State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

وسائل التواصل الاجتماعي

PDPPL-02050221A

المبادئ التوجيهية للأفراد

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-02050220A	المبادئ التوجيهية لشكاوى الأفراد الموجهة للأفراد
PDPPL-02050214A	المبادئ التوجيهية لشكاوى الأفراد الموجهة للمخاطبين بأحكام القانون
PDPPL-02050219A	المبادئ التوجيهية لحقوق الأفراد الموجهة للأفراد
PDPPL-02050205A	المبادئ التوجيهية لحقوق الأفراد الموجهة للمخاطبين بأحكام القانون

تنويه \ الحقوق القانونية

تم إعداد هذه المبادىء التوجيهية للأفراد الذين تتم معالجة بياناتهم الشخصية إلكترونيًا؛ الذين يتم جمع بياناتهم الشخصية أو استلامها أو استخراجها تحسبًا لمعالجتها إلكترونيًا أو معالجة بياناتهم الشخصية من خلال مجموعة من تقنيات المعالجة الإلكترونية والتقليدية. كما أنها تعمل على توفير المعلومات إلى المراقب والمعالج والأطراف المهتمة الأخرى حول كيفية امتثال المؤسسات لقانون حماية خصوصية البيانات الشخصية PDPPL - (Personal Data Privacy Protection Law).

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 أوكلّي يجب أن تقر شؤون الحوكمة والضمان السيبراني الوطني والوكالة الوطنية للأمن السيبراني كمصدر للوثيقة ومالك لوثيقة "المبادئ التوجيهية لوسائل التواصل الاجتماعي الموجهة للأفراد".

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.

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 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 هذه المبادئ التوجيهية هو تزويد الأفراد بمعلومات حول كيفية حماية خصوصية بياناتهم الشخصية وخصوصيتهم عند استخدام وسائل التواصل الاجتماعي.
- يجب على الأفراد اتباع نهج فعّال للحفاظ على خصوصيتهم عند استخدام هذه الوسائل والمنصات.
- إن استخدام وسائل التواصل الاجتماعي ينتج عنه كميات كبيرة من البيانات الشخصية، حيث أن هذه المعلومة قد لا تكون واضحة للأفراد. إن التفاعل البسيط مثل "الإعجاب" أو "مشاركة" منشور على وسائل التواصل الاجتماعي، قد يولد معلومات حول موقع الفرد أو تفضيلاته الشخصية أو اهتماماته أو شخصيته.
- المعلومات التي يشاركها الأفراد علنًا على وسائل التواصل الاجتماعي معرضة لخطر الحصول عليها وإساءة استخدامها من قبل المراقب بطرق يمكن أن تسبب ضررًا جسيماً للأفراد. بعض الأمثلة على كيفية إساءة استخدام البيانات الشخصية المنشورة على وسائل التواصل الاجتماعي من قبل المراقب هي:
  - الإعلان الموجه للأفراد دون موافقة بناء على تحديد التفضيلات الشخصية المتوفرة بشكل عام.
  - التأثير على الأفراد لاتخاذ إجراء معين من خلال الهندسة الاجتماعية التي يمكن أن تعرض الفرد للخطر.
  - استخدام هذه البيانات الشخصية للتأثير على الفهم السياسى أو الاقتصادي أو الاجتماعى للفرد بعد مراقبة سلوكه.
  - الحصول على المعلومات السرية المتعلقة بمشروع معيّن أو الاستدلال عليها بسبب النشر غير المبالي للفرد.
  - إنشاء حسابات "وهمية" تنتحل شخصية الفرد.
- بعض الأمثلة على الخطوات التي يمكن للأفراد اتخاذها لحماية أنفسهم على منصات وسائل التواصل الاجتماعي هي:
  - مراجعة إعدادات الخصوصية بانتظام على منصات وسائل التواصل الاجتماعي.
  - تقليل حجم المعلومات التي يتم مشاركتها على وسائل التواصل الاجتماعي.
  - الحفاظ على كلمات مرور قوية لتسجيل الدخول إلى منصات وسائل التواصل الاجتماعي.
  - تقييم الطلبات الواردة من مستخدمين آخرين أو حسابات للتأكد من حقيقة شخصيهم وتقليل عدد المستخدمين الذين يتواصلون معهم للحد من شبكة الأفراد والمؤسسات التى يمكنها الوصول إلى مشاركاتهم على وسائل التواصل الاجتماعي.

٢ - المقدمة

غالبًا ما يشمل استخدام وسائل التواصل الاجتماعي مشاركة البيانات الشخصية. تعني طبيعة البيانات الشخصية المتاحة للجميع والتي يمكن الوصول إليها عالميًا على هذه الوسائل أنها متاحة في بعض الأحيان بسهولة للأفراد أو المراقب أو الجهات الفاعلة الأخرى التي قد تسعى إلى استخدامها للضرر بالأفراد أصحاب البيانات.

تظهر وسائل التواصل الاجتماعية الجديدة بانتظام ويتم تحديث المنصات الحالية كما يتم إضافة ميزات جديدة بشكل دائم، لذا يجب على الأفراد اتباع نهج فعّال للنظر في خصوصيتهم عند استخدام هذه المنصات.

تحدد هذه المبادئ التوجيهية الاحتياطات التي يجب على الأفراد اتخاذها عند استخدام وسائل التواصل الاجتماعي لحماية بياناتهم الشخصية وخصوصيتهم.

٣ - ما هي وسائل التواصل الاجتماعي وكيف يتم استخدامها؟

وسائل التواصل الاجتماعي هي منصات أو تقنيات أو خدمات رقمية تمكّن الأفراد من الاتصال بأفراد أو مجموعات أو مؤسسات أخرى لتبادل الأفكار والمعلومات وربما تجارة السلع والخدمات والانخراط في الشبكات الاجتماعية والمجتمعات الافتراضية.

بالإضافة إلى استخدامها من قبل الأفراد، أصبحت وسائل التواصل الاجتماعي أداة قوية بشكل متزايد يقوم باستخدامها المراقب والجهات الفاعلة الأخرى لتعزيز مصالحهم من خلال التعامل مع الأفراد، من بين أسباب أخرى، من أجل:

- تحسين المشاركة؛
- التسويق المستهدف؛
- زيادة الوعي بالعلامة التجارية والولاء لها؛
- جمع التعليقات لتحسين خدماتهم.

يقوم العديد من مراقبي البيانات بتوجيه أنشطتهم على أفراد معينين باستخدام البيانات الشخصية التي نشرها الأفراد على الإنترنت.

٤ - كيف يمكن للمراقب إساءة استخدام البيانات التي يشاركها الأفراد على وسائل التواصل الاجتماعي؟

يفرض استخدام وسائل التواصل الاجتماعي العديد من المخاطر على حماية خصوصية الأفراد والبيانات الشخصية نظرًا للطبيعة العامة للمنصات وكيفية تخزين البيانات الشخصية ومشاركتها.

يتعرض الأفراد باستمرار لكثير من المعلومات التي لا يتم التحكم فيها بالضرورة أو التحقق من صحتها من أجل الدقة أو الملاءمة وعادة ما يتم تشجيعهم على مشاركة المعلومات على وسائل التواصل الاجتماعي. قد يشارك الأفراد أيضًا معلومات أكثر مما يدركون ويجب أن يدركوا أن أي نشاط صغير يتم إجراؤه على منصة وسائل التواصل الاجتماعي يولد بيانات يمكن تتبعها إلى الفرد (ومن ثم تشكل بيانات شخصية). على سبيل المثال، كل "إعجاب" أو "مشاركة" على منصة وسائل التواصل الاجتماعي يولد بيانات شخصية حول اهتمامات الفرد ويمكن لهذه المؤسسات استخدامها للتأثير على الفرد لشراء منتج أو خدمة.

تم تصميم معظم منصات التواصل الاجتماعية بطريقة تجعل من السهل الاشتراك فيها. وبالتالي، زادت وسائل التواصل الاجتماعي الناجحة عدد المستخدمين النشطين بشكل كبير مما جعل المزيد من البيانات متاحة لمراقبي البيانات بشكل أكبر.

يمكن للمراقب الوصول إلى كمية هائلة من البيانات التي تم إنشاؤها بواسطة الأفراد على وسائل التواصل الاجتماعي بسهولة تامة. بالإضافة إلى ذلك، يمكن للمراقب الحصول على بيانات شخصية عن نفس الشخص من وسائل التواصل الاجتماعية المتعددة ودمج مجموعات البيانات هذه.

يمكن إساءة استخدام هذه البيانات لتحقيق مكاسب للمراقب من خلال أحد الإجراءات التالية:

- الإعلان الموجه للتأثير على الفرد لشراء منتج أو خدمة. يتم جعل هذه الإعلانات المستهدفة فعّالة من خلال جذب المصالح والاهتمامات الخاصّة للفرد، والتي لن يكون من السهل استهدافها من خلال وسائل الإعلام التقليدية.
- سرقة هوية الفرد من خلال إنشاء ملف تعريف "مزيف" للفرد على وسائل التواصل الاجتماعية. يمكن استخدام ملف التعريف المزيف هذا للحصول على معلومات سرية أو للتأثير على الأفراد الذين لن يتأثروا بخلاف ذلك الملف الشخصي "الحقيقي".
- حيل الهندسة الاجتماعية التي يمكن استخدامها لسرقة الأموال للأفراد، على سبيل المثال مؤسسة ضارّه تنشئ متجرًا مزيفًا عبر الإنترنت يسرق من الأفراد من خلال "بيع" منتجات أو خدمات بطريقة تبدو حقيقية.
- بيع السلع والخدمات غير المشروعة التي لن تكون ممكنة عبر وسائل الإعلام التقليدية أصبح ممكناً على وسائل التواصل الاجتماعي. يستهدف هؤلاء البائعون الأفراد بالارتكاز على بياناتهم الشخصية التي يولدونها أو يقومون بمشاركتها.
- عند استخدام الفرد لمنصات وسائل التواصل الاجتماعي، فقد يتسبب هذا في معرفة موقع الفرد بشكل واضح من قبل المراقب.
- يمكن تجميع بيانات الأفراد من أكثر من منصة لوسائل التواصل الاجتماعي وبيعها لأطراف ثالثة دون موافقة الفرد أو حتى معرفته.
- قد لا يتم حذف بيانات الأفراد من منصات وسائل التواصل الاجتماعي، حتى إذا قام الفرد بحذف ملفه الشخصي من منصة وسائل التواصل الاجتماعي.
- يمكن لمخترقي البيانات والأنظمة استخدام وسائل التواصل الاجتماعي لتثبيت برامج ضارّة على أجهزة الكمبيوتر الفردية، مما قد يؤدي لمخاطر متعلقه ببيانات الأفراد الشخصية.

- قد لا تطبق منصات وسائل التواصل الاجتماعي الاحتياطات المناسبة كما هو مطلوب من قبل قانون حماية خصوصية البيانات الشخصية (PDPPL) لحماية بيانات الأطفال. الأطفال عرضة للتأثر بسهولة بهذه المنصات لوسائل التواصل الاجتماعي.

٥ - ما الذي يجب على الأفراد فعله لحماية خصوصيتهم على وسائل التواصل الاجتماعي؟

هناك عدد من الخطوات التي يمكن للأفراد اتخاذها لحماية خصوصيتهم وبياناتهم الشخصية عند استخدام وسائل التواصل الاجتماعي. وتشمل هذه:

- **مراجعة إعدادات الخصوصية:** يجب على الأفراد مراجعة وتحديث إعدادات الخصوصية الخاصة بهم بانتظام للأنظمة الأساسية وحسابات منصات وسائل التواصل الاجتماعي لتقليل عدد الأشخاص والمؤسسات التي يمكنها عرض أنشطتهم.
- **تقليل مشاركة المعلومات الشخصية**: يجب على الأفراد تقليل البيانات الشخصية التي يشاركونها عن أنفسهم عبر الإنترنت والنظر في كيفية استخدام الممثلين ذوي النوايا السيئة لمثل هذه المعلومات. قد تكون هذه البيانات الشخصية تفضيلات، على سبيل المثال "الإعجابات" و "المشاركات" والصور ومقاطع الفيديو والاختبارات أو المشاركات عبر الإنترنت التي تعبر عن وجهات النظر التي يمكن تحليلها للكلمات الرئيسية بواسطة أجهزة الكمبيوتر لتحديد وجهات نظرهم وتفضيلاتهم.
- **تطوير الوعي بكيفية استخدام البيانات الشخصية في المجال العام:** يجب أن يكون الأفراد على دراية بمدى إنشاء البيانات الشخصية من خلال أفعالهم عبر الإنترنت، وكيف يمكن استخدامها لتحليل أفعالهم وتفضيلاتهم ومعتقداتهم وما إلى ذلك. كما يجب أن يكون الأفراد على دراية بشكل مستمر حول كيفية استخدام وسائل التواصل الاجتماعي هذه أو إساءة استخدامها للبيانات الشخصية التي تمت مشاركتها أو إنشاؤها على هذه الوسائل، خاصّة في ضوء أي حالات إساءة استخدام تم الإبلاغ عنها بواسطة وسائل التواصل الاجتماعي.
- **الحفاظ على كلمات مرور قوية:** يجب على الأفراد استخدام كلمات مرور قوية حيث يجب تغييرها بشكل مستمر. نصائح لكلمة مرور جيدة هي:
    - استخدام كلمات مرور طويلة، كلما كانت أطول كان ذلك أفضل؛
    - استخدام الأرقام والأحرف الخاصّة والحروف الكبيرة والصغيرة؛
    - عدم استخدام معلومات شخصية واضحة (الاسم ، مدينة الميلاد ، إلخ) يمكن تخمينها بواسطة معارف الفرد؛
    - عدم استخدام نفس كلمة المرور لمنصتين أو أكثر؛
    - استخدام تطبيق موثوق به لإدارة كلمات المرور؛
    - تغيير كلمات المرور بانتظام.
- **قصر "الأفراد أو الجهات التي يتم التواصل معها" على الأفراد المعروفين:** يجب على الأفراد ألّا يقبلوا كل طلب اتصال يتلقونه عبر الإنترنت.
- **لا تنقر على روابط مريبة:** يمكن بسهولة توزيع البرامج الضارة على الإنترنت.
- **الإبلاغ عن أي نشاط مشبوه** على منصة وسائل التواصل الاجتماعي.
- **رفع شكوى إلى** شؤون الحوكمة والضمان السيبراني: فيما يخص المراقب الذي يعالج البيانات الشخصية بطريقة لا تتوافق مع قانون حماية خصوصية البيانات الشخصية (PDPPL).

لمزيد من المعلومات حول حقوق الأفراد وشكاوى الأفراد، يرجى الاطّلاع إلى المبادئ التوجيهية لحقوق الأفراد و المبادئ التوجيهية لشكاوى الأفراد الموجهة للمخاطبين بأحكام القانون والأفراد.

نهاية الوثيقة