State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

نظام إدارة حماية البيانات

PDPPL-02050203A

قائمة المراجعة 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
لا يوجد	**لا يوجد**

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 لنظام إدارة حماية 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 - المقدمة

تحدد قائمة المراجعة هذه الأنشطة الأساسية التي يجب على المراقب/المعالج القيام بها لوضع نظام إدارة البيانات الشخصية (PDMS) خاص بهم. إن إدراك ما إذا كنتم تعالجون بيانات شخصية وكيفية عمل ذلك سيمكّنكم من فهم ما إذا كان قانون حماية خصوصية البيانات الشخصية (PDPPL) ينطبق على مؤسستكم وكيفية ذلك. البيانات الشخصية هي معلومات تتعلق بشخص محدد أو يمكن تحديده.

يمكن للمراقب/المعالج استخدام قائمة التحقق هذه لتخطيط أنشطة الامتثال لحماية خصوصية البيانات الخاصة بهم. هذه القائمة ليست شاملة ويجب قراءتها بالتوازي مع جميع التوجيهات المقدمة من شؤون الحوكمة والضمان السيبراني الوطني وكذلك القانون وأي قرارات وزارية ذات صلة. سيساهم تنفيذ قائمة المراجعة هذه في إظهار التزام المراقب/المعالج بمتطلبات قانون حماية خصوصية البيانات الشخصية (PDPPL) لإنشاء نظام إدارة حماية البيانات (PDMS).

لا تعتبر هذه القائمة بمثابة شهادة بالامتثال، حيث أن استكمال جميع الأنشطة المذكورة لا يؤكد عدم امكانية خرق قانون حماية خصوصية البيانات الشخصية (PDPPL).

٢ - قائمة مراجعة نظام إدارة حماية البيانات

تتم مناقشة جميع الأنشطة أدناه بمزيد من التفصيل في وثائق إرشادات قانون حماية خصوصية البيانات الشخصية (PDPPL) الأخرى. توفر هذه القائمة للمراقب/المعالج نقطة انطلاق لبرنامج حماية البيانات الخاص حيث أن لكل قسم يحتوي على مربع اختيار توجد ملاحظة توجيهية تابعة له. يجب على المراقب/المعالج استخدام هذه القائمة كنقطة انطلاق عامة لرسم أنشطة الامتثال الخاصة به وقراءة الإرشادات التابعة لها أثناء معالجة كل جانب بالتفصيل.

☐ لقد أخذنا في الاعتبار مبادئ خصوصية البيانات وتأثيرها على أنشطة المعالجة الخاصة بنا.

- لقد راجعنا مبادئ حماية البيانات الشخصية ونعي كيف تشكل الأسس لحماية البيانات. نحن نأخذ ذلك في الاعتبار عند اتخاذ قرارات بشأن البيانات الشخصية في مؤسساتنا.
- تكمن هذه المبادئ في صميم نهجنا للبيانات الشخصية:
  - الشفافية، والأمانة واحترام كرامة الإنسان؛
  - تقليل البيانات؛
  - الدقّة؛
  - محدودية التخزين؛
  - النزاهة والسرية؛
  - محدودية الغرض؛
  - المساءلة؛

☐ تم الأخذ في الاعتبار الإجراءات المطلوبة لإعداد سجل أنشطة معالجة البيانات الشخصية (RoPA).

- لقد اعتبرنا ووثقنا ما إذا كنا بحاجة إلى سجل أنشطة معالجة البيانات الشخصية لتمكين الامتثال لقانون حماية خصوصية البيانات الشخصية (PDPPL).
- لقد حددنا أصحاب المصلحة الرئيسيين في الأقسام التي من المرجح أن تعالج البيانات الشخصية.
- بعد النظر في النموذج المقدم من شؤون الحوكمة والضمان السيبراني الوطني تم اختيار الصيغة والشكل المناسب لإعداد قائمة بجميع أنشطة معالجة البيانات الشخصية.
- لقد جعلنا أصحاب المصلحة الرئيسيين على دراية بالمعلومات التي تحتاج إلى جمعها وتسجيلها في سجل أنشطة معالجة البيانات الشخصية.
- لقد أكملنا سجل أنشطة معالجة البيانات الشخصية مع صاحب المصلحة الرئيسي في كل قسم حيث يحتوي السجل على المعلومات المطلوبة لدعم برنامج الامتثال لحماية خصوصية البيانات لدينا. على سبيل المثال ممارسة الحقوق، وإدارة الطرف الثالث، ومتطلبات الإبلاغ عن الاختراقات والمخالفات وما إلى ذلك.

- نقوم بمراجعة سجل أنشطة معالجة البيانات الشخصية الخاصة بنا باستمرار وتتم إضافة أنشطة معالجة جديدة قبل بدءها، ويكون أحد موظفينا مسؤولاً عن بقائها محدثة ودقيقة.

☐ تم الأخذ في الاعتبار حقوق الأفراد المرتبطة ببياناتهم الشخصية والتي قد يستخدموها وكيفية الاستجابة لهذه الطلبات.

- لقد راجعنا الحقوق المتاحة للأفراد في قانون حماية خصوصية البيانات الشخصية (PDPPL) ونعي ما يجب علينا القيام به للامتثال والاستجابة للمتطلبات. هذه الحقوق هي:
  - الحق في حماية البيانات الشخصية ومعالجتها بشكل مشروع؛
  - الحق في سحب الموافقة السابقة على معالجة البيانات الشخصية؛
  - حق الاعتراض؛
  - حق الحذف؛
  - حق طلب تصحيح البيانات الشخصية؛
  - حق الإخطار بمعالجة البيانات الشخصية؛
  - حق الإخطار بأي إفشاء بيانات شخصية غير دقيقة؛
  - الحق في الوصول للبيانات الشخصية.
- لقد وضعنا عملية لاستقبال طلبات حقوق الأفراد والرد عليها.
- لقد أكدنا أن القائمين بالأعمال ذات الصلة في مؤسساتنا قادرين على تنفيذ الإجراءات المطلوبة للامتثال لكل فئة من الطلبات بعد وضع العملية ذات الصلة.

☐ لدينا نظام لضمان أن الأفراد قادرين على طرح التساؤلات والشكاوى.

- لقد قمنا بالنظر في كيفية التعامل مع شكاوى الأفراد ولدينا عملية لتسهيل ذلك.
- لقد قمنا بتحديد جهة الاتصال المسؤولة للتعامل مع هذه الشكاوى والاستجابة في غضون الإطار الزمني المطلوب.

☐ تم الأخذ في الاعتبار شرط وجود غرض مشروع لكل من أنشطة معالجة البيانات الشخصية الخاصة بنا.

- لقد قمنا بتحديد الغرض المشروع لكل نشاط معالجة قبل إجراء المعالجة، وقمنا بتوثيقه في سجل أنشطة معالجة البيانات الخاص بنا.
- لقد قمنا بتحديد الشروط التابعة لنا لمعالجة البيانات الشخصية ذات الطبيعة الخاصة قبل أن نبدأ في معالجة هذه البيانات وتوثيقها.
- لقد قمنا بمراجعة سجل أنشطة معالجة البيانات الخاص بنا وحددنا غرضًا مشروعا لكل نشاط معالجة مع فريقنا القانوني.
- لقد قمنا بتحديد العمليات التي تتطلب منا الحصول على موافقة الأفراد حيث ليس لدينا غرض قانوني.

- عندما نقوم بمعالجة البيانات الشخصية ذات الطبيعة الخاصة، فقد قمنا بتحديد غرضًا مشروعاً لنشاط المعالجة وشرطًا إضافيًا محددًا لمعالجة البيانات الشخصية ذات الطبيعة الخاصة كشرط للحصول على إذن من شؤون الحوكمة والضمان السيبراني الوطني .
- عندما يتضمن نشاط المعالجة معالجة بيانات شخصية ذات طبيعة خاصة ، فإننا نقوم بإجراء تحليل تأثير حماية خصوصية البيانات (DPIA) نظرًا لزيادة احتمالية حدوث ضرر خطير للأفراد ناتج عن معالجة مثل هذه البيانات.

☐ لقد قمنا بالنظر في شرط الحصول على موافقة الأفراد في حال عدم وجود غرض مشروع بديل للمعالجة أو الإعفاء.

- لقد قمنا بتحديد العمليات التي تتطلب منا الحصول على موافقة الأفراد في الحالات التي لا ينطبق فيها غرض مشروع مثل (الالتزام التعاقدي أو الالتزام القانوني أو المصالح المشروعة).
- لدينا عملية للحصول على الموافقة وتتبع الموافقات المقدمة مع الأدلة وتمكين الأفراد من سحب الموافقة بسهولة حين يرغبون في ذلك:
  - تتطلب موافقتنا تمكينًا إيجابيًا ولا تستخدم المربعات المختارة مسبقًا أو أي طريقة أخرى للموافقة الافتراضية.
  - بيانات موافقتنا واضحة ومحددة وموجزة ومنفصلة عن الشروط والأحكام الأخرى.
  - تحدد بيانات الموافقة الخاصة بنا أي طرف ثالث قد يعتمد على الموافقة لمعالجة البيانات.
- نضمن أننا نتجنب الموافقة على المعالجة كشرط مسبق لتقديم الخدمة.
- نراجع موافقاتنا وممارساتنا للحصول على الموافقة بشكل مستمر ، وعند الضرورة ، نقوم بتحديثها.

☐ تم الأخذ في الاعتبار الاحتياطات الإدارية والتقنية والمالية المناسبة لحماية البيانات الشخصية.

- نتحمل مسؤولية الامتثال لقانون حماية خصوصية البيانات الشخصية (PDPPL)، على أعلى مستوى إداري وفي جميع أنحاء المؤسسة، وعند الضرورة، تنفيذ رؤية استراتيجية وحوكمة تفصيلية لدعم نظام إدارة حماية البيانات (PDMS) الخاص بنا.
- لقد قمنا بأخذ حماية خصوصية البيانات الشخصية في اعتبارنا عند تصميم طرق جديدة لمعالجة البيانات الشخصية، والمعروفة أيضًا باسم "حماية خصوصية البيانات الشخصية المتضمنة بالتصميم".
- نقوم باستخدام تحليل تأثير حماية خصوصية البيانات لتقييم خطر أنشطة المعالجة الجديدة وتحديد الاحتياطات المناسبة والاحتفاظ بسجل خاص لها.
- يتم تدوين احتياطات حماية البيانات لدينا في وثائق مناسبة من السياسات والإجراءات.
- نقوم بتنفيذ تدابير أمنية مناسبة لحماية سرية وسلامة وتوافر البيانات الشخصية.
- نقوم بالأخذ في الاعتبار إمكانية استخدام الاسم المستعار والتشفير عند معالجة البيانات الشخصية لتقليل مخاطر المعالجة.
- نقوم بتعزيز وعي موظفينا بمتطلبات حماية خصوصية البيانات الشخصية من خلال خطط التدريب المناسبة.
- نقوم بإجراء اختبارات ومراجعات داخلية لاحتياطيات حماية البيانات لدينا على أساس دوري منتظم.

- نقوم بمراجعة احتياطاتنا الإدارية والفنية والمالية بانتظام ، وعند الضرورة ، نقوم بتحديثها لمراعاة التطورات والتحديثات التكنولوجية في مجال حماية البيانات.

☐ نحن نعي أهمية إجراء تحليل تأثير حماية خصوصية البيانات الشخصية من أجل تحديد وتقليل المخاطر المرتبطة بأنشطة المعالجة الجديدة.

- لقد قمنا بتحديد أنشطة المعالجة التي نقوم بها والتي قد تسبب ضررًا خطيرًا للأفراد (بما في ذلك معالجة البيانات الشخصية ذات الطبيعة الخاصة) أو التي قد تتطلب معالجة كمية كبيرة من البيانات الشخصية وقمنا بإجراء تحليل تأثير حماية خصوصية البيانات خاصة بها.
- لقد قمنا بإعداد عملية لتقييم تأثير معالجة البيانات الشخصية باستخدام (تحليل تأثير حماية خصوصية البيانات) ومراجعة الاحتياطات لحماية البيانات الشخصية قبل المعالجة.
- يجب أن تشمل عمليات (تحليل تأثير حماية خصوصية البيانات) النقاط التالية:
  - وصف طبيعة وأهمية البيانات الشخصية التي تتم معالجتها تحت حمايتكم؛
  - تحديد أي خطر يسبب ضرر جسيم للأفراد نتيجة إجراء المعالجة؛
  - وصف حجم ونطاق عمليات مؤسسة المراقب/المعالج والإدارة ؛
  - الأخذ في الاعتبار أحدث الاحتياطات والضوابط والأنظمة والإجراءات والتدابير الحديثة؛
  - إجراء تقييم للاحتياطات التي تتناسب مع طبيعة نشاط المعالجة وما إذا كانت تخفف بشكل كاف من أي خطر يتعلق بحدوث ضرر جسيم للأفراد؛
  - الحصول على موافقة شخص في مؤسسة المراقب/المعالج لديه المعرفة ذات الصلة بكلٍ من عمليات المؤسسة وحماية البيانات؛
  - يعاد تقييمها إذا كان هناك أي تغيير في مستويات المخاطر التي قد تتطلب اتخاذ مزيد من الاحتياطات.
- نحن نضمن أن موظفينا مدركين لمتطلبات وكيفية إجراء تحليل تأثير حماية خصوصية البيانات قبل الانخراط في أنشطة معالجة جديدة.
- نحن نحتفظ بسجل لجميع عمليات تحليل تأثير حماية خصوصية البيانات (DPIA) التي نجريها للمساهمة في التحسين المستمر ودعم التحاليل العديدة المطلوب في حالة حدوث أي خرق.

☐ نحن ندرك نوع البيانات الشخصية التي تعتبر بيانات شخصية ذات طبيعة خاصة.

- عندما نعالج البيانات الشخصية ذات الطبيعة الخاصّة، نقوم بتحديد غرضًا مشروعاً للمعالجة وشرطًا منفصلاً لمعالجة هذه البيانات.
- نحن نفهم فئات البيانات الشخصية ذات الطبيعة الخاصة والمتطلبات المتعلقة بالحصول على إذن لمعالجة هذه البيانات من شؤون الحوكمة والضمان السيبراني.
- لدينا عملية موجودة لطلب والحصول على إذن من شؤون الحوكمة والضمان السيبراني.

- نحن نراقب منشورات شؤون الحوكمة والضمان السيبراني الوطني بشكل دوري في حالة تحديد الوزير فئات إضافية من البيانات الشخصية ذات الطبيعة الخاصة.

☐ نحن ندرك كيفية تحديد وضعنا إما كمراقب أو معالج وهو أمر بالغ الأهمية لضمان الامتثال لقانون حماية خصوصية البيانات الشخصية (PDPPL).

- إذا كنا نمتلك صناعة القرار على سبب وكيفية معالجة البيانات الشخصية، فإننا ندرك ما هي مسؤولياتنا كمراقب للبيانات.
- إذا كنا نتبع تعليمات المراقب أو معالج البيانات الشخصية نيابة عنهم، فإننا نفهم مسؤولياتنا كمعالج.
- نضمن وجود الاحتياطات المناسبة المعمول بها، وهي المتطلبات التعاقدية المكتوبة، لحماية البيانات الشخصية التي يتم معالجتها نيابة عنا بواسطة المعالج.

☐ لقد قمنا بالنظر في آثار عمليات نقل البيانات عبر الحدود.

- نحن ندرك أنه إذا قمنا بجمع البيانات الشخصية داخل دولة قطر ونقلنا تلك البيانات الشخصية إلى موقع أو كيان يقع خارج قطر، سوف يعتبر ذلك نقلًا للبيانات عبر الحدود.
- نحن ندرك عند إجراء عمليات نقل البيانات عبر الحدود التي "قد تتسبب في أضرار جسيمة لبيانات الأفراد الشخصية أو الخصوصية" ، يجب وضع إجراءات حماية مناسبة لحماية الأفراد وأن يكون لدينا عملية للقيام بذلك.
- لقد قمنا بتحديد أنشطة المعالجة الخاصة بنا التي تتضمن عمليات نقل البيانات عبر الحدود ووضعنا الإجراءات الوقائية المناسبة لحماية البيانات الشخصية المعنية، ما لم يكن هناك استثناء.

☐ لقد قمنا باتخاذ الاحتياطات اللازمة لحماية البيانات الشخصية ولدينا خطة للإبلاغ عن انتهاكات هذه الاحتياطات.

- نحن نعي الشروط المنصوص عليها في المادة ١٤ من قانون حماية خصوصية البيانات الشخصية (PDPPL) لإخطار كل من شؤون الحوكمة والضمان السيبراني الوطني والأفراد حين تتطلب الخرق أو المخالفة ولدينا إجراء للقيام بذلك.
- نحن ندرك أهمية إجراءات تحديد الخروقات مثل الاختبار والفحص لضمان وجود سياسات شاملة لأمن المعلومات.
- نحن ندرك أنه يجب وضع سياسات أمن المعلومات والاستجابة للخروقات حتى نتمكن من تضمين مسؤوليات فريقنا ذو التخصصات المتعددة.
- نحن نضمن أن معالجي البيانات على دراية بمسؤوليتهم القانونية من أجل إبلاغنا بأي انتهاكات للبيانات الشخصية التي يعالجونها بالنيابة عنا.
- نحن نحتفظ بسجل لجميع الخروقات التي تنطوي على البيانات الشخصية سواء كانت بحاجة إلى إعلام أم لا، لتسجيل عملية صنع القرار لدينا ودعم التحسين المستمر.

☐ لقد أدركنا أن قانون حماية خصوصية البيانات الشخصية (PDPPL) حدد عددًا من الإعفاءات من بعض الحقوق والالتزامات في ظروف معينة.

- نحن نعالج البيانات الشخصية فقط بموجب إعفاء على أساس كل حالة على حدة.
- نحن نبرر ونوثق أسبابنا للاعتماد على الاستثناءات.

- نعتمد على قانون حماية خصوصية البيانات الشخصية (PDPPL) إذا لم يكن هناك إعفاء يغطي نشاط المعالجة الذي نقوم به.

نهاية الوثيقة