State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

مذكرة استرشادية بشأن إعداد

برنامج شامل لحماية خصوصية البيانات الشخصية

PDPPL-202501AN (A)

إدارة حماية خصوصية البيانات الشخصية

الوكالة الوطنية للأمن السيبراني

التاريخ: أكتوبر **2025**

الإصدار: **0.1**

التصنيف: عام

سجل الوثيقة

رقم الإصدار	الوصف	التاريخ
1.0	وثيقة منشورة – 1.0	**أكتوبر 2025**

الوثائق ذات الصلة (المبادئ التوجيهية)

مرجع الوثيقة	عنوان الوثيقة
PDPPL-02050201A	مبادئ خصوصية البيانات - المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02050213A	إشعار الخصوصية - المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02040203A	نظام إدارة حماية البيانات الشخصية - قائمة المراجعة للمخاطبين بأحكام القانون
PDPPL-02050205A	حقوق الأفراد - المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02050206A	تحليل تأثير حماية خصوصية البيانات - المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02050208A	حماية خصوصية البيانات الشخصية المتضمنة بالتصميم والمتضمنة افتراضياً - المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02050209A	مراقبي ومعالجي البيانات الشخصية - المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02050212A	سجل معالجة البيانات الشخصية - المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02050217A	معالجة البيانات الشخصية ذات الطبيعة الخاصة- المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02050215A	إخطارات اختراق البيانات الشخصية - المبادئ التوجيهية للمخاطبين بأحكام القانون

الوثائق ذات الصلة (أدوات التقييم والنماذج)

عنوان أداة التقييم والنموذج
أداة تقييم امتثال الخصوصية على مستوى المؤسسة
أداة خصوصية البيانات المتضمنة بالتصميم (باللغة الإنجليزية)
تحليل تأثير حماية خصوصية البيانات الشخصية – المبادئ التوجيهية للمخاطبين بأحكام القانون
أداة إدارة خصوصية الموردين (باللغة الإنجليزية)

الأُطر ذات الصلة المُستخدمة

عنوان الإطار
الإطار الوطني لإدارة الحوادث

1. إخلاء المسؤولية / الحقوق القانونية

أُعدت هذه المذكرة الاستشارية لصالح الجهات المخاطبة بأحكام القانون رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية (يُشار إليه فيما بعد حيثما ورد بـ "القانون")، والتي تقوم بجمع ومعالجة البيانات الشخصية.

تُخلي إدارة حماية خصوصية البيانات الشخصية (يُشار إليها فيما بعد حيثما وردت بـ "الإدارة") بالوكالة الوطنية للأمن السيبراني (يُشار إليها فيما بعد حيثما وردت بـ "الوكالة") مسؤوليتها القانونية عن أي استخدام أو تفسير لهذه المذكرة الاستشارية، بما في ذلك، عدم تحمل الإدارة المسؤولية عن أي عواقب للقرارات أو الإجراءات التي تتخذها المؤسسة استناداً إليها، وتلتزم الجهة المعنية المسؤولية القانونية الكاملة بشأن أي من الممارسات التي تتعلق بحماية خصوصية البيانات الشخصية الخاصة بها، بما في ذلك على سبيل المثال لا الحصر، مراجعة وتحديث سياساتها وإجراءاتها بشكل دوري لضمان الالتزام المستمر بأحكام القانون. ويجوز لكل من يستخدم هذه المذكرة الاستشارية الرجوع إلى مستشار قانوني و/أو مهني للحصول على المشورة القانونية أو غيرها.

ويجب عند إعادة إنتاج هذه الوثيقة، سواء بشكل كلي أو جزئي وبصرف النظر عن وسيلة النسخ، الإشارة إلى الإدارة والوكالة كمصدر ومالك للوثيقة.

وتتطلب أي عملية إعادة إنتاج لهذه الوثيقة، لأي سبب أو غرض، الحصول على إذن خطي مُسبق من الإدارة. وتحتفظ الإدارة بالحق في تقييم مدى صلاحية وقابلية استخدام أي نسخة مكررة من هذه الوثيقة تم إنشائها لأي غرض عام.

ولا يجوز تفسير التفويض الصادر من الإدارة على أنه بمثابة مصادقة على النسخة المعاد إنتاجها، ويتحمل المطوّر المسؤولية الكاملة عن عدم الترويج أو إساءة عرض هذا التفويض بأي وسيلة إعلامية أو في أي مناقشات شخصية أو اجتماعية.

.

2. الأساس القانوني

بالاطلاع على القرار الأميري رقم (1) لسنة 2021 بإنشاء الوكالة الوطنية للأمن السيبراني، وحيث أن إدارة حماية خصوصية البيانات الشخصية (يُشار إليها فيما بعد حيثما وَرَدت بـ "**الإدارة**") منوط به تنفيذ أحكام القانون رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية (يُشار إليه فيما بعد حيثما وَرَد بـ "**القانون**") والقرارات المُنفذة له باعتبارها الإدارة المختصة، وتتولى مباشرة كافة الاختصاصات والصلاحيات اللازمة بشأن التحقيق في الشكاوى المنطوية على وقائع تتعلق باختراق خصوصية البيانات الشخصية، بما في ذلك، اتخاذ ما يلزم من تدابير وقائية وتنظيمية بهذا الشأن.

وعليه، فقد نصت المادة (27) من أحكام القانون على أحقية الإدارة باتخاذ كافة التدابير اللازمة لتطبيق وتنفيذ أحكامه، كما نصت المادة (8/ بند 3) من ذات القانون على اختصاص الإدارة بتحديد الاحتياطات الإدارية والفنية والمادية المناسبة التي يجب على الجهة المخاطبة بأحكام القانون الالتزام بها لضمان امتثالها لأحكام القانون والقرارات الصادرة تنفيذاً له.

أُعدت هذه المذكرة الاستشارية مع الأخذ في الاعتبار القوانين والتشريعات السارية حاليًا في دولة قطر. وفي حال وجود أي تعارض بين هذه الوثيقة وأحكام القوانين القطرية، يُعتد بتلك القوانين والتشريعات، ويُستبعد أي نص يتعارض معها من هذه الوثيقة بالقدر اللازم، دون المساس بباقي أحكامها. وفي هذه الحالة، يجب إدخال التعديلات اللازمة لضمان التوافق مع القوانين والتشريعات المعمول بها في دولة قطر. وتنوه الإدارة بأن ما ورد من أحكام في هذه المذكرة الاستشارية ليست شاملة بشكل كامل، ويجب قراءتها بالاقتران مع أحكام القانون والقرارات الصادرة تنفيذاً له والمبادئ التوجيهية الصادرة عن الإدارة.

المذكرة الاستشارية تكمل المبادئ التوجيهية وتنوي المساهمة في تطبيق حدود الامتثال القانوني، وتقدم توصيات عملية وممارسات مُنظمة ومناهج حوكمة مهمة لتعزيز الامتثال، ودعم المساءلة، وترسيخ إدارة خصوصية البيانات الشخصية ضمن العمليات اليومية. وتشكل المبادئ التوجيهية والمذكرات الاستشارية معاً مجموعة شاملة من الأدوات التي ترسخ من خلالها ارشادات الامتثال لأحكام القانون، بينما تساهم المذكرة الاستشارية في تعزيز ثقافة إدارة المخاطر الاستباقية والمساءلة، مما يسهم في تحسين الموقف المؤسسي المتعلق بخصوصية البيانات الشخصية (كما يشار اليه فيما بعد حيثما وردت بـ "**خصوصية البيانات**").

جدول المحتويات

1. المقدمة

في ظل التحول إلى عصر التكنولوجيا الرقمية الحالية، تُعد المعالجة الآمنة للبيانات الشخصية وإدارتها أمرًا بالغ الأهمية، ومع تزايد الهجمات السيبرانية والاختراقات المتعلقة بتلك البيانات، وبالنظر إلى المتطلبات التنظيمية المنصوص عليها في أحكام القانون، فإن إنشاء برنامج فعال لحماية خصوصية البيانات الشخصية يُعد ضرورة قصوى.

2. نطاق المذكرة الاستشارية

تقدم هذه المذكرة الاستشارية نهجًا منظمًا يساعد المؤسسات على إعداد وتفعيل برنامج لحماية خصوصية البيانات الشخصية، وتقدم خطوات متتابعة تبدأ بوضع استراتيجية للخصوصية وهيكل الحوكمة، تليها تقييم للوضع الحالي لخصوصية البيانات داخل المؤسسة، ثم تنفيذ المتطلبات الخاصة بخصوصية البيانات، وأخيرًا الإجراءات اللازمة لاستدامة برنامج خصوصية البيانات مع مرور الوقت.

وتهدف هذه المذكرة الاستشارية إلى دعم المؤسسات في مواءمة ممارساتها المتعلقة بخصوصية البيانات مع الالتزامات القانونية والتنظيمية ذات الصلة، وأفضل الممارسات المعتمدة في مجال حماية خصوصية البيانات الشخصية، من خلال دمج مفاهيم خصوصية البيانات في العمليات التشغيلية، وتعزيز ثقافة المساءلة والشفافية في معالجة البيانات الشخصية.

وتنطبق هذه المذكرة الاستشارية على جميع الجهات المخاطبة بأحكام القانون في مختلف القطاعات التي تقوم بمعالجة البيانات الشخصية، وتهدف إلى المساعدة في مواءمة ممارسات المؤسسات مع التزامات حماية البيانات والممارسات الفضلى ذات الصلة.

هذه المذكرة الاستشارية موجهة بالدرجة الأولى إلى:

- الإدارة العليا، لوضع آلية الرقابة والمساءلة بشأن خصوصية البيانات الشخصية.
- إدارات (حماية خصوصية البيانات الشخصية، والشؤون القانونية، والمخاطر، والامتثال) المسؤولة عن تنفيذ ضوابط خصوصية البيانات ومراقبتها.
- الوظائف التشغيلية والداعمة المشاركة في معالجة البيانات الشخصية.

ولا تفرض هذه المذكرة الاستشارية حلاً موحداً يناسب جميع الحالات، بل تقدم توصيات قابلة للتكيف يمكن تعديلها وفقًا لحجم المؤسسة وتعقيدها ومستوى المخاطر الخاص بها.

ويمكن تطبيق النهج الموصى به في هذه المذكرة الاستشارية بطريقة قابلة للتدرج، بحيث يمكن اعتماده من قبل المؤسسات بمختلف مراحل نضجها في مجال خصوصية البيانات، سواء في بداية رحلتها أو في إطار تعزيز برنامج خصوصية البيانات القائم لديها.

3. مراحل برنامج حماية خصوصية البيانات الشخصية

يجب أن يتضمن برنامج حماية خصوصية البيانات الشخصية الشامل المراحل التالية:

- **المرحلة الأولى: الأساس الاستراتيجي**: وضع الأطر الأساسية والحوكمة التي تشكّل أساس جميع أنشطة حماية خصوصية البيانات الشخصية.
- **المرحلة الثانية: التقييم**: تقييم وفهم الوضع الحالي لخصوصية البيانات في المؤسسة، ومدى الالتزام، والمتطلبات التنظيمية المطبقة.
- **المرحلة الثالثة: التنفيذ**: تنفيذ الاستراتيجيات المحددة ضمن برنامج خصوصية البيانات.
- **المرحلة الرابعة: الاستدامة**: الحفاظ على برنامج خصوصية البيانات وتحسينه بشكل مستمر.

4. فوائد إنشاء برنامج شامل لحماية خصوصية البيانات الشخصية

فيما يلي بعض الفوائد الرئيسية لإنشاء برنامج منظم وشامل لحماية خصوصية البيانات الشخصية:

- **تحقيق الامتثال التنظيمي**: ضمان الالتزام بأحكام القانون واللوائح والقرارات الصادرة تنفيذاً له.
- **تقليل مخاطر خصوصية البيانات**: تحديد وتقييم والتخفيف من المخاطر المرتبطة بمعالجة البيانات الشخصية والاختراقات المحتملة.
- **تعزيز ثقة أصحاب المصلحة**: إظهار المساءلة والشفافية في التعامل مع البيانات الشخصية.
- **تحسين الكفاءة التشغيلية**: دمج ممارسات خصوصية البيانات ضمن العمليات المؤسسية لتحسين إدارة البيانات الشخصية.
- **تعزيز ثقافة الوعي بخصوصية البيانات**: تعزيز الوعي وتحمل المسؤولية على جميع المستويات داخل المؤسسة.

- **خفض التكاليف**: تقليل التكاليف التشغيلية على المدى الطويل وتقليل مخاطر الغرامات الناتجة عن عدم الامتثال للمتطلبات التنظيمية.

5. المرحلة الأولى: الأساس الاستراتيجي

تركّز هذه المرحلة على وضع الأطر والمبادئ الأساسية التي تقود جميع أنشطة خصوصية البيانات وحمايتها وتشمل إعداد ميثاق لبرنامج خصوصية البيانات، وإنشاء مكتب لخصوصية البيانات، وتحديد التوجه الاستراتيجي لجهود خصوصية البيانات داخل المؤسسة.

5.1 إعداد ميثاق برنامج حماية خصوصية البيانات الشخصية ورؤيته ورسالته

يمثل إعداد ميثاق لبرنامج حماية خصوصية البيانات الشخصية، إلى جانب صياغة رؤية ورسالة واضحتين لممارسات خصوصية البيانات، حجر الأساس الذي يمنح البرنامج اتجاهًا واضحًا وجهدًا مؤسسيًا منظّمًا. ويجب أن يوضح هذا الميثاق نطاق البرنامج وأهدافه والمسؤوليات الرئيسية فيه، بما يتماشى مع الأهداف المؤسسية ومتطلبات الامتثال لمعايير خصوصية البيانات. كما يجب أن تعكس الرؤية والرسالة الأهداف طويلة الأمد للبرنامج، وتُبرز التزام المؤسسة بحماية البيانات الشخصية واعتبار خصوصية البيانات قيمة أساسية.

المرجع: أداة تقييم امتثال الخصوصية على مستوى المؤسسة

5.2 هيكل حوكمة خصوصية البيانات

يضمن هيكل حوكمة خصوصية البيانات أن تكون إدارة خصوصية البيانات جزءًا متأصلاً داخل المؤسسة، وأن تكون هناك مساءلة من خلال تحديد واضح للأدوار والمسؤوليات المُسندة إلى الجهات المعنية لضمان الامتثال لمتطلبات حماية البيانات. ويُعد إنشاء مكتب لخصوصية البيانات محوراً رئيسيًا لمبادرات خصوصية البيانات، حيث يتولى هذا المكتب مسؤولية تطوير وتنفيذ ومتابعة امتثال المؤسسة لأحكام القانون والمتطلبات الأخرى ذات الصلة. ويمكن أن يكون مكتب خصوصية البيانات قسمًا مستقلاً يضم مسؤول حماية البيانات، أو دوراً داخل قسم مناسب آخر (وعادة ما يكون ضمن الإدارة القانونية). ويجب أن يكون مسؤول حماية البيانات في موقع يمكنه من أداء مهامه بكفاءة وحيادية. يجب أن يُمارس مسؤول حماية البيانات مهامه بشكل مستقل، وأن تتركز أنشطته الرئيسية على الإشراف وتنفيذ الأنشطة

الأساسية، لا على الأعمال الثانوية التي يجب أن تُسند إلى وظائف أخرى تبعًا لهياكل المؤسسة، ودرجة تعرضها لمخاطر خصوصية البيانات، وأولوياتها التشغيلية. وفيما يلي بعض الأمثلة على هيكل المسؤوليات، مع توضيح الفوائد والتحديات:

- مكتب أمن المعلومات: يحقق توافقًا بين خصوصية البيانات وتدابير الأمن السيبراني، إلا أنه قد يركز بشكل أكبر على مخاطر الأمن بدلاً من الامتثال الأشمل لمتطلبات خصوصية البيانات.
- مكتب إدارة البيانات: يُدمج خصوصية البيانات ضمن استراتيجيات حوكمة البيانات، لكنه قد يُعطي الأولوية لاستخدام البيانات على حساب الامتثال التنظيمي.
- الإدارة القانونية/الامتثال: يعزز الالتزام بالمتطلبات التنظيمية وإدارة المخاطر، إلا أنه قد يفتقر إلى السيطرة التشغيلية المباشرة على الأمن السيبراني ووظائف البيانات.

ولتفعيل خصوصية البيانات بكفاءة، يُوصى بتعيين "ممثلي خصوصية البيانات" داخل الإدارات المختلفة لضمان إدماج مبادئ خصوصية البيانات ضمن العمليات اليومية. ويعمل ممثلو خصوصية البيانات هؤلاء كحلقة وصل بين مكتب خصوصية البيانات والإدارات، مما يساعد على تعزيز الامتثال ونشر الوعي.

6. المرحلة الثانية: التقييم

تقوم المؤسسة في هذه المرحلة بتقييم وفهم وضع خصوصية البيانات الحالي، والمتطلبات المطبقة، ومستوى الامتثال القائم. ويتضمن ذلك تحديد البيانات الشخصية التي تتم معالجتها، وإجراء تقييم لحالة الامتثال الحالي لخصوصية البيانات، ووضع خارطة طريق لمعالجة أي ثغرات تم تحديدها في الامتثال.

6.1 جرد البيانات الشخصية

تبدأ الخطوة الأولى في مرحلة التقييم بتحديد البيانات الشخصية التي تتم معالجتها داخل المؤسسة من خلال إعداد سجل شامل أو قائمة بجميع أنشطة المعالجة (للمزيد من التفاصيل حول كيفية إعداد هذه السجلات: يرجى الرجوع إلى القسم 4-3 من سجل معالجة البيانات الشخصية - المبادئ التوجيهية للمخاطبين بأحكام القانون).

ويجب تنفيذ هذا النشاط على مستوى وحدة الأعمال/العمليات لضمان التغطية الشاملة لكافة جوانب المؤسسة، ويُعد ذلك ضروريًا لفهم مسار تدفق البيانات داخل المؤسسة. ويشمل هذا النهج تصنيف أنواع

البيانات المختلفة التي تتم معالجتها، وفهم الغرض من معالجتها، وتوثيق مسار تدفق هذه البيانات عبر أنظمة المؤسسة وعملياتها. ويُعد هذا النهج الدقيق ضرورياً لتحديد المخاطر المحتملة على خصوصية البيانات ، ووضع تدابير واضحة للمساءلة.

علاوة على ذلك، يجب أن تخضع سجلات أنشطة المعالجة للمراجعة الدورية للتحقق من وجود أي تغييرات في أنشطة المعالجة الأساسية، وكذلك لضمان إدراج جميع العمليات الجديدة ضمن هذه السجلات.

المرجع: سجل معالجة البيانات الشخصية - المبادئ التوجيهية للمخاطبين بأحكام القانون.

6.2 تقييم الامتثال لمتطلبات خصوصية البيانات ووضع خارطة الطريق

يُعد إجراء تقييم للحالة الراهنة أمراً بالغ الأهمية لتحديد المتطلبات المطبقة وتقييم الثغرات ومستوى مخاطر عدم الامتثال، ويجب أن يقود مكتب خصوصية البيانات هذا التقييم، مع تقديم الدعم الكافي من وحدات الأعمال الأخرى.

وبعد الانتهاء من التقييم، يجب على مكتب خصوصية البيانات، بالتعاون مع أصحاب المصلحة المعنيين، إعداد خارطة طريق تنفيذية قابلة للتطبيق لمعالجة أوجه عدم الامتثال التي تم تحديدها أثناء التقييم. ويجب أن تتضمن هذه الخارطة المبادرات اللازمة للامتثال وخطوات العمل المحددة، إلى جانب الجداول الزمنية المرتبطة بها والجهات المسؤولة عن التنفيذ. ويتعين على مكتب خصوصية البيانات استخدام هذه الخارطة كأداة لتتبع التقدم المحرز فيما يتعلق بمبادرات الامتثال لأحكام القانون.

المرجع: أداة تقييم امتثال الخصوصية على مستوى المؤسسة

7. المرحلة الثالثة: التنفيذ

تتضمن هذه المرحلة تنفيذ الاستراتيجيات الموضحة ضمن برنامج حماية خصوصية البيانات الشخصية. وتشمل الأنشطة الرئيسية وضع وصياغة سياسات وإجراءات خصوصية البيانات، وإدارة دورة حياة البيانات الشخصية، وتقديم إشعارات خصوصية البيانات للأفراد، وإدارة مخاطر خصوصية البيانات المرتبطة بالأطراف الثالثة، والتعامل مع طلبات الأفراد المتعلقة بحقوقهم، والمعالجات ذات الطبيعة الخاصة،

وتنفيذ التدابير الخاصة بإدارة اختراقات البيانات الشخصية، وتطبيق مبدأ "الخصوصية من خلال التصميم".

7.1 وضع السياسات والإجراءات

يجب أن تستند عملية وضع وصياغة سياسات وإجراءات خصوصية البيانات إلى نتائج تقييم حالة الامتثال الحالية وخارطة الطريق التنفيذية، ويُعد وضع سياسات وإجراءات خصوصية شاملة أمرًا ضروريًا لضمان الامتثال لأحكام القانون، ويُنصح بإعداد سياسة داخلية شاملة للخصوصية تُغطي جميع المتطلبات ذات الصلة بخصوصية البيانات داخل المؤسسة، بالإضافة إلى وضع سياسات وإجراءات متخصصة تُركّز بشكل خاص على متطلبات الامتثال لأحكام القانون، مثل إدارة حقوق الأفراد، وحوادث اختراق البيانات، والاحتفاظ بالبيانات وإتلافها، والإشراف على معالجي البيانات، وغير ذلك.

ويجب على مكتب خصوصية البيانات أن يضمن مراجعة جميع السياسات والإجراءات المرتبطة بخصوصية البيانات بشكل دوري، وأن يتم اعتمادها رسميًا من قبل الإدارة العليا، تأكيداً على التزام المؤسسة بخصوصية البيانات ومساءلتها عنها إلى جانب التواصل الفعال بشأن هذه السياسات والإجراءات مع جميع الموظفين، ومراقبة الإدارات المعنية لضمان حصول الموظفين على التدريب المناسب داخل إداراتهم، وأن يكونوا على دراية كافية ولديهم إمكانية الوصول السهل إلى الموارد اللازمة.

المرجع: نظام إدارة حماية البيانات الشخصية - قائمة المراجعة للمخاطبين بأحكام القانون

7.2 إدارة دورة حياة البيانات الشخصية

يتطلب تنفيذ إدارة دورة حياة البيانات الشخصية بما يتوافق مع أحكام القانون اتباع نهج منظم يشمل جميع المراحل من جمع البيانات وحتى التخلص منها، بما يضمن الالتزام بمتطلبات القانون وحماية خصوصية الأفراد. يجب أن تبدأ المؤسسات بجمع البيانات بعناية، مع الاكتفاء بجمع المعلومات الضرورية فقط، والحصول على الموافقة المناسبة (عند الاقتضاء) أو الاعتماد على أساس قانوني آخر مشروع. ويجب أن تُعالج البيانات الشخصية بطريقة آمنة، مع تقييد الوصول إليها ليقتصر على الموظفين المخولين أو أولئك الذين تتطلب مهامهم ذلك تحقيقًا للغرض المحدد من المعالجة. وعند الاقتضاء، يتعين على المؤسسات تنفيذ تقنيات التشفير، وإجراء عمليات تدقيق دورية للتحقق من سلامة وسرية

البيانات. كما يجب تدريب الموظفين أو الأشخاص المعنيين بعملية المعالجة بشكل مناسب، بما في ذلك مشاركة البيانات الشخصية مع طرف ثالث، والإجراءات التي يتعين اتخاذها والإخطارات الواجب إصدارها في حال حدوث اختراق للبيانات. وأخيرًا، من الضروري وضع إجراءات واضحة للتخلص من البيانات الشخصية، بما يتماشى مع سياسات الاحتفاظ بالبيانات لدى المؤسسة والمتطلبات القانونية ذات الصلة.

المرجع: مبادئ خصوصية البيانات - المبادئ التوجيهية للمخاطبين بأحكام القانون

7.3 إشعار خصوصية البيانات الموجه للأفراد

يُعد تقديم إشعارات خصوصية واضحة وموجزة وسهلة الوصول للأفراد بشأن معالجة بياناتهم الشخصية من المتطلبات الأساسية بموجب أحكام القانون. ويجب أن تُقدّم إشعارات خصوصية البيانات كتابيًا، بما في ذلك، عند الاقتضاء، من خلال الوسائل الإلكترونية. وتلتزم المؤسسات بتحديد الفئات المختلفة من الأفراد الذين تتم معالجة بياناتهم الشخصية، والتأكد من تقديم إشعار خصوصية البيانات لهم في وقت جمع البيانات الشخصية. ويجب أن يتضمن إشعار خصوصية البيانات المعلومات التالية بشأن كيفية معالجة بياناتهم الشخصية:

- طلب هوية وتفاصيل الاتصال بالمراقب
- تفاصيل الاتصال بمكتب/مسؤول حماية البيانات الشخصية، عند تعيينه أو وجود قسم مخصص لذلك
- تحديد البيانات الشخصية التي تتم معالجتها، مع تسليط الضوء على ما إذا كانت من البيانات ذات الطبيعة الخاصة
- كيفية جمع البيانات الشخصية
- الأسباب المصرح بها لجمع ومعالجة البيانات الشخصية
- الأسباب المصرح بها للإفصاح عن البيانات الشخصية لأطراف أخرى
- المدة الزمنية التي سيتم الاحتفاظ فيها بالبيانات الشخصية
- وصف آلية تأمين البيانات الشخصية
- الحقوق المختلفة التي يجوز للأفراد ممارستها بموجب أحكام القانون
- حق الأفراد في تقديم شكوى إلى الإدارة المختصة وفقاً لأحكام القانون

- تفاصيل أي عمليات إفصاح عن البيانات إلى خارج إقليم دولة قطر
- تفاصيل أي قرارات تُتخذ آليًا بما في ذلك إعداد الملفات التعريفية

علاوة على ذلك، إذا تم الاعتماد على الموافقة كأساس قانوني لمعالجة البيانات الشخصية، فيجب الحصول على موافقة صريحة من الأفراد من خلال عرض إشعار خصوصية البيانات عليهم.

المرجع: إشعار الخصوصية - المبادئ التوجيهية للمخاطبين بأحكام القانون

7.4 إدارة مخاطر خصوصية البيانات مع الأطراف الثالثة وعبر الحدود

تشكل الأطراف الثالثة التي تعالج البيانات نيابةً عن المؤسسة تحديات ومخاطر فريدة من نوعها. وتبدأ عملية إدارة مخاطر خصوصية البيانات المرتبطة بالأطراف الثالثة بتحديد جميع معالجي البيانات الحاليين، يلي ذلك إبرام اتفاقيات معالجة بيانات تتضمن بنوداً مناسبة بشأن حماية خصوصية البيانات. كما يُنصح بإخضاع معالجي البيانات من الأطراف الثالثة لعمليات تدقيق دورية. وبالإضافة إلى ذلك، يجب التأكد من إجراء العناية الواجبة اللازمة قبل التعاقد مع أي طرف ثالث جديد للعمل كمعالج بيانات.

وفي بعض الحالات، قد يكون الطرف الثالث جهة متحكمة أخرى، وفي هذه الحالة، يجب إبرام وتنفيذ اتفاقية تحكم مشتركة تُحدَّد من خلالها بوضوح مسؤوليات وحدود كل طرف فيما يتعلق بمعالجة البيانات الشخصية.

ولإدارة المخاطر الناتجة عن نقل البيانات عبر الحدود، يجب على المؤسسة اتخاذ ما يلي:

- تحديد وتوثيق جميع عمليات نقل البيانات الشخصية خارج إقليم دولة قطر
- إجراء تقييم للمخاطر لتحديد وإدارة أي مخاطر قد تنشأ عن تلك العمليات
- التأكد من أن الجهة المستقبلة للبيانات والموجودة خارج دولة قطر تُعالج البيانات الشخصية بما يتوافق مع متطلبات أحكام القانون، ويجب ضمان ذلك من خلال اتخاذ تدابير تعاقدية مناسبة.

المراجع:

مراقبي ومعالجي البيانات الشخصية - المبادئ التوجيهية للمخاطبين بأحكام القانون

أداة إدارة خصوصية الموردين (باللغة الإنجليزية)

7.5 برنامج إدارة حقوق الأفراد

يُعد وجود برنامج فعال لإدارة حقوق الأفراد أمرًا أساسيًا بموجب أحكام القانون. ويجب أن يتضمن هذا البرنامج إشعار الأفراد بوجود حقوق خصوصية البيانات الخاصة بهم، وتمكينهم من ممارسة الحقوق التالية في الوقت المناسب:

- 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

عند تلقي طلب من أحد الأفراد لممارسة حقوقه، يتعين على المؤسسة الرد على ذلك الفرد، وتأكيد أنه سيتم التعامل مع الطلب في الوقت المناسب. ويجب كذلك على المؤسسة التحقق من هوية الفرد قبل تنفيذ طلبه، وذلك لمنع الأشخاص ذوي النوايا الخبيثة من ممارسة حقوق تخص آخرين. وفي الحالات التي يكون لدى المؤسسة سبب مشروع لعدم تنفيذ طلب أحد الأفراد، يجب إخطار الفرد بالأسباب التي تقف وراء هذا الرفض.

المرجع: حقوق الأفراد - المبادئ التوجيهية للمخاطبين بأحكام القانون

7.6 إدارة حوادث اختراق خصوصية البيانات الشخصية

تشمل حوادث اختراق خصوصية البيانات الشخصية التدمير الغير مقصود أو غير القانوني أو الضياع أو الكشف غير المصرح به أو الوصول إلى البيانات الشخصية، وهذا يشمل كل من الاختراقات الغير

مقصودة وغير متعمدة. ولإدارة هذه الحوادث بفعالية، يجب على المؤسسات وضع عملية استجابة لحوادث الأمن السيبراني بما يتماشى مع الإطار الوطني لإدارة الحوادث، مع الالتزام بأحكام المادة (14) من القانون والتي تُلزم بإخطار الإدارة المختصة والأفراد المتأثرين، ويجب أن يتم الإخطار خلال 72 ساعة في حال كان من المحتمل أن يؤدي الاختراق إلى ضرر جسيم.

- **الإخطار والتصنيف**: يجب على الموظفين الإبلاغ فوراً عن أي حادثة خصوصية مشتبه بها إلى فرق خصوصية البيانات وأمن المعلومات. ويجب إجراء تقييم أولي لفهم طبيعة ونطاق الاختراق. إذا كان من المحتمل حدوث ضرر جسيم، يجب إخطار الإدارة المختصة والأفراد المتأثرين خلال 72 ساعة. أما في الحوادث التي تؤثر على الأمن السيبراني على المستوى الوطني، فيجب إخطار الوكالة الوطنية للأمن السيبراني خلال ساعتين.
- **بدء الإجراءات**: يجب تشكيل فريق استجابة متعدد التخصصات يضم أعضاء من إدارات خصوصية البيانات، وأمن المعلومات، والشؤون القانونية، والموارد البشرية، والاتصالات يبدء بتوثيق الحادثة، وإجراءات الاحتواء، والحفاظ على الأدلة ذات الصلة، مع تنسيق الخطوات التالية.
- **الاستجابة والتحقيق**: يجب على الفريق تحديد البيانات الشخصية المتأثرة، وطريقة حدوث الاختراق، وتقييم الأثر العام. ويجب إجراء تحليل لأسباب الاختراق الجذرية، وجمع الأدلة الجنائية إذا اقتضى الأمر. كما يجب الحفاظ على التواصل مع أصحاب المصلحة الداخليون والخارجيون، وبدء التنسيق مع فرق الاستجابة لحوادث الأمن السيبراني الخاصة بالقطاعات أو الوكالة الوطنية للأمن السيبراني عند الاقتضاء.
- **العلاج والتعافي**: يجب تنفيذ الإجراءات التصحيحية المناسبة لمنع تكرار الحوادث، بما في ذلك الإصلاحات التقنية، وتقييد الوصول، أو تعديل السياسات. ويجب تقديم إرشادات إضافية للأفراد المتأثرين إذا تم تحديد مخاطر مستمرة.
- **الإغلاق والمراجعة**: يجب إجراء مراجعة رسمية بعد معالجة الاختراق لتحديد الدروس المستفادة وتحسين جهود الاستجابة المستقبلية. كما يجب توثيق الاختراق في سجل المؤسسة، وتحديث الإجراءات الداخلية لتعكس أي ثغرات تم التعرف عليها.

المراجع:

إخطارات اختراق البيانات الشخصية - المبادئ التوجيهية للمخاطبين بأحكام القانون

الإطار الوطني لإدارة الحوادث

7.7 خصوصية البيانات من خلال التصميم

يُعد اتباع نهج شامل لخصوصية البيانات من خلال التصميم أمرًا أساسيًا لدمج اعتبارات خصوصية البيانات في المشاريع والمنتجات والعمليات التجارية الجديدة منذ المراحل الأولى. وتساعد هذه المنهجية في تقليل مخاطر خصوصية البيانات، وقد تؤدي إلى حلول أكثر ابتكارًا وملائمة للخصوصية. وفيما يلي الخطوات الرئيسية لتنفيذ خصوصية البيانات من خلال التصميم بفعالية:

- **تقييم أثر حماية البيانات**: إخضاع جميع العمليات والمشاريع المقترحة لتقييم أثر حماية البيانات لتحديد وتخفيف مخاطر خصوصية البيانات. يجب إجراء هذا التقييم قبل الشروع في أي مبادرة جديدة لضمان الامتثال للأنظمة المتعلقة خصوصية البيانات وحماية حقوق الأفراد.
- **تقييم خصوصية البيانات من خلال التصميم**: التأكد من خضوع المنتجات المقترحة لتقييم خصوصية البيانات من خلال التصميم باستخدام الأداة التي تنشرها الإدارة. يقيّم هذا التقييم تصميم البرنامج للتأكد من تضمين مبادئ خصوصية البيانات من المراحل الأولى، بما في ذلك اعتبارات مثل تقليل البيانات، وموافقة المستخدم، والشفافية، والأمن.
- **دمج خصوصية البيانات في التصميم والعمليات**: ضمان أن تكون خصوصية البيانات مكونًا أساسيًا في هيكلية النظام والعمليات التجارية وتنفيذ تدابير تقنية وتنظيمية تحمي خصوصية البيانات بشكل افتراضي في جميع جوانب المؤسسة.
- **تدريب الموظفين ونشر الوعي**: تدريب الموظفين على مبادئ خصوصية البيانات من خلال التصميم ودورهم في الحفاظ على معايير خصوصية البيانات وإجراء برامج توعوية منتظمة لتحديث الموظفين بأفضل الممارسات والتغيرات التنظيمية.
- **المراجعات والتحديثات الدورية**: مراجعة وتحديث سياسات وإجراءات وممارسات خصوصية البيانات باستمرار لمواكبة التهديدات الجديدة، والتطورات التقنية، والتغيرات التنظيمية. وتساعد التدقيقات والتقييمات المنتظمة في تحديد مجالات التحسين وضمان الامتثال المستمر.

المراجع:

حماية خصوصية البيانات الشخصية المتضمنة بالتصميم والمتضمنة افتراضياً - المبادئ التوجيهية للمخاطبين بأحكام القانون

أداة خصوصية البيانات المتضمنة بالتصميم (باللغة الإنجليزية)

تحليل تأثير حماية خصوصية البيانات - المبادئ التوجيهية للمخاطبين بأحكام القانون

أداة تحليل تأثير حماية خصوصية البيانات - المبادئ التوجيهية للمخاطبين بأحكام القانون

7.8 المعالجة ذات الطبيعة الخاصة

يُعد اتباع نهج شامل لإدارة معالجة البيانات الشخصية ذات الطبيعة الخاصة أمراً جوهريًا لضمان الامتثال لمتطلبات أحكام القانون وحماية خصوصية البيانات للأفراد. وفيما يلي الخطوات الأساسية للإدارة الفعّالة للمعالجة ذات الطبيعة الخاصة:

- **تحديد البيانات الشخصية ذات الطبيعة الخاصة**: تحديد جميع أنشطة المعالجة التي تتضمن معالجة بيانات شخصية ذات طبيعة خاصة.
- **الحصول على إذن**: بالنسبة لأنشطة المعالجة ذات الطبيعة الخاصة التي تم تحديدها، يجب الحصول على إذن مسبق من الإدارة، ويشمل ذلك ما يلي:
  - **إجراء تقييم أثر حماية البيانات**: تحديد المخاطر المرتبطة بالمعالجة والإجراءات المتخذة للتخفيف منها.
  - **تحديد الأسباب والشروط المسموح بها**: توثيق سبب مشروع للمعالجة بالإضافة إلى شرط إضافي لمعالجة البيانات ذات الطبيعة الخاصة ضمن السجلات.
  - **تقديم طلب**: تقديم طلب للحصول على تصريح بشأن معالجة البيانات الشخصية ذات الطبيعة الخاصة إلى الإدارة.

- **تدابير أمنية معززة**: تنفيذ ضوابط أمنية مشددة، مثل التشفير، وضوابط الوصول، وتقنيات إخفاء الهوية، لحماية البيانات الشخصية ذات الطبيعة الخاصة من الوصول غير المصرح به أو الاختراقات.
- **المراقبة والمراجعة**: مراقبة ومراجعة أنشطة معالجة البيانات ذات الطبيعة الخاصة بشكل دوري لضمان الامتثال المستمر للتشريعات المتعلقة بخصوصية البيانات ومعالجة أي مخاطر مستجدة.

المرجع: معالجة البيانات الشخصية ذات الطبيعة الخاصة- المبادئ التوجيهية للمخاطبين بأحكام القانون

8. المرحلة الرابعة: الاستدامة

تركّز المرحلة الأخيرة على الحفاظ على برنامج خصوصية البيانات وتحسينه بشكل مستمر من خلال المراقبة المستمرة وتحسين ممارسات خصوصية البيانات، والحفاظ على برنامج تدريبي فعال للموظفين لضمان فهم جميع العاملين لأدوارهم في الحفاظ على حماية البيانات والامتثال التنظيمي.

8.1 المراقبة والتحسين المستمران

تُعد المراقبة والتحسين المستمرين أمرين ضروريين للحفاظ على الامتثال والتكيف مع التغيرات في بيئة الأعمال أو الإطار التنظيمي. ويجب على المؤسسات القيام بما يلي:

- **مراجعة ممارسات خصوصية البيانات بشكل منتظم**: إجراء تقييمات دورية لممارسات حماية البيانات الشخصية لتحديد مجالات التحسين وضمان الامتثال المستمر للمتطلبات التنظيمية.
- **مواكبة التطورات التشريعية**: البقاء على اطلاع دائم بالتغييرات في قوانين وتشريعات وأنظمة حماية البيانات لضمان استمرار توافق ممارسات المؤسسة مع هذه المتطلبات.
- **إجراء عمليات تدقيق وتقييم**: تنفيذ عمليات تدقيق داخلية وخارجية منتظمة لتقييم فعالية ضوابط خصوصية البيانات وتحديد أية ثغرات أو نقاط ضعف.
- **إجراء تقييمات أثر حماية البيانات وتحديث سجلات أنشطة المعالجة**: استناداً إلى نوع البيانات الشخصية المعالجة ومدى المعالجة وأي تغييرات طرأت عليها، يجب إجراء تقييمات أثر حماية البيانات وتحديث سجلات أنشطة المعالجة بشكل دوري لتقييم التغيرات في مستوى التعرض للمخاطر وتوثيق أي تغييرات في بيئة معالجة البيانات الشخصية.

- **دمج التعليقات**: جمع آراء وتعليقات مختلف أصحاب المصلحة، بما في ذلك الموظفين والعملاء والجهات التنظيمية، ودمجها بهدف تطوير وتحسين برنامج خصوصية البيانات.

8.2 برنامج تدريب الموظفين

يُعد وجود برنامج تدريبي فعّال للموظفين أمرًا أساسيًا لضمان فهم جميع الموظفين لدورهم في الحفاظ على خصوصية البيانات والامتثال. ويجب أن يتضمن البرنامج التدريبي ما يلي:

- **تغطية العناصر الرئيسية لأحكام القانون**: التأكد من إلمام الموظفين بأحكام القانون الرئيسية وفهمهم لمسؤولياتهم بموجبه.
- **ممارسات خصوصية البيانات الخاصة بالمؤسسة**: توعية الموظفين بسياسات وإجراءات وأفضل ممارسات خصوصية البيانات المعتمدة لدى المؤسسة.
- **الاستجابة لطلبات الأفراد**: تدريب الموظفين على كيفية التعامل مع طلبات الأفراد المتعلقة ببياناتهم، بما في ذلك طلبات الوصول، والتصحيح، والحذف.
- **التعامل مع اختراقات البيانات**: تزويد الموظفين بالمعرفة اللازمة للتعرف على اختراقات البيانات الشخصية المحتملة والاستجابة لها، بما يضمن اتخاذ الإجراءات المناسبة وفي الوقت المناسب.
- **التحديثات والدورات التذكيرية المنتظمة**: عقد دورات تدريبية منتظمة ودورات تذكيرية لإبقاء الموظفين على اطلاع بأحدث ممارسات خصوصية البيانات.

يُعد وضع برنامج فعال للامتثال لحماية خصوصية البيانات أمرًا بالغ الأهمية لضمان الالتزام بأحكام القانون ولتوفير حماية شاملة للبيانات الشخصية داخل المؤسسة. ومن خلال اتباع النهج المنظم الموضح في هذه المذكرة الاستشارية، يمكن للمؤسسات تحسين ممارسات خصوصية البيانات لديها بشكل منظم. ولا يقتصر ذلك على ضمان الامتثال القانوني فحسب، بل يُسهم أيضًا في تعزيز الثقة لدى الأفراد وأصحاب المصلحة. ويُعد التحسين المستمر والتدريب المنتظم للموظفين عنصرين أساسيين لمواكبة التحديات المتغيرة في مجال خصوصية البيانات. وأخيرًا، يُسهم برنامج خصوصية البيانات المؤسسي المتكامل في ترسيخ ثقافة خصوصية البيانات وحمايتها باعتبارها قيمة أساسية للمؤسسة.

نهاية الوثيقة