State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

أسس حماية خصوصية البيانات

PDPPL-02050201A

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 لحماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً 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 لأسس 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 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 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 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 مبادئ معالجة البيانات الشخصية.
- يحدد قانون حماية خصوصية البيانات الشخصية (PDPPL) عددًا من المبادئ الأساسية لمعالجة البيانات الشخصية. وهذه هي:
  - الشفافية والأمانة واحترام الكرامة الإنسانية؛
  - تقليل البيانات؛
  - الدقّة؛
  - محدودية التخزين؛
  - النزاهة والسرية؛
  - محدودية الغرض؛
  - المساءلة؛
- يجب أن تكمن هذه المبادئ في صميم نهجكم في معالجة البيانات الشخصية.
- ستساعد هذه المبادئ المراقب / المعالج إصدار أحكام تتعلق بالمعالجة، على سبيل المثال عند اتخاذ القرار بشأن التوازن المناسب بين الاحتياطات لحماية البيانات الشخصية وخطر الضرر البالغ لخصوصية الأفراد.

٢ - المقدمة

يحدد قانون حماية خصوصية البيانات الشخصية (PDPPL) المبادئ الأساسية لمعالجة البيانات الشخصية. يجب أن تكون هذه المبادئ في صميم نهج المراقب / المعالج فيما يتعلق بمعالجة البيانات الشخصية كما ويجب أن ترشد هذه المبادئ المراقب / المعالج عند تفسير قانون حماية خصوصية البيانات الشخصية (PDPPL) وإنشاء نظام إدارة حماية البيانات الخاص بالمراقب / المعالج (PDMS).

كما يجب أن تؤخذ هذه المبادئ في الاعتبار عند وضع الاحتياطات المناسبة التي تحددها شؤون الحوكمة والضمان السيبراني.

تعتبر هذه المبادئ مفيدة بشكل خاص عند اتخاذ قرارات بشأن مستوى الحماية المناسب لبعض البيانات الشخصية، وعند تقييم التوازن بين حقوق الأفراد وضرورة معالجة بياناتهم الشخصية.

يمكن البحث عن المبادئ في المواد ١ و ٣ و ٥ و ١٠ من قانون حماية خصوصية البيانات الشخصية (PDPPL)، ويتم شرح كل مبدأ بمزيد من التفصيل أدناه.

الشفافية والأمانة واحترام الكرامة الإنسانية

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

"لكل فرد الحق في حماية خصوصية **بياناته الشخصية، ولا يجوز معالجة تلك البيانات إلا في اطار الشفافية والأمانة واحترام كرامة الإنسان** والممارسات المقبولة، وفقاً لأحكام هذا القانون".

يعني هذا أنه يجب أن تكون كيفية معالجة البيانات الشخصية للأفراد تتسم بالشفافية ولا يتم معالجتها بطريقة مضللة.

- الشفافية هي فكرة وجوب معالجة البيانات الشخصية بطريقة واضحة ومنفتحة ونزيهة، وبما يتماشى مع الحق في إبلاغها. وهذا يعني إبلاغ الأفراد عن هويتك كمراقب، ولماذا وكيف تعالج بياناتهم الشخصية، ومن الذي تشاركها مع، والمدة التي تنوي الاحتفاظ بها؛
- يعني مبدأ المصداقية أنه يجب معالجة البيانات الشخصية بشكل قانوني وليس بطريقة مضللة أو مخادعة للأشخاص المعنيين أو لغرض آخر غير الغرض الذي تم جمعها؛
- احترام الكرامة الإنسانية يتعلق بحق الأفراد في أن يتم تقديرهم واحترامهم، وهو ما يعني في هذا السياق أنه يجب استخدام معالجة البيانات الشخصية بشكل عادل وأخلاقي.

تقليل البيانات

تنص المادة ١٠ من قانون حماية خصوصية البيانات الشخصية (PDPPL) على ما يلي:

"على المراقب التحقق من أن البيانات الشخصية التي يجمعها، أو التي يتم جمعها لصالحه، **ذات صلة** بالأغراض المشروعة **وكافية** لتحقيقها...".

يعني مبدأ تقليل البيانات أنه يجب التأكد من أن أي بيانات شخصية يجمعها المراقب تكون كافية وذات صلة ومحدودة. يجب أن تكون البيانات الشخصية التي يتم جمعها:

- كافية: يجب أن تكون البيانات الشخصية التي يقوم المراقب بمعالجتها كافية لتحقيق غرضكم؛
- ذات صلة: يجب فقط معالجة البيانات الشخصية بطريقة تتوافق مع الغرض الأصلي الذي تمت المعالجة من أجله؛

- مقتصرة على ما هو ضروري: يجب عدم الاحتفاظ ببيانات شخصية أكثر من تلك المطلوبة لتحقيق الغرض الذي تتم المعالجة من أجله.

تتطلب حماية البيانات المتضمنة افتراضياً، تقديم افتراضات حول حماية خصوصية البيانات قوية فيما يتعلق بتفضيلات المستخدم حتى لا يضطر الأفراد إلى اتخاذ أي إجراء محدد لحماية خصوصيتهم. لذلك يجب تقليل هذه البيانات بشكل افتراضي؛ أي أنه لا يجب على الأفراد اتخاذ أي إجراء للتأكد من أن المراقب لا يجمع البيانات الشخصية بما يتجاوز الحد المطلوب، أو معالجتها عند غير الضرورة.

تم تناول حماية البيانات المتضمنة افتراضياً، يرجى الاطّلاع على المبادئ التوجيهية لحماية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً لمزيد من المعلومات.

الدقّة

تنص المادة ١٠ من قانون حماية خصوصية البيانات الشخصية (PDPPL) على ما يلي:

"...على المراقب التحقق من أن تلك البيانات **دقيقة ومكتملة ومحدثة** بما يفي بالأغراض المشروعة..."

يجب على المراقب التأكد من صحة البيانات الشخصية ومدى تحديثها. عند معالجة البيانات الشخصية ، يجب على المراقب:

- اتخاذ خطوات مناسبة للتأكد من صحة البيانات الشخصية وعدم تضليلها في الواقع؛
- تحديث البيانات الشخصية عند الضرورة؛
- اتخاذ خطوات مناسبة لحذف أو تصحيح البيانات الشخصية غير الصحيحة؛
- تزويد الأفراد بالوسائل لتصحيح وتحديث بياناتهم الشخصية؛
- تزويد الأفراد بأدلة توضيحية عند قيام المراقب بمشاركة بيانات شخصية غير دقيقة عن الأفراد.

محدودية التخزين

تنص المادة ١٠ من قانون حماية خصوصية البيانات الشخصية (PDPPL) على ما يلي:

"وألا يحتفظ بها لمدة تزيد على **المدة الضرورية** لتحقيق تلك الأغراض".

يجب على المراقب عدم تخزين البيانات الشخصية لفترة أطول مما هو مطلوب لتنفيذ الغرض الذي تمت المعالجة من أجله. عند تخزين البيانات الشخصية، يجب على المراقب:

- أن يكون على دراية بالبيانات الشخصية التي يحتفظ بها ولماذا يحتاج إلى تخزينها؛
- أن يكون لدى المراقب سياسة تحدد نهج فترات الاحتفاظ ومحو البيانات الشخصية؛
- النظر بعناية في مدة الاحتفاظ بالبيانات الشخصية وما إذا كان يمكن تبرير هذه الفترة؛
- مراجعة البيانات الشخصية التي تحتفظون بها بانتظام ومحوها أو إخفاء هويتها عندما لا تكون مطلوبة.

النزاهة والسرية

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

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

تنص المادة ٨,٣ من قانون حماية خصوصية البيانات الشخصية (PDPPL) على ما 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".

يجب على كل من المراقب والمعالج التأكد من أن لديهم الاحتياطات المناسبة المعمول بها لحماية البيانات الشخصية التى يحتفظون بها والحفاظ على مستوى عال لأمن المعلومات. تقرر شؤون الحوكمة والضمان السيبراني الوطني أن الاحتياطات المناسبة لإثبات لمبدأ النزاهة والسرية هي:

- التأكد من أن لديكم عمليات قائمة لتقييم وتنفيذ إجراءات أمن المعلومات التي تتناسب مع طبيعة وأهمية البيانات الشخصية الجاري معالجتها؛
- فهم البيانات الشخصية التى ستقومون بمعالجتها والتى يجب الحفاظ على سريتها، والنظر فى جاهزية إتاحة بعض البيانات الشخصية؛
- تمكين طرق التشفير و / أو التسمية المستعارة عند الاقتضاء للقيام بذلك؛
- الحفاظ على وجود سياسات وإجراءات وتدابير تقنية لأمن المعلومات والتأكد من الالتزام بها وتحديثها بانتظام؛
- الحفاظ على وجود عمليات لاختبار فعالية الإجراءات الخاصة بالمراقب والمعالج والنظر في أي تحسينات قد تكون ضرورية على بانتظام؛
- وضع ضوابط فنية مثل تلك المحددة في الأطر القائمة مثل سياسة ضمان المعلومات الوطنية ٢,٠.

محدودية الغرض

تنص المادة ٥,٣ من قانون حماية خصوصية البيانات الشخصية (PDPPL) على ما يلي:

"طلب حذف بيانات الأفراد الشخصية أو محوها في الحالات المشار إليها في البندين السابقين، أو **عند انتهاء الغرض** الذي تمت من أجله معالجة تلك البيانات، أو إذا **لم يكن هناك مبرر** للاحتفاظ بها لدى المراقب".

تنص المادة ١٠ من قانون حماية خصوصية البيانات الشخصية (PDPPL) على ما يلي:

"... **وألا يحتفظ بها لمدة تزيد على المدة الضرورية** لتحقيق تلك الأغراض"

يجب التأكد من محو البيانات الشخصية أو إخفاء هويتها بشكل افتراضي عندما لا يكون المراقب والمعالج بحاجة إليها. هذا يعني أن الغرض الأصلي الذي كانت تتم معالجة البيانات الشخصية من أجله لم يعد موجودًا، ولم يعد هناك أيضًا أي مبرر قانوني أو تجاري آخر للاحتفاظ بها.

يجب على المراقب عدم معالجة البيانات الشخصية لأغراض أخرى غير تلك التي تم جمعها من أجلها إلا إذا:

- قام بتقدير أن هذا الغرض الجديد متوافق مع الغرض الأصلي؛

- قام بالحصول على موافقة الأفراد؛
- لدى المراقب التزام قانوني للقيام بذلك.
-

المساءلة

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."

يجب على المراقب إعداد نظام إدارة البيانات الشخصية (PDMS) الذي يتضمن احتياطات إدارية وفنية ومالية مناسبة لحماية البيانات الشخصية.

يجب على المراقب إجراء عمليات تدقيق ومراجعات شاملة حول امتثال المؤسسة لقانون حماية خصوصية البيانات الشخصية (PDPPL)، كما هو مطلوب في المادة ١١,٧. علما بأن هذا يعد عنصر رئيسي لإثبات الامتثال لقانون حماية خصوصية البيانات الشخصية (PDPPL).

يجب توثيق السياسات والإجراءات والأهداف والنظم والضوابط المطلوبة كجزء من نظام إدارة البيانات الشخصية، بالإضافة إلى سجلات عمليات التدقيق والمراجعات الدورية للاحتياطات التي تتبعها ومدى فعاليتها. سيساعد هذا على إظهار الالتزام بحماية البيانات الشخصية والذى يتم التحقق منه من قبل شؤون الحوكمة والضمان السيبراني الوطني في حالة حدوث خروقات امنية.

لإثبات الامتثال لمبدأ المساءلة، يجب على المراقب تنفيذ نظام إدارة حماية البيانات (PDMS) وذلك لضمان اتباع نهج "حماية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً"، الذي يتكون من الاحتياطات المنصوص عليها في دليل نظام إدارة حماية البيانات (PDMS) بالاضافة الى أي احتياطات ضرورية أخرى تتناسب مع طبيعة وأهمية البيانات الشخصية التي يقوم المراقب بمعالجتها.

٣ - الخلاصة

تختلف كل مؤسسة عن الأخرى ولا توجد إجابة واحدة مناسبة للجميع للامتثال لقانون حماية خصوصية البيانات الشخصية (PDPPL). يجب على كل مؤسسة مراجعة وفهم متطلبات القانون لتحديد كيفية تطبيقها على المؤسسة وما هو المطلوب القيام به لضمان الامتثال.

يجب على كل مؤسسة أن تأخذ في الاعتبار الطرق التي تعالج بها البيانات الشخصية وتحمل مسؤولية ذلك. يجب على كل مؤسسة اتّباع نهج قائم على المخاطر، بناءً على مبادئ الخصوصية الموضحة أعلاه، ووضع هذه المبادئ في صميم نهج معالجة المراقب / المعالج للبيانات الشخصية.

نهاية الوثيقة