State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

سجل معالجة البيانات الشخصية

PDPPL-02050212A

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
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 لسجل معالجة البيانات الشخصية الموجهة للمخاطبين بأحكام القانون".

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 للاتصال الالكتروني لغرض التسويق المباشر الموجهة للمخاطبين بأحكام القانون".

لايعتبر 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 6
٢ - المقدمة 7
٣ - ما الذي ينص عليه قانون حماية خصوصية البيانات الشخصية (PDPPL) فيما يخص سجل معالجة البيانات الشخصية؟ 8
٤ - كيف يمكن لمراقب البيانات وضع سجل معالجة البيانات الشخصية؟ 9
٤,١ - من الذي يحتاج إلى وضع سجل أنشطة معالجة البيانات الشخصية؟ 9
٤,٢ - ما الذي يجب تضمينه من قبل المراقب في سجلات أنشطة معالجة البيانات الشخصية 9
٤,٣ - ما هي المعلومات الأخرى الذي يجب تضمينها في سجلات أنشطة معالجة البيانات الشخصية من قبل المراقب؟ 10
٤,٤ - ما هي الخطوات التي يمكن أن يتبعها المراقب لإعداد سجلات أنشطة معالجة البيانات الشخصية؟ 12

١ - النقاط الرئيسية

- يتطلب قانون حماية خصوصية المعلومات الشخصية (PDPPL) من المراقب وضع نظام إدارة البيانات الشخصية (PDMS).
- أحد العناصر الرئيسية لنظام إدارة البيانات الشخصية (PDMS) هو سجل أنشطة معالجة البيانات الشخصية (RoPA) الذي يتم فيه جمع المعلومات الأساسية حول البيانات الشخصية التي يعالجها المراقب وكيفية قيامه بذلك.
- تعد سجلات أنشطة معالجة البيانات الشخصية (RoPA) احتياطات إدارية أساسية للامتثال لعدد من متطلبات قانون حماية خصوصية البيانات الشخصية (PDPPL).
- قد توفر قواعد حماية البيانات (ROPA) أيضًا مزايا تشغيلية لمؤسسات مثل تحسين إدارة البيانات، وزيادة كفاءة الأعمال بين المؤسسات أخرى.

٢ - المقدمة

يشكل سجل أنشطة معالجة البيانات الشخصية (RoPA) الأساس لبرنامج الامتثال لحماية خصوصية بيانات والمراقب مما يسهل الامتثال لمختلف الالتزامات بموجب قانون حماية خصوصية البيانات الشخصية (.PDPPL)

تحدد هذه المبادئ التوجيهية سبب إلزام المراقب بوضع سجل أنشطة معالجة البيانات الشخصية (ROPA)، وما الذي يجب أن يتضمنه هذا السجل لإثبات الامتثال للمتطلبات المحددة في قانون حماية خصوصية البيانات الشخصية (PDPPL).

قبل وضع سجل لأنشطة معالجة البيانات الشخصية (RoPA)، يجب أن يضمن المراقب أنه قد قام بمراجعة وفهم محتوى المبادئ التوجيهية المرتبطة بقانون حماية خصوصية البيانات الشخصية (PDPPL) الأخرى لتمكينه من جمع وتسجيل معلومات دقيقة ضمن سجل أنشطة معالجة البيانات الشخصية (RoPA) الخاصة به والتابعة لمعالجته للبيانات الشخصية.

٣ - ما الذي ينص عليه قانون حماية خصوصية البيانات الشخصية (PDPPL) فيما يخص سجل معالجة البيانات الشخصية؟

على الرغم من عدم إلزام قانون حماية خصوصية البيانات الشخصية (PDPPL) المراقب بوضع سجل لأنشطة معالجة البيانات الشخصية (RoPA)، فإن هذا السجل يشكل الأساس لنظام إدارة البيانات الشخصية (PDMS) للمراقب. إن سجل أنشطة معالجة البيانات الشخصية (RoPA) هو احتياط إداري مناسب يمكّن الامتثال لمتطلبات قانون حماية خصوصية البيانات الشخصية (PDPPL) الأخرى.

سيتطلب من المراقب وضع سجل لأنشطة معالجة البيانات الشخصية (RoPA) لتمكين الامتثال للمتطلبات من أجل:

- تتبع الموافقة: تتبع أنشطة المعالجة التي تم الحصول على الموافقة عليها (المواد ٤ و٥,١ و١٧,٢ و٢٢)؛
- نشر إشعار خصوصية: إبلاغ الأفراد بالمعلومات حول كيفية معالجة المراقب للبيانات الشخصية للأفراد عبر إشعار الخصوصية (المادتان ٦,١ و٩)؛
- إدارة تقييمات حماية خصوصية البيانات: تتبع تحليلات تأثير حماية خصوصية البيانات (DPIAs) (المادة ١١,١)؛
- خطة التدريب: تتبع البيانات الشخصية داخل منشأة المراقب لضمان تقديم التدريب والمعرفة للموظفين الذين يتعاملون مع البيانات الشخصية فيما يخص مسؤولياتهم (المادة ١١,٣)؛
- إدارة الخروقات والإخطارات: الاستجابة بسرعة وفعالية للخروقات التي تتعلق بالبيانات الشخصية (المادتان ١١,٥ و١٣)؛
- التحقق من امتثال معالج البيانات: تتبع البيانات الشخصية التي تتم مشاركتها مع أطراف ثالثة (المادة ١١,٨)؛
- إدارة نقل البيانات عبر الحدود: تتبع البيانات الشخصية المنقولة إلى موقع خارج قطر (المادة ١٥)؛
- إدارة معالجة البيانات ذات الطبيعة الخاصة: تتبع معالجة البيانات الشخصية ذات الطبيعة الخاصة وإدارة التصاريح (المادة ١٦).

بالإضافة إلى تمكين المراقب من الامتثال لقانون حماية خصوصية البيانات الشخصية (PDPPL)، يمكن أن توفر سجلات أنشطة معالجة البيانات الشخصية (RoPA) أيضًا مزايا أخرى مثل:

- تحسين إدارة البيانات وحوكمتها: يمكن لسجلات البيانات التي يعالجها المراقب أن تمكّن ممارسة جيدة في إدارة البيانات وحوكمتها، مما يوفر رؤية موحدة لمعالجة البيانات الشخصية التي يمكنها تحسين جودة البيانات واكتمالها ودقتها والأسس الرئيسية لتحليلات البيانات الفعالة؛
- زيادة كفاءة الأعمال: قد تتيح المعرفة التامة بالبيانات الشخصية التي يحتفظ بها المراقب، وسبب الاحتفاظ، ومدة الاحتفاظ بالبيانات الشخصية تطوير العمليات لتكون أكثر فعالية وتنظيماً.

٤ - كيف يمكن لمراقب البيانات وضع سجل معالجة البيانات الشخصية؟

قدمت شؤون الحوكمة والضمان السيبراني الوطني نموذجًا لسجل أنشطة معالجة البيانات الشخصية (RoPA) الذي قد يستخدمه المراقب لتوثيق أنشطة المعالجة الخاصة به. قد يستخدم المراقب النموذج المقدم أو يقوم بطرح نموذج خاص به.

٤,١ - من الذي يحتاج إلى وضع سجل أنشطة معالجة البيانات الشخصية؟

توصي شؤون الحوكمة والضمان السيبراني الوطني بأن يقوم كل مراقب بوضع سجل لأنشطة معالجة البيانات الشخصية (RoPA) لتتبع أنشطة المعالجة الخاصة به. يكون المراقب هو صاحب القرار بشأن ما إذا كان سيتم وضع سجل لأنشطة معالجة البيانات الشخصية (RoPA) لدعم الامتثال للالتزامات بموجب قانون حماية خصوصية البيانات الشخصية (PDPPL). إذا لم يقم المراقب بالاحتفاظ بسجل لأنشطة معالجة البيانات الشخصية (RoPA) وتم تقديم شكوى بشأن التزاماته، فقد يكون المراقب مسؤولاً عن الغرامات بموجب المادة ٢٣ و / أو ٢٤ من قانون حماية خصوصية البيانات الشخصية (PDPPL).

توصي شؤون الحوكمة والضمان السيبراني الوطني في حال وجود عدد من أنشطة المعالجة لدى المعالج، أن يقوم بوضع سجل لأنشطة معالجة البيانات الشخصية (RoPA) لدعم أنشطة الامتثال الخاصة بالمراقب.

٤,٢ - ما الذي يجب تضمينه من قبل المراقب في سجلات أنشطة معالجة البيانات الشخصية

يمكّن سجل أنشطة معالجة البيانات الشخصية (ROPA) المراقب من الوفاء بالتزاماته بموجب قانون حماية خصوصية البيانات الشخصية (PDPPL). يوضح الجدول أدناه المعلومات المطلوبة للوفاء بالالتزامات الموضحة أعلاه.

المعلومات المطلوبة	أمثلة
اسم وبيانات الاتصال بكبار الموظفين المسؤولين عن حماية خصوصية البيانات في المنشأة.	على سبيل المثال الاسم الأول، اللقب ، رئيس مسؤولي الخصوصية ، البريد الإلكتروني: [...] ، هاتف [...]
اسم وتفاصيل الاتصال بمالك كل عملية؛	على سبيل المثال الاسم الأول، اللقب ، رئيس مسؤولي الخصوصية ، البريد الإلكتروني: [...] ، هاتف [...]
الغرض من معالجة البيانات الشخصية؛	على سبيل المثال لترتيب تسليم منتج تم طلبه عن طريق أحد عملاء الشركة.
السبب الذي يسمح بمعالجة البيانات الشخصية؛	على سبيل المثال الموافقة / المصالح المشروعة / الالتزام القانوني / الالتزام التعاقدي
فئات الأفراد التي تتم معالجة بياناتهم الشخصية؛	على سبيل المثال الموظفين والعملاء والطلاب والمرضى والركاب، إلخ.

المعلومات المطلوبة	أمثلة
فئات البيانات الشخصية و / أو البيانات الشخصية ذات الطبيعة الخاصة التي تتم معالجتها؛	على سبيل المثال الأصل العرقي، الأطفال، الصحة، الحالة الجسدية أو النفسية، العقائد الدينية، العلاقات الزوجية، الجرائم الجنائية والقياسات الحيوية.
المعلومات المتعلقة بتحليل تأثير حماية خصوصية البيانات لنشاط معالجة البيانات الشخصية؛	على سبيل المثال رابط إلى النموذج المكتمل لتحليل تأثير حماية خصوصية البيانات (DPIA) ذات الصلة أو معلومات عن مكان تخزينها.
أي أطراف داخلية تتم مشاركة البيانات الشخصية معها، على سبيل المثال قسم آخر داخل منظمة المراقب المالي	على سبيل المثال قسم العمليات، قسم تكنولوجيا المعلومات، قسم الموارد البشرية إلخ.
إن أمكن، اسم أو فئة وموقع جغرافي لأية أطراف أو منظمات خارجية يتم نقل البيانات الشخصية إليها؛	على سبيل المثال [موفر خدمات بطاقة الائتمان PLC، الدوحة قطر]، [Hospital Corporation Limited، لندن ، المملكة المتحدة]، أو وصف مثل البنوك المراسلة / وكلاء السفر وما إلى ذلك.
معلومات حول مدة احتفاظ المراقب بالبيانات الشخصية الجارية معالجتها.	على سبيل المثال سنة واحدة بعد تاريخ السفر الأولى، عدد سنوات يتماشى مع متطلبات البنك المركزي وما إلى ذلك.
وصف عام للاحتياطات الإدارية والتقنية والمالية للمراقب المتعلقة تحديدًا بأمن المعلومات.	على سبيل المثال معلومات تتعلق: التشفير، ضوابط الوصول، التدريب، إلخ.

* الأمثلة المقدمة أعلاه تزود الأفراد بالأمثلة فقط ولن تكون بالضرورة كافية لوصف أنشطة المعالجة الخاصة بالمراقب. المراقب مسؤول عن تحديد المعلومات المحددة المناسبة لتمكينه من الامتثال لالتزاماته.

٤,٣ - ما هي المعلومات الأخرى الذي يجب تضمينها في سجلات أنشطة معالجة البيانات الشخصية من قبل المراقب؟

ما المعلومات الإضافية التي قد تكون مفيدة عند صياغة إشعار حماية خصوصية البيانات؟

يجب على المراقب إخطار الأفراد بمعلومات معينة قبل معالجة بياناتهم الشخصية. يتم ذلك عن طريق إعداد إشعار الخصوصية ليتم تقديمه للأفراد قبل المعالجة ضمن مجموعة من التدابير أخرى. يوضح الجدول أدناه المعلومات التي قد يرغب المراقب في جمعها كجزء سجل أنشطة معالجة البيانات الشخصية (ROPA) لاستخدامها عند صياغة إشعار الخصوصية الخاص به.

معلومات المطلوبة	مثال
إذا كانت الموافقة هى السبب الذي يسمح بمعالجة البيانات الشخصية، حينها يجب تزويد معلومات فيما يخص تفاصيل بيان الموافقة المحدد المستخدم، وتاريخ تقديم الموافقة ومعلومات عن مكان تخزين سجلات الموافقة.	على سبيل المثال بيان الموافقة رقم ١٢٣، ١٣ مايو ٢٠١٧.
إذا كانت المصلحة المشروعة هي السبب الذي يسمح بمعالجة البيانات الشخصية، حينها يجب تزويد معلومات فيما يخص تفاصيل عن المصالح المشروعة للمعالج.	على سبيل المثال ملخص عن المصلحة المشروعة المحددة.
إذا كان ذلك قابلاً للتطبيق، فإن وجود عملية صنع قرار مؤتمتة، بما فى ذلك عملية التصنيف. فى حالات معينة، سيحتاج المراقب إلى إخبار الناس عن المنطق المتضمن والعواقب المتوقعة لذلك.	على سبيل المثال ملخص لكيفية استخدام صنع القرار الآلي للبيانات الشخصية لإصدار رأي أو قرار .
تزويد الأفراد بمصدر البيانات الشخصية إن أمكن. هذا مهم عندما لا يحصل المراقب على بيانات شخصية مباشرة من فرد.	على سبيل المثال وكلاء السفر / مواقع مقارنة الأسعار / الممارس العام عند الطلب.

ما المعلومات الأخرى التي قد تكون مفيدة لسجلات أنشطة معالجة البيانات الشخصية

قد يجد المراقب أنه من المفيد أيضًا توثيق المعلومات التالية:

- العقود المتعلقة بنشاط معالجة البيانات الشخصية: اسم ومالك وتخزين العقد أو رابط إلى مكان العقد.
- موقع البيانات الشخصية: الموقع الذي يتم تخزين البيانات الشخصية فيه لتمكين المراقب من تحديده بسهولة عند طلب الأفراد لممارسة حقوقهم أو أثناء أي اختراق لأمن المعلومات.
- المعلومات المتعلقة بالخروقات السابقة: روابط لأي وثائق تتعلق بالخروقات السابقة قد تمكن المراقب من تحديد أي أنماط أو سلوكيات مثيرة للقلق.
- الشرط الإضافي لمعالجة البيانات الشخصية ذات الطبيعة الخاصة: الشرط الإضافي المعتمد عليه لمعالجة البيانات الشخصية ذات الطبيعة الخاصة.
- تصاريح معالجة البيانات الشخصية ذات الطبيعة الخاصة: روابط لأي تصريح تم الحصول عليه لمعالجة البيانات الشخصية ذات الطبيعة الخاصة من شؤون الحوكمة والضمان السيبراني الوطني التي تتعلق بنشاط معالجة البيانات الشخصية.

٤,٤ - ما هي الخطوات التي يمكن أن يتبعها المراقب لإعداد سجلات أنشطة معالجة البيانات الشخصية؟

كما هو مذكور أعلاه، قدمت شؤون الحوكمة والضمان السيبراني الوطني نموذجًا لسجل أنشطة معالجة البيانات الشخصية (RoPA) الذي قد يستخدمه المراقب لتوثيق أنشطة المعالجة الخاصة به. يمكن للمراقب استخدام النموذج المقدم، أو إعداد نموذج خاص به.

يجب على المراقب اتباع نهج منظّم لتوثيق أنشطة معالجة البيانات الشخصية الخاصة به من أجل التأكد من أنه قد حصل على المعلومات المطلوبة. يمكن توثيق سجل أنشطة معالجة البيانات الشخصية (ROPA) ورقياً أو إلكترونياً حسب تقدير المراقب. قد يرغب المراقب في التفكير في تضمين الخطوات التالية في مبادرته لإعداد سجل أنشطة معالجة البيانات الشخصية (RoPA):

١- **تأكيد المتطلبات**: مراعاة الإجراءات المطلوبة لإعداد سجل أنشطة معالجة البيانات الشخصية (ROPA) من خلال التأكد من فهمه للمتطلبات الواردة في قانون حماية خصوصية البيانات الشخصية (PDPPL)؛

٢- **تحديد أصحاب المصلحة**: تحديد أصحاب المصلحة الرئيسيين في الإدارات التي من المرجح أنها تعالج البيانات الشخصية؛

٣- **قرار تنسيق الوثيقة**: توثيق القرارات حول ما يجب تضمينه في سجل أنشطة معالجة البيانات الشخصية (RoPA) وكيف يمكّن ذلك من الامتثال لقانون حماية خصوصية البيانات الشخصية (PDPPL) بعد الأخذ في عين الاعتبار هذه المبادئ التوجيهية والنموذج المقدم من شؤون الحوكمة والضمان السيبراني؛

٤- **تقديم موجز لأصحاب المصلحة**: توعية أصحاب المصلحة بالمعلومات التي يحتاجون إلى جمعها وتوثيقها في سجل أنشطة معالجة البيانات الشخصية (RoPA) لكي يتمكنوا من جمعها داخل أقسامهم؛

٥- **استكمال سجل أنشطة معالجة البيانات الشخصية (**RoPA**)**: التأكد من أن أصحاب المصلحة في الإدارات يتلقون الدعم والتوجيه الكافي لإكمال سجل أنشطة معالجة البيانات الشخصية (RoPA) لضمان أن المعلومات الملتقطة كافية فيما يتعلق بأنشطة معالجة البيانات الشخصية من قبل المراقب؛

٦- **المراجعة المستمرة**: مراجعة سجل أنشطة معالجة البيانات الشخصية (RoPA) بشكل مستمر والتأكد من إضافة أنشطة معالجة جديدة قبل البدء بإجرائها، بالإضافة إلى التأكد من إدراج مسؤولية إبقاء السجلات محدثة ودقيقة ضمن مسؤوليات الموظفين المعنيين.

نهاية الوثيقة