State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

مراقبي ومعالجي البيانات الشخصية

PDPPL-02050209A

المبادئ التوجيهية للمخاطبين بأحكام القانون

شؤون الحوكمة والضمان السيبراني الوطني

الإصدار: ٢,٠

تاريخ الإصدار الأولي: نوفمبر ٢٠٢٠

تاريخ التحديث الأخير: سبتمبر٢٠٢٢

تصنيف الوثيقة: عام

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	سبتمبر٢٠٢٢

الوثائق ذات صلة

الرقم المرجعي للوثيقة	اسم الوثيقة
PDPPL-02050208A	المبادئ التوجيهية لحماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً الموجهة للمخاطبين بأحكام القانون
PDPPL-02050205A	المبادئ التوجيهية لحقوق الأفراد 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)

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 لمراقبي ومعالجي البيانات الشخصية 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 قبل 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 (١) لسنة ٢٠٢١، فإن شؤون الحوكمة والضمان السيبراني الوطني مخولة من قبل الوكالة الوطنية للأمن السيبراني باعتبارها هي الإدارة المختصة بتطبيق القانون رقم (١٣) لسنة ٢٠١٦ بخصوص قانون حماية خصوصية البيانات الشخصية.

تتطلب 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.

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، والمبادئ التوجيهية الصادرة عن شؤون الحوكمة والضمان السيبراني الوطني وأي قرارات وزارية ذات صلة.

قائمة المحتويات

١ - النقاط الرئيسية 6
٢ - المقدمة 8
٢,١ - كيف يمكن تحديد ما إذا كان الشخص أو المؤسسة تعتبر مراقب أو معالج للبيانات؟ 8
٣ - الاعتبارات التي يجب أخذها في الاعتبار من قبل المراقب 9
٣,١ - كيف يحدد مراقب البيانات المعالج المكلّف المسؤول عن حماية البيانات الشخصية؟ 9
٣,٢ - كيف يقوم المراقب بمراجعة إجراءات حماية الخصوصية عند تكليف معالج؟ 9
٣,٣ - كيف يتحقق المراقب من امتثال المعالج المكلّف للتعليمات والاحتياطات المناسبة؟ 10
٤ - الاعتبارات التي يجب أخذها في الاعتبار من قبل المعالج 11
٤,١ - ما هي مسؤوليات معالج البيانات؟ 11
٥ - الاعتبارات التعاقدية لكل من المراقب والمعالج 12
٥,١ - ما أهمية الاتفاق التعاقدي؟ 12
٥,٢ - ما الذي يجب تضمينه في العقود؟ 12
٥,٣ - ما هي تفاصيل معالجة البيانات الشخصية التي يجب تضمينها في العقود؟ 13
٥,٤ - ما الذي يجب تضمينه في العقود حول تعليمات المراقب الموجهة للمعالج؟ 14
٥,٥ - ما هي الإجراءات المناسبة الخاصة بأمن المعلومات التي يجب تضمينها في العقود؟ 14
٥,٦ - ماذا الذي يجب أن تنص عليه العقود حول تكليف معالج بيانات من الباطن؟ 15
٥,٧ - ما الذي يجب أن تشمله العقود حول سرية البيانات؟ 16
٥,٨ - ماذا الذي يجب أن تنص عليه العقود حول حقوق الأفراد؟ 16
٥,٩ - ما هي المساعدة التي يجب توفيرها للمراقب من قبل المعالج؟ 17
٥,١٠ - ما هي التزامات التدقيق والمراجعة التي يجب تضمينها في العقود؟ 18
٥,١١ - ماذا يجب أن يحدث للبيانات الشخصية عند نهاية الاتفاق التعاقدي؟ 19

١ - النقاط الرئيسية

- الغرض من هذه المبادئ التوجيهية هي توضيح من هو "مراقب البيانات" و من هو "معالج البيانات" بموجب قانون حماية خصوصية البيانات الشخصية وكيفية امتثال المراقب لالتزاماته بما في ذلك استخدام العقود لتأكيد الامتثال مع قانون حماية خصوصية البيانات الشخصية لأي معالج بيانات مكلّف من قبل المراقب.
- يضع قانون حماية خصوصية البيانات الشخصية متطلبات مرتبطة بالمراقب والمعالج لحماية خصوصية البيانات الشخصية وخصوصية الأفراد في دولة قطر.
    - تعتبر أي مؤسسة هي "مراقب للبيانات" فيما يتعلق بنشاط معالجة بيانات شخصية إذا كانت هي صانع القرار الرئيسي التي تمارس السيطرة الشاملة على سبب وكيفية معالجة البيانات الشخصية.
    - تعتبر أي مؤسسة هي "معالج للبيانات" فيما يتعلق بنشاط معالجة بيانات شخصية إذا كانت تتبع تعليمات المراقب أو تقوم بمعالجة البيانات الشخصية نيابة عن المراقب.
    - تعتبر أي مؤسسة هي "معالج مشترك" فيما يتعلق بنشاط معالجة بيانات شخصية إذا قامت باتخاذ قرارات بشكل مشترك أو ممارسة سيطرة مشتركة على سبب وكيفية معالجة البيانات الشخصية مع مراقب آخر.
- تشمل مسؤوليات المراقب النقاط التالية:
    - القيام بإجراءات استقصائية عن المعالج لتقييم ما إذا كانت لديه الاحتياطات المناسبة لحماية خصوصية البيانات الشخصية.
    - التحقق من امتثال المعالج المكلّف من قبل المراقب لقانون حماية خصوصية البيانات الشخصية وتعليمات المراقب وأن لدى المعالج الاحتياطات المناسبة المعمول بها قبل وأثناء وبعد الانتهاء من معالجة البيانات الشخصية التي يقوم بها نيابة عن المراقب. للقيام بذلك، سيحتاج المراقب إلى عقد مكتوب لإضفاء الطابع الرسمي على العلاقة.
    - إبلاغ الأفراد و / أو شؤون الحوكمة والضمان السيبراني الوطني في الوقت المناسب بعد أن يصبح على علم بأي خروقات لقانون حماية خصوصية البيانات الشخصية أو حروقات الإجراءات التي لديه لحماية خصوصية البيانات الشخصية أو إذا ظهر أي خطر يهدد البيانات الشخصية التي تتم معالجتها.

- تشمل مسؤوليات المعالج النقاط التالية:
  - الالتزام بمبادئ وأحكام قانون حماية خصوصية البيانات الشخصية وتطبيق الإجراءات المناسبة لحماية خصوصية البيانات الشخصية بشكل مستقل ومنفصل عن أي مراقب تتم المعالجة بالنيابة عنه.
  - إبلاغ المراقب في الوقت المناسب عند العلم بأي خروقات لقانون حماية خصوصية البيانات الشخصية أو خروقات للإجراءات المتبعة من قبل المعالج لحماية خصوصية البيانات الشخصية أو إذا ظهر أي خطر يهدد البيانات الشخصية التي تتم معالجتها.

٢ - المقدمة

يتطلب قانون حماية خصوصية البيانات الشخصية من المراقب التأكد من امتثال أي معالج طرف ثالث مكلّف للتعليمات التي يقدمها له واعتماد الاحتياطات المناسبة، كما يجب مراقبة هذا الامتثال بشكل منتظم كجزء من نظام إدارة البيانات الشخصية (PDMS). المعالج هو أي شخص أو مؤسسة تقوم بمعالجة البيانات الشخصية بالنيابة عن المراقب، أو وفقًا للتعليمات المأخوذه منه.

يجب على المراقب وضع إجراءات للتأكد من أن المعالج المكلّف لمعالجة البيانات الشخصية يتوافق مع متطلبات قانون حماية خصوصية البيانات الشخصية، وعلى وجه الخصوص يجب أن يتضمن عمل المعالج التالي:

- متابعة أي تعليمات يقدمها المراقب؛
- تأسيس نظام إدارة بيانات شخصية (PDMS) متوافق وممتثل مع المتابعة المنتظمة له؛
- تأسيس الاحتياطات الإدارية والتقنية والمالية المناسبة لحماية خصوصية البيانات الشخصية مع المتابعة المنتظمة له؛
- حماية حقوق الأفراد بموجب قانون حماية خصوصية البيانات الشخصية.

يمكن الإطّلاع على تعريفات المراقب والمعالج في المادة ١ من قانون حماية خصوصية البيانات الشخصية. يمكن الإطّلاع على المتطلبات الرئيسية للمراقب والمعالج في المواد ٨ و ١١ و ١٣، ويتم شرح كل متطلب بمزيد من التفاصيل أدناه

٢,١ - كيف يمكن تحديد ما إذا كان الشخص أو المؤسسة تعتبر مراقب أو معالج للبيانات؟

يقدم قانون حماية خصوصية البيانات الشخصية تعريفات المراقب والمعالج بموجب المادة ١ من قانون حماية خصوصية البيانات الشخصية.

تنص المادة ١ من قانون حماية خصوصية البيانات الشخصية على ما يلي:

"تكون للكلمات والعبارات التالية، المعاني الموضحة قرين كل منها..."

المراقب: **الشخص الطبيعي أو المعنوي** الذي يقوم منفرداً أو الاشتراك مع آخرين بتحديد **كيفية معالجة البيانات الشخصية** والغرض منها.

المعالج: **الشخص الطبيعي أو المعنوي** الذي يقوم **بمعالجة البيانات الشخصية لصالح المراقب.**

إن الدور التي تقوم به المؤسسة في تحديد الغرض من معالجة البيانات الشخصية يحدد ما إذا كانت المؤسسة هي "مراقب للبيانات"، "مراقب مشترك"، أو "معالج للبيانات" كما هو موضح في النقاط الرئيسية.

٣ - الاعتبارات التي يجب أخذها في الاعتبار من قبل المراقب

٣,١ - كيف يحدد مراقب البيانات المعالج المكلّف المسؤول عن حماية البيانات الشخصية؟

تنص المادة ١١ من قانون حماية خصوصية البيانات الشخصية على ما يلي:

"على المراقب اتخاذ الإجراءات التالية:

١. **مراجعة إجراءات حماية الخصوصية** قبل إدراج عمليات معالجة جديدة.

٢. **تحديد المعالجين المسؤولين** عن حماية البيانات الشخصية...."

لكي يتمكن المراقب من الامتثال للمادة ١١,٢ من قانون حماية خصوصية البيانات الشخصية، يتوجب عليه تحديد قائمة معالجين البيانات المستخدمين من قبله. يمكن للمراقب تحديد معالجين البيانات المستخدمين حالياً من خلال عدة وسائل والتي تشمل ولا تقتصر على:

- مراجعة العقود من المعالج لتحديد تلك التي تتعلق بالخدمات التي تتطلب معالجة بيانات شخصية أو نقل البيانات الشخصية من قبل أو لمعالج طرف ثالث؛
- إعداد وجمع سجلات لجميع معالجات البيانات الشخصية الخاصة بالمراقب، وتحديد المعالجين كجزء من هذا الإجراء؛
- إعداد مخطط تدفق البيانات الفنية لتحديد البيانات الشخصية التي يتم نقلها من مؤسسة المراقب إلى مؤسسة المعالج.

قد يقوم المراقب بتنفيذ أي من هذه الأنشطة أو جميعها لإعداد رؤية كاملة للمعالجين المستخدمين. كما يجب على المراقب تحديد الوسائل المناسبة للقيام بذلك وتوثيق هذا القرار لإثبات الامتثال إذا لزم ذلك من قبل شؤون الحوكمة والضمان السيبراني.

٣,٢ - كيف يقوم المراقب بمراجعة إجراءات حماية الخصوصية عند تكليف معالج؟

المراقب مسؤول عن القيام بإجراءات استقصائية عن المعالج لتقييم ما إذا كانت لديه الاحتياطات المناسبة لحماية خصوصية البيانات الشخصية. لجمع المعلومات المطلوبة من المعالج، يمكن للمراقب إجراء التالي:

- إجراء تحليل تأثير حماية خصوصية البيانات الشخصية (DPIA) مع المعالج، بالإضافة الى جمع معلومات منهم كجزء من هذا التقييم؛
- القيام بالطلب من المعالج تقديم معلومات بشأن احتياطاته لحماية خصوصية البيانات الشخصية لتمكين المراقب من إكمال إجراء تحليل تأثير حماية خصوصية البيانات الشخصية (DPIA). يجب أن يتم ذلك عند تصميم و / أو تغيير و / أو تطوير المنتجات والأنظمة والخدمات التي تعالج البيانات الشخصية وقبل الشروع في العمليات الجديدة وفقًا لمتطلبات المادتين (٢) ٨ و ١١,١ من قانون حماية خصوصية البيانات الشخصية .

يجب على المراقب أن يأخذ الوقت الكافي لتقييم الاحتياطات المطبقة من قبل كل معالج مرتبطة بجميع الأنشطة المتعلقة بالبيانات الشخصية وأنشطة المعالجة التي يقوم بها المعالج بالنيابة عن المراقب وتوثيق مثل هذه التقييمات.

يجب أن يقوم المراقب بتوثيق قراره بشأن ما إذا كان المعالج قد وضع الاحتياطات المناسبة وأن يتضمن القرار المعلومات المقدمة من المعالج. كما يجب أن يتضمن هذا تحليلاً لكيفية تحديد المراقب أن احتياطات المعالج تتناسب مع طبيعة نشاط المعالجة وما إذا كانت تخفف بشكل كافٍ من مخاطر حدوث أضرار جسيمة للأفراد.

٣,٣ - كيف يتحقق المراقب من امتثال المعالج المكلّف للتعليمات والاحتياطات المناسبة؟

تنص المادة ١١,٨ من قانون حماية خصوصية البيانات الشخصية على ما يلي:

"على المراقب:

التحقق من التزام المعالج بالتعليمات التي يوجهها إليه، **واتخاذ الاحتياطات المناسبة** لحماية البيانات الشخصية، ورصد ومتابعة ذلك بصفة مستمرة".

المراقب هو المسؤول عن تأكيد امتثال المعالج لقانون حماية خصوصية البيانات الشخصية ولتعليمات المراقب. بالاضافة يجب التأكد من أن لدى المعالج الاحتياطات المناسبة قبل وأثناء وبعد الانتهاء من معالجة البيانات الشخصية التي يقوم بها المراقب نيابة عن المعالج.

يعتبر وضع مسؤوليات ملزمة قانونياً لحماية خصوصية البيانات الشخصية من خلال اتفاق تعاقدي هو الإحتياط الإداري المناسب عند تكليف معالج للبيانات.

قبل البدء بمعالجة البيانات الشخصية، يترتب على المراقب إجراء الآتي:

بعد مراجعة المراقب لإجراءات حماية خصوصية البيانات المطبقة من قبل المعالج، يجب أن ينفذ المراقب عقدًا بينه وبين المعالج يحدد فيه مسؤوليات معالجة البيانات الشخصية ومشاركتها قبل البدء بمعالجة البيانات الشخصية.

- المراقبة المنتظمة لامتثال المعالج للعقد والإجراءات الإدارية والتقنية والمالية المناسبة المتفق عليها؛
- تنفيذ أي إجراءات تدقيق أو مراجعة منصوص عليها في العقد المتفق عليه.

بعد الانتهاء من معالجة البيانات الشخصية، تماشيا مع مبادئ تحديد الغرض والحد من التخزين، يترتب على المراقب إجراء الآتي:

- توجيه المعالج للتوقف عن معالجة البيانات الشخصية بمجرد تحقيق الغرض من المعالجة أو انتهاء وجود الغرض؛
- التأكد من أن المعالج قد قام بمحو هذه البيانات المعالجة إذا لم يعد تخزينها ضروريًا.

٤ - الاعتبارات التي يجب أخذها في الاعتبار من قبل المعالج

٤,١ - ما هي مسؤوليات معالج البيانات؟

يحدد قانون حماية خصوصية البيانات الشخصية أن المعالج مسؤول عن اتخاذ الاحتياطات المناسبة لحماية خصوصية البيانات الشخصية بشكل مستقل عن أي مراقب تتم المعالجة نيابتاً عنه. كما أن المعالج مطالب بالامتثال لأية احتياطات منصوص عليها في أي اتفاقيات تعاقدية يعقدونها مع المراقب. تساهم هذه الاحتياطات في تعزيز وتمكين نظام إدارة البيانات الشخصية (PDMS) الخاص بالمعالج وتثبت امتثاله لمبادئ وأحكام قانون حماية خصوصية البيانات الشخصية.

تنص المادة ١٣ من قانون حماية خصوصية البيانات الشخصية 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. ويجب أن تكون تلك الاحتياطات **متناسبة مع طبيعة وأهمية البيانات الشخصية** المراد حمايتها. وعلى المعالج أن **يخطر المراقب بوجود أي إخلال بالاحتياطات** المشار إليها، أو عند حدوث أي خطر يهدد البيانات الشخصية للأفراد بأي وجه، فور علمه بذلك".

إذا كان المعالج يقوم بمعالجة البيانات الشخصية نيابة عن المراقب، فيجب عليه إبلاغ المراقب في الوقت المناسب عند معرفة أو إدراك أحد الأحداث التالية:

- يعاني المعالج من اختراق قد ينتج عنه ضياع أو تلف أو تغيير أو إفشاء و / أو وصول غير قانوني / غير مقصود إليه و / أو استخدامه غير قانوني للبيانات؛
- أن إجراءات المعالج الإدارية والفنية والمالية لحماية البيانات الشخصية قد تعرضت للخطر؛
- هنالك خطر يؤثر على البيانات الشخصية التي يقوم المعالج بمعالجتها.

يمكّن طلب الإبلاغ هذا المراقب من اتخاذ خطوات لمعالجة الخروقات والوفاء بالتزامات إخطار الخروقات بموجب قانون حماية خصوصية البيانات الشخصية.

٥ - الاعتبارات التعاقدية لكل من المراقب والمعالج

كما هو موضح أعلاه، فإن المراقب ملزم قانونياً لتأكيد امتثال المعالج المكلّف بموجب المادة (٨) ١١ من قانون حماية خصوصية البيانات الشخصية، وكذلك اتخاذ الاحتياطات المناسبة لحماية خصوصية البيانات الشخصية التي يقوم المراقب بمعالجتها. لكي يتمكن المراقب من تنفيذ هذا الالتزام القانوني والتأكد من هذا الامتثال، فإنه يجب وضع عقد مكتوب لإضفاء الطابع الرسمي على العلاقة بين المراقب والمعالج المكلّف.

الغرض من هذا القسم من المبادئ التوجيهية هو دعم المنظمات في فهم الأحكام التعاقدية التي ينبغي وضعها والأسباب الكامنة وراء هذه الأحكام.

٥,١ - ما أهمية الاتفاق التعاقدي؟

على الرغم من اعتباره التزامًا قانونيًا بموجب المادة (٨) ١١ من قانون حماية خصوصية البيانات الشخصية، فإن وجود عقد مكتوب بين المراقب والمعالج مهم حتى يتمكن كلا الطرفين من إدراك الالتزامات والمسؤوليات فيما يتعلق بالبيانات الشخصية التي يعالجونها

تمكن أهمية الاتفاق التعاقدي في التأكد من وجود النقاط التالية:

- يمكن للمراقب والمعالج التأكد بسهولة أكبر على أنهما يمتثلان لالتزاماتهما بموجب قانون حماية خصوصية البيانات الشخصية؛
- البيانات الشخصية للعملاء والموظفين وغيرهم محمية بشكل كاف وفعّال للمعايير المطلوبة بموجب قانون حماية خصوصية البيانات الشخصية؛
- يدرك المراقب والمعالج ادوارهما بوضوح الأدوار فيما يتعلق بالبيانات الشخصية التي تتم معالجتها؛
- يمكن للمراقب والمعالج أن يثبتا أنهما ينفذان ما هو مطلوب منهم تجاه الأفراد وشؤون الحوكمة والضمان السيبراني.

٥,٢ - ما الذي يجب تضمينه في العقود؟

يجب أن تحدد العقود، سواء كانت بين المراقب والمعالج أو بين المعالج والمعالج المكلّف من الباطن تفاصيل المعالجة، وتحديداً:

- موضوع ومدة معالجة البيانات الشخصية؛
- طبيعة معالجة البيانات الشخصية والغرض منها؛

- نوع البيانات الشخصية الجاري معالجتها، وفئات الأفراد المعنيين؛
- واجبات وحقوق مراقب البيانات.

يجب أن تتضمن العقود أيضًا أحكامًا محددة تتعلق بما يلي:

- يجب على المعالج معالجة البيانات الشخصية فقط وفقًا لتعليمات المراقب الموثقة؛
- الإجراءات الأمنية المناسبة؛
- استخدام معالج بيانات من الباطن؛
- الواجبات تجاه سرية البيانات؛
- حقوق الأفراد؛
- المساعدة التي يجب أن يوفرها المعالج للمراقب؛
- الحقوق المتعلقة بالتدقيق والإجراءات التفتيشية؛
- ما هي الإجراءات التي يجب فعلها عند انتهاء الاتفاق التعاقدي.

يرد مزيد من التفاصيل حول كل من هذه المتطلبات أدناه.

٥,٣ - ما هي تفاصيل معالجة البيانات الشخصية التي يجب تضمينها في العقود؟

لا بد من أن تتّسم العلاقة ومنذ البداية بين المراقب والمعالج بالشفافية والوضوح فيما يتعلق بمدى معالجة البيانات الشخصية التي يتم التعاقد عليها وتكليفها للمعالج.

يجب أن يتضمن العقد التفاصيل التالية حول معالجة البيانات الشخصية:

- موضوع المعالجة ومدتها وطبيعتها. هذا يعني تحديد الغرض من معالجة البيانات الشخصية، المدة الزمنية للمعالجة، وتفاصيل عن كيفية إجراء المعالجة؛
- نوع البيانات الشخصية الجاري معالجتها؛ على سبيل المثال فئات البيانات الشخصية مثل الأسماء والعناوين وتواريخ الميلاد وما إلى ذلك؛

- فئات الأفراد الذين تتم معالجة بياناتهم الشخصية؛ على سبيل المثال العملاء والموظفين والأطراف الثالثة وما إلى ذلك؛
- واجبات وحقوق مراقب البيانات.

٥,٤ - ما الذي يجب تضمينه في العقود حول تعليمات المراقب الموجهة للمعالج؟

يجب أن ينص العقد على أنه لا يمكن للمعالج معالجة البيانات الشخصية إلا بناء على تعليمات المراقب المكتوبة، بما في ذلك فيما يتعلق بنقل البيانات الشخصية خارج دولة قطر. تكون الحالة المذكورة مطبّقة ما لم يُطلب من المعالج معالجة البيانات الشخصية بموجب متطلب قانوني آخر.

يجب أن تكون التعليمات المكتوبة للمراقب:

- يتم توثيقها وحفظها في مكان ما بحيث يكون هناك سجل للتعليمات؛
- توضح أن المراقب وليس المعالج هو الذي يتحكم بشكل مطلق في ما يحدث للبيانات الشخصية.

إذا كان المعالج يعمل خارج تعليمات المراقب وقام باتخاذ القرارات بشكل فردي حول ما يجب القيام به بخصوص البيانات الشخصية، فإن المعالج معرض لخطر أن يعتبر هو المراقب. قد يعني هذا:

- سيتعين على المعالج الآن الامتثال لالتزامات المراقب بموجب قانون حماية خصوصية البيانات الشخصية؛
- سيكون للمعالج نفس التزامات المراقب المترتبة عليه بموجب قانون حماية خصوصية البيانات الشخصية.

٥,٥ - ما هي الإجراءات المناسبة الخاصة بأمن المعلومات التي يجب تضمينها في العقود؟

يجب أن ينص العقد على أن المراقب والمعالج سينفذا الإجراءات الأمنية المطلوبة بموجب المادة ١١ والمادة ١٣ من قانون حماية خصوصية البيانات الشخصية.

هذه الإجراءات الأمنية هي كما يلي:

- مراجعة إجراءات حماية خصوصية البيانات قبل الشروع في أنشطة المعالجة الجديدة؛
- إنشاء أنظمة داخلية لإدارة الشكاوى للتمكن من تلقي الشكاوى والتحقيق فيها وطلبات الوصول إلى البيانات وطلبات التصحيح من الأفراد؛
- إعداد نظام إدارة البيانات الشخصية (PDMS)، بما في ذلك القدرة على الإبلاغ عن أي اختراق لإجراءات حماية خصوصية البيانات؛

- استخدام التقنيات المناسبة لتمكين الأفراد من ممارسة حقوقهم بموجب قانون حماية خصوصية البيانات الشخصية؛
- إجراء عمليات تدقيق ومراجعات شاملة حول الامتثال لمتطلبات حماية خصوصية البيانات؛
- التأكد من امتثال المعالج للتعليمات المقدمة له فيما يتعلق بمعالجة البيانات الشخصية والتأكد من أن المعالج يتخذ الاحتياطات المناسبة لحماية خصوصية البيانات الشخصية. كما يجب أن يتم تقييم هذا الامتثال والاحتياطات بانتظام من قبل المراقب؛
- اتخاذ الاحتياطات اللازمة لحماية خصوصية البيانات الشخصية من الفقدان أو التلف أو التعديل أو الإفشاء أو الوصول أو الاستخدام بطريقة غير قانونية أو عن طريق الخطأ.

تشمل بعض الإجراءات الأخرى التي قد يرغب المراقب والمعالج في إلزام أحد الطرفين بها بإدراجها في العقد:

- التشفير واستخدام الأسماء المستعارة؛
- القدرة على ضمان السرية والنزاهة والتوافر والمرونة المستمرة لأنظمة وخدمات معالجة البيانات الشخصية؛
- القدرة على استعادة الوصول إلى البيانات الشخصية في حالة وقوع حادث أو اضطراب للأعمال؛
- إجراء الاختبارات بانتظام وتقييم فعالية إجراءات حماية خصوصية البيانات.

لمزيد من المعلومات حول الإجراءات المناسبة، يرجى الاطّلاع على المبادئ التوجيهية لحماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضياً.

٥,٦ - ماذا الذي يجب أن تنص عليه العقود حول تكليف معالج بيانات من الباطن؟

بموجب المادة (٢) ١١ من قانون حماية خصوصية البيانات الشخصية، يجب على المراقب "تحديد المعالجين المسؤولين عن حماية البيانات الشخصية".

كجزء من الامتثال لهذه المادة، يجب أن يشتمل العقد بين الطرفين على أحكام تنظم استخدام "معالج البيانات من الباطن". إذا كان المعالج قام بتكليف مؤسسة أخرى للمساعدة في معالجته للبيانات الشخصية المتعلقة بالمراقب، فإن هذه المؤسسة ستكون معالج بيانات من الباطن.

يجب أن يتضمن العقد أحكامًا تقتضي تطبيق النقاط التالي:

- يجب أن يحصل المعالج إما على تفويض محدد مسبقًا أو تفويض خطي مكتوب من المراقب للتمكن من تكليف أي "معالج بيانات من الباطن"؛
- في حالة منح تفويض مكتوب عام من قبل المراقب، يجب على المعالج إبلاغ المراقب بأي تغييرات متعمدة تتعلق بمعالج البيانات من الباطن كما يجب منح المراقب الحق في الاعتراض على هذه التغيرات؛
- عندما قيام المعالج بتكليف معالجًا من الباطن، فإنه يجب أن يضمن المعالج وجود عقد يفرض نفس المستوى من التزامات حماية خصوصية البيانات على المعالج من الباطن مثل تلك المدرجة في العقد بين المراقب والمعالج؛
- سيكون المعالج مسؤولاً أمام المراقب عن امتثال المعالج من الباطن لالتزامات حماية خصوصية البيانات.

٥,٧ - ما الذي يجب أن تشمله العقود حول سرية البيانات؟

يجب أن تتضمن العقود أحكاماً تنص على أن المعالج سيضمن أن أي شخص أو أشخاص يعالجون البيانات الشخصية يضمنون أن إجراءات سرية البيانات مأخوذة في الاعتبار ومطبّقة. يشمل الأشخاص المعنيين موظفي المعالج بالإضافة إلى أي مقاولين وعمال مؤقتين وأطراف ثالثة.

٥,٨ - ماذا الذي يجب أن تنص عليه العقود حول حقوق الأفراد؟

يجب أن يتضمن العقد على أحكام لضمان أن المعالج سيساعد المراقب في الاستجابة لطلبات حقوق الأفراد بموجب المادة ٥ والمادة ٦ من قانون حماية خصوصية البيانات الشخصية.

هذه الحقوق هي كما يلي:

- 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.

يجب أن ينص العقد على مدى مسؤولية كل طرف في الاستجابة لطلبات المتعلقة بحقوق الأفراد، بالإضافة الى أي طرف سيكون مسؤولاً عن تكاليف هذه المساعدة ويجب أن يحدد جدولًا زمنيًا يجب تقديم هذه المساعدة خلاله.

للحصول على مزيد من الإرشادات حول حقوق الأفراد، يرجى الاطّلاع على المبادئ التوجيهية لحقوق الأفراد.

٥,٩ - ما هي المساعدة التي يجب توفيرها للمراقب من قبل المعالج؟

يجب أن ينص العقد على أن المعالج سيقوم بمساعدة المراقب للتأكد من امتثال المعالج بالتزاماته بموجب قانون حماية خصوصية البيانات الشخصية. تشمل التزامات المعالج هذه تلك المنصوص عليها في المواد التالية من قانون حماية خصوصية البيانات الشخصية.

المادة ٨

- معالجة البيانات الشخصية بأمانة ومشروعية؛
- مراعاة الضوابط الخاصة بتصميم أو تغيير أو تطوير المنتجات والنظم والخدمات المتعلقة بمعالجة البيانات الشخصية؛
- اتخاذ الاحتياطات الإدارية والفنية والمادية المناسبة لحماية البيانات الشخصية، وفقاً لما كما هو محدد من قبل شؤون الحوكمة والضمان السيبراني؛
- الامتثال لمعايير سياسات والمبادئ التوجيهية لحماية خصوصية البيانات ذات الصلة الصادرة عن شؤون الحوكمة والضمان السيبراني.

المادة ٩

- على المعالج، قبل البدء في معالجة أية بيانات شخصية، أن يُعلم الفرد بما يلي:
  - بيانات المراقب، أو أي طرف آخر يتولى معالجة البيانات لصالح المراقب أو لاستغلالها من قبله؛
  - الأغراض المشروعة التي يرغب المراقب أو أي طرف آخر في معالجة البيانات الشخصية من أجلها؛
  - الوصف الشامل والدقيق لأنشطة المعالجة ودرجات الإفصاح عن البيانات الشخصية للأغراض المشروعة، وإذا لم يتمكن المراقب من ذلك، فيتعين عليه تمكين الفرد من وصف عام لها؛
  - أية معلومات أخرى تكون ضرورية ولازمة لاستيفاء، شروط معالجة البيانات الشخصية.

المادة ١٠

- التحقق من أن البيانات الشخصية التي يجمعها المراقب، أو التي يتم جمعها لصالحة، ذات صلة بالأغراض المشروعة وكافية لتحقيقها؛
- التحقق من أن تلك البيانات دقيقة ومكتملة ومحدثة.

المادة ١١

- الامتثال للأحكام المتعلقة بأمن معالجة البيانات الشخصية على النحو المنصوص عليه في المادة ١١ من قانون حماية خصوصية البيانات الشخصية. كما نوقش بمزيد من التفصيل تحت عنوان "الإجراءات المناسبة الخاصة بأمن المعلومات" أعلاه.

المادة ١٣

- اتخاذ الاحتياطات اللازمة لحماية البيانات الشخصية من الضياع أو التلف أو التعديل أو الإفشاء، أو الوصول إليها أو استخدامها بشكل عارض أو غير مشروع؛
- على المعالج أن يخطر المراقب بوجود أي إخلال بالاحتياطات المشار إليها؛
- على المعالج أن يخطر المراقب حدوث أي خطر يهدد البيانات الشخصية للأفراد بأي وجه، فور علمه بذلك.

المادة ١٤

- إخطار الوكالة الوطنية للأمن السيبراني والأفراد ذوي الصلة بأي خروقات للإجراءات المرتبطة بحماية خصوصية البيانات، لا سيما أنه هناك احتمالية أن تتسبب هذه الخروقات في إلحاق أضرار جسيمة بالأفراد.

٥,١٠ - ما هي التزامات التدقيق والمراجعة التي يجب تضمينها في العقود؟

يجب أن يتضمن العقد التزامات على المعالج لمساعدة المراقب في تدقيق ومراجعة امتثال المعالج لقانون حماية خصوصية البيانات الشخصية، على النحو المنصوص عليه في المادة (٧) ١١.

قد تشمل هذه الالتزامات النقاط التالية:

- أن المعالج سيسمح للمراقب أو المدقق المعين من قبل المراقب بتدقيق امتثال المعالج بموجب قانون حماية خصوصية البيانات الشخصية؛

- أن المعالج سيساهم في عمليات التدقيق هذه عند اللزوم؛
- أي طرف سيكون مسؤولاً عن التكاليف المادية عن عمليات التدقيق هذه؛
- أن المعالج سيوفر جميع المعلومات كما هو مطلوب لإظهار امتثاله لقانون حماية خصوصية البيانات الشخصية إلى المراقب. قد يكون ذلك عن طريق إجراء تدقيق أو من خلال تقديم وثائق من هذا القبيل إلى المراقب.

٥,١١ - ماذا يجب أن يحدث للبيانات الشخصية عند نهاية الاتفاق التعاقدي؟

يجب أن ينص العقد على أنه في نهاية العقد سيقوم المعالج بما يلي:

- حذف جميع البيانات الشخصية التي يتم معالجتها بالنيابة عن المراقب أو إرجاعها إلى المراقب، وأن المراقب هو صاحب القرار حول ما إذا كان سيتم إرجاع هذه البيانات أو حذفها؛
- حذف أي نسخ موجودة للبيانات الشخصية ما لم يكن هناك سبب قانوني آخر للاحتفاظ بها؛
- يجب أن يتم أي حذف أو إعادة للبيانات الشخصية من قبل المعالج بطريقة آمنة وفقًا لإجراءات الأمان المنصوص عليها في المادة ١١ من قانون حماية خصوصية البيانات الشخصية.

نهاية الوثيقة