإبلاغ عن أي خروقات للأفراد و إدارة شؤون الحوكمة والضمان السيبراني الوطني وحماية البيانات.
- **تحليل تأثير حماية خصوصية البيانات** DPIAs: تطلب المادة (١) ١١ من المراقب مراجعة تدابير حماية خصوصية البيانات قبل الشروع في المعالجة. يتم ذلك من خلال استكمال تحليل تأثير حماية خصوصية البيانات (DPIA) وتنفيذ الإجراءات المناسبة للحد من المخاطر.
- **حقوق الأفراد والشكاوى:** تتطلب المادة (١) ١١ من المراقب وضع نظام لتمكين الأفراد من ممارسة حقوقهم وإدارة الشكاوى والتحقيق فيها حول كيفية معالجة المراقب للبيانات الشخصية.
- **تمكين الأفراد المراجعة والتحكم في بياناتهم الشخصية:** تتطلب المادة (٦) ١١ من المراقب وضع التقنيات المناسبة لتمكين الأفراد من الوصول إلى البيانات الشخصية الخاصة بهم ومراجعتها وتصحيحها.
- **الشفافية:** تتطلب المادة ٩ من المراقب بإخطار الأفراد بالمعلومات الأساسية حول كيفية وسبب قيام المراقب بمعالجة بياناتهم الشخصية قبل بدء عملية المعالجة. يتم ذلك من خلال إشعار الخصوصية العامة.
- **تدريب الموظفين وتوعيتهم:** تتطلب المادة (٣) ١١ من المراقب توفير التدريب والتوعية للموظفين الذين يقومون بمعالجة البيانات الشخصية حول حماية خصوصية البيانات.
- **أمن البيانات:** تتطلب المادة ١٣ من المراقب اتخاذ الاحتياطات اللازمة لحماية خصوصية البيانات الشخصية من الضياع أو التلف أو التعديل أو الكشف أو الوصول أو الاستخدام بشكل غير قانوني أو عن طريق الخطأ. هذا يشمل كلاً من إجراءات الأمان الفنية والمادية.
- **معالج البيانات:** تتطلب المادة (٢) ١١ من المراقب تحديد المعالج المسؤول عن حماية خصوصية البيانات الشخصية التي يقوم بمعالجتها نيابة عن المراقب. تطلب المادة (٨) ١١ من المراقب تأكيد امتثال المعالج إلى تعليماته، بالإضافة إلى تأكيد اعتماد المعالج للاحتياطات المناسبة لحماية خصوصية البيانات الشخصية وتقييم مثل هذا الامتثال والاحتياطات بانتظام.

- **ضمان الاحتياطات المناسبة:** تتطلب المادة (٧) ١١ من المراقب إجراء عمليات تدقيق ومراجعة شاملة منتظمة حول الامتثال لمتطلبات حماية خصوصية البيانات.

الاحتياطات المذكورة أعلاه والموضحة في المادتين ١١ و١٣ من قانون حماية خصوصية البيانات الشخصية (PDPPL) ضرورية ولكن ليست هذه القائمة الحصرية. على سبيل المثال ،يعتمد عمق التدريب أو شمولية نظام إدارة البيانات الشخصية PDMS الخاص بالمراقب على البيانات الشخصية التي يعالجها وكيفية معالجتها. إن التأكد من أن احتياطات المراقب تستوفي الشروط المطلوب واعتبارها "مناسبة" قد يتطلب من المراقب المزيد من الجهد والعمل.

النقطة الأساسية هي أن المراقب يجب أن يأخذ في عين الاعتبار قضايا حماية خصوصية البيانات منذ بداية أي نشاط معالجة، بالإضافة إلى تطبيق سياسات وإجراءات تتناسب مع المخاطر ذات الأضرار الجسيمة التي قد تلحق بالأفراد.

٧ - كيف يمكن للمراقب تطبيق حماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً (DPbDD) في مؤسسته؟

يجب على المراقب وضع الاحتياطات الإدارية والتقنية والمالية المناسبة لتنفيذ مبادئ حماية خصوصية البيانات وحماية حقوق الأفراد والحفاظ على أمن البيانات. يمكن أن تكون هذه الاحتياطات وظائف وعمليات وضوابط وأنظمة وإجراءات وتدابير يمكن للمؤسسات تطبيقها لتعزيز المعالجة الآمنة ،تخزين البيانات الشخصية ،تجنب خروقات البيانات، وتسهيل الامتثال لالتزامات حماية خصوصية البيانات ذات الصلة.

لا توجد طريقة "مناسبة للجميع" للقيام بذلك، ولا توجد مجموعة واحدة من الإجراءات التي يجب على المراقب وضعها. يعتمد على الظروف والحالات الخاصة بكل مراقب.

كما هو مذكور أعلاه، تعني حماية خصوصية البيانات الشخصية ما يلي:

- معالجة البيانات الشخصية وفقا لأحكام ومبادئ قانون حماية خصوصية البيانات الشخصية (PDPPL)؛
- التأكد من الاحتفاظ بالبيانات بشكل آمن بحيث لا يتم مشاركتها عن قصد أو عن غير قصد مع أي شخص أو مؤسسة؛
- تمكين الأفراد من التحكم ببياناتهم الشخصية من خلال تمكينهم من ممارسة حقوقهم بموجب قانون حماية خصوصية البيانات الشخصية (PDPPL).

يجب أن يكون المراقب على ثقة من أن الإجراءات التي يحددها لحماية خصوصية البيانات الشخصية والتي تتم معالجتها تتناسب مع المخاطر ذات الأضرار الجسيمة لخصوصية الأفراد وبياناتهم الشخصية. هذا يتطلب تحقيق التوازن الصحيح بين الإجراءات الاحترازية المناسبة والمخاطر التي يتعرض لها الأفراد، مع مراعاة التالي:

- الممارسات الرائدة بما في ذلك أحدث التقنيات لتكنولوجيا المعلومات؛
- تكاليف تنفيذ إجراءات حماية خصوصية البيانات المختلفة المتاحة؛
- طبيعة ونطاق وسياق وأغراض المعالجة ("ماذا" و "من" و "كيفية" و "سبب" المعالجة)؛
- المخاطر ذات الأضرار الجسيمة على الأفراد.

يجب أن يقوم المراقب بتقييم الإجراءات التي تم تحديدها مقابل احتمال حدوث ضرر جسيم كجزء من تحليل تأثير حماية خصوصية البيانات الشخصية (DPIA). إذا كان هناك اختراق وقد تسبب ذلك في أضرار للأفراد فإن المراقب مسؤول عن الاحتياطات التي وضعها.

للحصول على مزيد من المعلومات حول تحليلات تأثير حماية خصوصية البيانات الشخصية (DPIAs)، يرجى الإطّلاع على المبادئ التوجيهية لتحليلات تأثير حماية خصوصية البيانات الشخصية.

٧,١ - كيف يجب أن تبدو الاحتياطات من المنظور العملي؟

تعتمد الطريقة التي يتبعها المراقب في تطبيق الاحتياطات المناسبة لحالتهم وظروفهم الخاصة، على سبيل المثال، من هم، طبيعة عملهم، والموارد المتاحة، وطبيعة البيانات التي يعالجها. قد لا يحتاج المراقب دائمًا إلى وجود مجموعة من المستندات والضوابط التنظيمية، على الرغم من أنه في كثير من الظروف سيطلب منه توفير بعض المستندات المتعلقة بمعالجة البيانات الشخصية.

ما هي الأمثلة على الاحتياطات الإدارية التي قد يتخذها مراقب؟

الاحتياطات الإدارية هي تلك التي تتعلق بإدارة مؤسسة المراقب والطريقة التي يؤدي بها المهام لتوفير حماية خصوصية البيانات. تشمل الأمثلة الشائعة للاحتياطات الإدارية ما يلي:

- **أطر الإدارة:** نموذج تشغيل يحتوي على الحوكمة والمساءلات ويحدد من المسؤول عن تنفيذ أنشطة الامتثال لقانون حماية خصوصية البيانات الشخصية (PDPPL).
- **سجلات معالجة البيانات الشخصية:** تزويد المراقب بفهم كامل للبيانات الشخصية التي يقوم بمعالجتها.
- **تحليل تأثير حماية خصوصية البيانات الشخصية (DPIA):** لمراجعة إجراءات حماية خصوصية البيانات قبل وخلال دورة حياة أنشطة معالجة البيانات الشخصية.
- **سياسات وإجراءات خصوصية البيانات:** سياسات حماية خصوصية البيانات، حماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً (DPbDD) و حقوق الأفراد بالإضافة الى أمور أخرى تحدد العمليات التي يجب اتباعها من أجل الامتثال لمبادئ ومتطلبات قانون حماية خصوصية البيانات الشخصية (PDPPL).
- **إجراءات التدريب والتطوير:** لبناء ثقافة الوعي بحماية خصوصية البيانات في مؤسسة المراقب وإبلاغ الموظفين بمسئولياتهم. قد يشمل هذا الشهادات المقدمة من قبل الجمعيات الدولية.
- **تدابير الشفافية:** إشعار الخصوصية ذو 'لغة واضحة' حيث يمنح الأفراد القدرة على التحكم ببياناتهم الشخصية بما في ذلك سبب وكيفية معالجة البيانات من قبل المراقب. كما يتضمن الإشعار معلومات عن حقوق الأفراد وكيفية ممارستها بالإضافة الى من هو المسؤول عن حماية خصوصية البيانات الشخصية في المؤسسة.
- **أدوات التحكم للأفراد:** لتمكينهم من تحديد كيفية استخدام المراقب لبياناتهم الشخصية، وما إذا كان المراقب يفرض سياساته بشكل صحيح.
- **تقديم افتراضيات خصوصية قوية:** تقديم افتراضيات خصوصية قوية، خيارات وعناصر تحكم سهلة الاستخدام واحترام تفضيلات المستخدم.
- **وضع متطلبات على معالجات الجهات الخارجية:** طلب أدلة على نضج حماية خصوصية البيانات لدى المعالج حيث تكون هذه الاعتبارات متضمنة في عملية اختيار المراقب، بالإضافة الى وضع العقود أو الاتفاقيات

المكتوبة موضع التنفيذ حيث تشمل إجراءات التدقيق بما في ذلك تعليمات المعالج حول كيفية حماية خصوصية البيانات الشخصية. لمزيد من المعلومات حول المتطلبات التعاقدية، يرجى الاطّلاع إلى المبادئ التوجيهية لمراقبي ومعالجي البيانات الشخصية.

- **سياسات وإجراءات أمن المعلومات:** تتضمن
  - المسؤوليات المرتبطة بأمن المعلومات،
  - الوصول إلى المباني و/أو المعدات،
  - ترتيبات استمرارية أعمال التي تحدد كيفية حماية وإستعادة أي بيانات شخصية من قبل المراقب،
  - المراقبة الدورية للتأكد من أن إجراءات الحماية مناسبة محدّثة.

ما هي أمثلة الاحتياطات التقنية التي قد يتخذها المراقب؟

الاحتياطات التقنية هي تلك المتعلقة باستخدام التكنولوجيا لتنفيذ المهام أو تحقيق نتائج معينة لتوفير حماية خصوصية البيانات. تشمل الأمثلة الشائعة للاحتياطات التقنية ما يلي:

- **الاسم المستعار والتشفير:** استخدام اسم مستعار (استبدال مواد التعريف الشخصية بمعرفات اصطناعية) والتشفير (تشفير الرسائل بحيث يتمكن فقط المسموح لهم من قراءتها) ؛
- **ضوابط الوصول والاحتفاظ:** لضمان الامتثال لمبادئ تقليل البيانات، محدودية الغرض ومحدودية التخزين؛
- **التكنولوجيا المتعلقة بالتحكم الفردي:** تقنيات لتمكين الأفراد من الوصول إلى بياناتهم الشخصية ومراجعتها وتصحيحها.
- **إجراءات الأمن المادي:**
  - جودة الأبواب والأقفال وأجهزة الإنذار أو الدوائر التلفزيونية المغلقة (CCTV)؛
  - كيفية تحكم المراقب في الوصول إلى أماكن عملهم، وكيف يتم الإشراف على الزوار؛
  - كيفية تخلص المراقب من أي نفايات ورقية أو إلكترونية؛
  - كيفية محافظة المراقب على معدات تكنولوجيا المعلومات وخاصة الأجهزة المحمولة بشكل آمن.
- **إجراءات الأمن السيبراني:**
  - أمن النظم - أمان شبكة التحكم وأنظمة المعلومات بما في ذلك تلك التي تعالج البيانات الشخصية؛
  - أمن البيانات - أمان البيانات التي يحتفظ بها المراقب داخل أنظمته، على سبيل المثال ضمان وجود ضوابط وصول مناسبة وحفظ البيانات بشكل آمن؛

- الأمن عبر الإنترنت - على سبيل المثال أمان الموقع الالكتروني للمراقب وأي خدمة أو تطبيق عبر الإنترنت يستخدمه المراقب؛
- أمن الأجهزة - بما في ذلك السياسات المتعلقة بجلب الأجهزة الخاصة (BYOD) إذا كان ذلك مقدم من قبل المراقب.

مع مرور الوقت وفي ظل التطور المستمر للتكنولوجيا، سيستلزم ذلك تحديث الاحتياطات الفنية والتقنية اللازمة بشكل مستمر لتتناسب مع حماية خصوصية البيانات الشخصية ومعالجتها مع أحدث تطورات التكنولوجيا. بذلك أيضا، ينبغي على المراقب إدراج هذه الاعتبارات في تحليلات مخاطر أمن المعلومات وتحليلات تأثير حماية خصوصية البيانات الشخصية (DPIA).

ما هي أمثلة الاحتياطات المالية التي قد يتخذها المراقب؟

الاحتياطات المالية هي تلك التي تتعلق بالاستثمار في المنتجات أو الخدمات لتنفيذ المهام أو تحقيق نتائج معينة لتوفير حماية خصوصية البيانات. يمكن أن يكون هذا الاستثمار يتعلق بتنفيذ الاحتياطات الإدارية أو التقنية.

تشمل الأمثلة الشائعة للاحتياطات المالية ما يلي:

- **الاستثمار في التكنولوجيا:** لتزويد الأفراد بالتحكم في بياناتهم الشخصية، أو للحفاظ على أمان بياناتهم أو لدعم المؤسسات ببرنامج الامتثال الخاص بالمراقب.
- **الاستثمار في الاستشارة المهنية:** للحصول على مشورة متخصصة في حماية خصوصية البيانات أو أمن المعلومات ضمن نطاق أوسع من وثيقة المبادئ التوجيهية هذه.
- **تخصيص ميزانية للامتثال لحماية خصوصية البيانات**: سيمكن هذا في القيام بأنشطة تتعلق بحماية خصوصية البيانات الشخصية للإمتثال لقانون حماية خصوصية البيانات الشخصية (PDPPL) أو أفضل الممارسات الدولية.

كيف يقوم المراقب بتحديد الاحتياطات المناسبة للمخاطر ذات الأضرار الجسيمة؟

ستكون بعض الاحتياطات التي يضعها المراقب يمكن تطبيقها على مستوى المؤسسة بينما يمكن لاحتياطات اخرى ان يتم تطبيقها على مستوى العمليات والأنشطة.

يجب أن تحمي احتياطات المراقب البيانات الشخصية من خلال:

- معالجة البيانات وفقا لأحكام ومبادئ قانون حماية خصوصية البيانات الشخصية (PDPPL)؛
- التأكد من الاحتفاظ بالبيانات بشكل آمن بحيث لا يتم مشاركتها عن قصد أو عن غير قصد مع أي شخص أو مؤسسة؛

- تزويد الأفراد بالقدرة على التحكم ببياناتهم الشخصية من خلال تمكينهم من ممارسة حقوقهم بموجب قانون حماية خصوصية البيانات الشخصية (PDPPL).

يجب أن يقوم المراقب بتقييم مدى ملاءمة وفعالية الاحتياطات باستخدام تحليل تأثير حماية خصوصية البيانات (DPIA) مع مراعاة ما يلي:

- يجب أن تكون احتياطات المراقب مناسبة لحجم المؤسسة واستخدامات الشبكات ونظم المعلومات الخاصة به؛
- يجب أن يأخذ في عين الاعتبار التطور التكنولوجي المستمر بالإضافة الى النظر في تكاليف التنفيذ والتطبيق؛
- يجب أن تكون احتياطات المراقب مناسبة لممارساته التجارية. على سبيل المثال، إذا قامت مؤسسة بتزويد الموظفين بإمكانية العمل من المنزل، فإن المراقب بحاجة إلى وضع الإجراءات المناسبة للتأكد من أن ذلك لا يضر بحماية خصوصية البيانات؛
- يجب أن تكون احتياطات المراقب مناسبة لطبيعة البيانات الشخصية التي بحوزته والأضرار الجسيمة التي قد تنجم عن الخروقات أو اضطرابات الأعمال.

عند تقييم الاحتياطات المناسبة، يجب أن تؤخذ في عين الاعتبار بشكل خاص المخاطر التي تبرز كنتيجة لمعالجة البيانات الشخصية، ولا سيما من الضرر الغير المقصود أو الغير قانوني أو الفقدان أو التغيير أو الكشف الغير مصرح به أو الوصول إلى البيانات الشخصية المنقولة أو المخزنة أو المعالجة.

تتحد برامج الامتثال لحماية خصوصية البيانات الناجحة خلف رؤية مشتركة وتوظف نهجًا كليًا متعدد التخصصات يجمع بين الخبرة من فرق حماية خصوصية البيانات القانونية وأمن المعلومات والمخاطر والبيانات مع سفراء من جميع أنحاء المؤسسة الذين لديهم فهم عميق لكيفية معالجة المؤسسة للبيانات الشخصية. من المهم أن يقوم المراقب بإشراك الأشخاص في عملية التقييم الخاصة بهم بالخبرة المطلوبة لدعم القرارات المتخذة حول ما يعتبر "مناسبًا".

قد يرغب المراقب أيضًا في الاستفادة من خبرة مزودي الخدمة المعتمدين في مقابل المعايير الوطنية لأمن المعلومات و/أو الخصوصية لدعم برامجهم مثل إطار الامتثال لأمن المعلومات الوطني (NISCF).

تشمل المعلومات الأساسية في دعم الإعتبارات بشأن التدابير المناسبة ما يلي:

- الأجزاء ذات الصلة من الإطار التشريعي التي تحتوي على أحكام أمن المعلومات، مثل السياسة الوطنية لضمان المعلومات وسياسة أمن الحوسبة السحابية.
- مخرجات المؤسسات الرقابية مثل هيئة تنظيم الاتصالات لقطاع الاتصالات على سبيل المثال.
- مخرجات معلومات المراكز الأمنية المتميزة مثل المركز القومي لأمن المعلومات (Q-CERT).

- أطر السياسات الخاصة بالحكومات الوطنية، مثل الخطط الوطنية لحماية خصوصية البيانات والأمن السيبراني.
- السياسات التنظيمية والإرشادات الأخرى الصادرة عن الجهات المنظمة لحماية خصوصية البيانات الوطنية من قبل الجهات المنظمة للقطاع.
- القرارات حول إجراءات الإنفاذ التنظيمية التي تقدمها هيئات التنظيم الوطنية لحماية خصوصية البيانات والجهات التنظيمية ذات الصلة.
- قرارات المحاكم والهيئات القضائية في المجالات ذات الصلة.
- المعايير الوطنية والدولية لأفضل الممارسات، مثل سياسة قطر الوطنية لضمان المعلومات، أي اعتمادات أو شهادات صادرة عن شؤون الحوكمة والضمان السيبراني، سلسلة ISO 27000، معايير أمن بيانات صناعة بطاقات الدفع، و**CBEST** وإطار NIST.
- تقارير تقييم المخاطر والأبحاث الخاصة بالمواضيع العالمية الأساسية التي تنشرها شركات ومستشاري أمن وحماية تقنية المعلومات.
- مخرجات الجمعيات المهنية ذات الصلة والمجموعات الفئوية. هناك العديد من العاملين في هذه المحالات، مثل الرابطة الدولية لمحترفي حماية خصوصية البيانات، وتحالف أمن الحوسبة السحابية (Cloud Security Alliance) ومنتدى أمن المعلومات.

هذه القائمة ليست حصرية، ولكنها تقدم أمثلة على مجموعة من المصادر المتاحة في تحديد الاحتياطات المناسبة.

يجب أن يقوم المراقب بتوثيق الاعتبارات التي قام بها في تقييم المخاطر ذات الضرر الجسيم، والاحتياطات المتاحة ومدى ملاءمتها.

للحصول على مزيد من المعلومات حول تحليلات تأثير حماية خصوصية البيانات الشخصية (DPIAs)، يرجى الإطّلاع على المبادئ التوجيهية لتحليلات تأثير حماية خصوصية البيانات الشخصية.

نهاية الوثيقة