دليل خصوصية البيانات

الدليل الأولي للامتثال لخصوصية البيانات

pwc

المحتويات

مقدمة عن خصوصية البيانات

هنالك العديد من التعريفات لمصطلح «خصوصية البيانات»، غير أن المفهوم الأبسط عنها هو أنه على الاشخاص (العملاء، الموظفين، أي شخص!) معرفة نوعية البيانات الشخصية التي تجمعها المؤسسات عنهم وكيفية استخدامها لتلك البيانات. وبالطبع، هذا المفهوم هو مفهوم مبسط، ولكنه مفيد في وضع الأسس للموضوع.

خصوصية البيانات أكثر بكثير من مجرد أمن و حماية البيانات الشخصية. خلاصة هذا الموضوع متمحورة حول كيفية استخدام المؤسسات للبيانات الشخصية. يجب على المؤسسات معالجة البيانات الشخصية بطريقة أخلاقية وقانونية. هذا يعني عدم القيام بكثرة ارسال الرسائل النصية القصيرة التسويقية غير المرغوب فيها من تلك المؤسسات للعملاء، بل قد أيضاً يعني بكل بساطة عدم مشاركت المعلومات الشخصية مع أطراف خارجية دون موافقة العميل. هذا لا يعني أن التسويق قد أصبح الآن محظوراً بموجب قوانين خصوصية البيانات، ولكنه يعني أن المؤسسات عليها أن تتحلي بالشفافية فيما يخص ماهي البيانات الشخصية التي تجمعها وكيفية استخدامها بها. الكثير من المؤسسات تعي المخاطر الهائلة التي تُمثلها الهجمات السيبرانية واختراق البيانات، ولكنهم يعجزوا عن استيعاب التدابير الأخرى اللازمة لوقاية ما يُشار إليه باسم «حقوق وحريات الأفراد».

شهد العام الماضي سلسلة من اختراقات بيانات بالغة الأهمية، والتي تبعها فرض الجهات التنظيمية لغرامات ضخمة، وهو ما أفضى إلى زيادة الوعي بأهمية خصوصية البيانات وحمايتها. وفي السياق نفسه، أصدر الاتحاد الأوروبي «اللائحة العامة لخصوصية البيانات» التي أرسى بها معاييراً أكثر صرامة بشأن خصوصية البيانات وحمايتها وعزز من الوعي بشأن أهمية الامتثال لمعايير خصوصية البيانات.

أما على صعيد الشرق الأوسط، فقد اعتمدت بعض دول مجلس التعاون الخليجي قوانينها بشأن خصوصية البيانات، بينما أعربت دول أخرى عن اعتزامها إصدار تشريعات مماثلة في المستقبل القريب. وشهدت الكثير من قوانين خصوصية البيانات التي صدرت مؤخراً، بما في ذلك قوانين خصوصية البيانات المحلية بمنطقة الشرق الأوسط، على العديد من أوجه التشابه البارزة مع اللائحة العامة لخصوصية البيانات الصادرة عن الاتحاد الأوروبي، وهو ما ليس مستغرباً حيث قد أدخلت تلك اللائحة إصلاحات شاملة وجذرية على ممارسات خصوصية البيانات وتُعد الآن المعيار الذهبي في خصوصية البيانات في جميع أنحاء العالم.

نُبذة عن هذا الدليل

يتسم مجال خصوصية البيانات بالتعقيد والتطور الدائم. يبرز الكثير من التحديات التي تواجه المؤسسات من خلال تسببه في خلق الحيرة على عدة اصعدة، سواءً من ناحية كيفية معالجة البيانات الشخصية أو توقيت تلك المعالجة. إن التطبيق المعقد للائحة العامة لخصوصية البيانات، بالإضافة الى الجهود المستمرة على مستوى العالم لصياغة لوائح محلية تنظّم خصوصية البيانات، يمثلان أمراً ذو تأثير جدي على قدرات المؤسسات لتحديث وموائمة ممارسات الأعمال مع المتطلبات التنظيمية المتغيرة باستمرار.

قد اعددنا هذا الدليل في محاولة منا لتبسيط المتطلبات وتقديم الدعم اللازم لكم من أجل الانطلاق في رحلة الامتثال لمعايير خصوصية البيانات. يضم الدليل معلومات ومصادر مفيدة سوف تساعدكم في تقييم ممارسات الأعمال المتبعة لديكم ومقارنتها بأفضل الممارسات في مجال خصوصية البيانات ومن ثم اتخاذ الخطوات اللازمة لتحسين تلك الممارسات.

كما يتضمن هذا الدليل أفضل الممارسات التي تتوافق مع متطلبات اللائحة العامة لخصوصية البيانات، المتطلبات والممارسات الخاصة بمنطقة الشرق الأوسط بالإضافة إلى أطر العمل الخاصة ببرايس وترهاوس كوبرز. يتناسب هذا الدليل مع جميع المؤسسات التي تعالج البيانات الشخصية والتي تبحث عن منهجية عملية تبني عليها برامج خصوصية البيانات، سواءً كان بغرض الامتثال للوائح الخصوصية أم لإكتساب ميزة تنافسية.

ما هي أسباب أهمية خصوصية البيانات؟

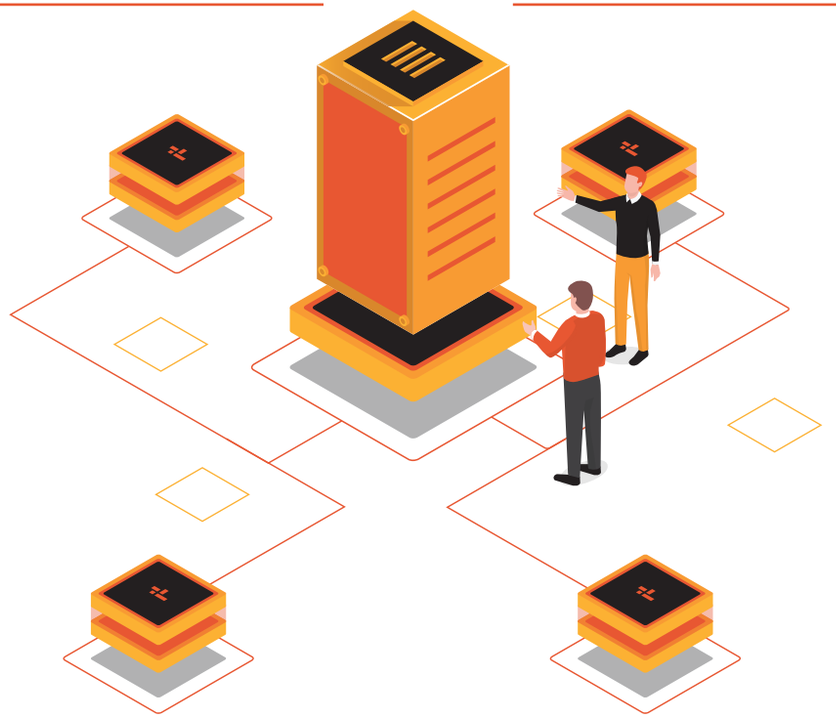
الشركات التي تعجز عن حماية البيانات الشخصية والتمثل للوائح خصوصية البيانات لا تعرض نفسها لمخاطر الغرامات المالية فحسب، بل أيضا مخاطر تشغيلية، تدخل الجهات التنظيمية والرقابية، بل والأهم من ذلك تكون عرضة للفقدان الدائم لثقة العملاء.

السمعة

قد ينتج عدم الامتثال للقوانين إلى تضرر العلامة التجارية وفقدان ثقة العملاء وثقة الموظفين وتأثر الحصة السوقية.

التنظيمية

قد تفرض الجهات التنظيمية المعنية بخصوصية البيانات إجراء عمليات تدقيق إلزامية أو إطلاع على المستندات والإثباتات بل وقد تأمر رسمياً بامتناع المؤسسة عن معالجة البيانات الشخصية.



التشغيلية

تمنح معظم قوانين خصوصية البيانات أصحاب البيانات حقوقاً على بياناتهم، مثل حق الاطلاع على بياناتهم وحق حذفها. وهو ما قد يُشكل عبئاً تشغيلياً هائلاً حال عدم تنفيذها بصورة فعالة.

المالية والجنائية

قد تؤدي الانتهاكات إلى فرض الغرامات، بل وقد تؤدي إلى عقوبة السجن في بعض البلدان، وذلك اعتماداً على نوع الانتهاك.كما قد تتعرض الشركة أيضاً لخسارة الإيرادات وتكبد تكاليف طائلة في التقاضي وتدارك الأوضاع.

المفاهيم الرئيسية

تستعرض قوانين خصوصية البيانات عدداً من المصطلحات والمفاهيم الجديدة التي يجب التعرف إليها قبل مواصلة عرض تفاصيل هذا الدليل.

"معالجة البيانات" أو **"المعالجة"** تعني أي عمليات مؤتمتة أو يدوية تُجرى على البيانات الشخصية. وبشكل أساسي، يُغطي هذا المفهوم جميع الإجراءات ذات الصلة التي قد تُجرى على المعلومات، بما في ذلك جمع البيانات، تسجيلها، تنظيمها، تصنيفها، تخزينها، تعديلها، تغييرها، استعادتها، استخدامها او الإفصاح عنها بطريق البث، النشر، النقل، الإتاحة للغير، دمجها، حجبها، حذفها أو إتلافها.

"سلطة خصوصية البيانات" أو **"السلطة"** هي الجهة الوطنية التي يتم تأسيسها لتولي المسؤولية لمساندة أصحاب البيانات في حفظ حقوقهم لحماية بياناتهم الشخصية عن طريق فرض ومراقبة الامتثال مع قوانين خصوصية البيانات المحلية.

"صاحب البيانات" أو **"الفرد"** يُعرّف بأنه الشخص الذي ترتبط به البيانات الشخصية.

"البيانات الشخصية" تُعرف بأنها البيانات التي ترتبط بالشخص الممكن تحديد هويته سواء بصورة مباشرة أم غير مباشرة. يُرجى مراجعة الصفحة ١٠ لمزيد من التفاصيل.

"البيانات الشخصية الحساسة" هي مجموعة بيانات فرعية من البيانات الشخصية وتُعرف بأنها المعلومات التي تكشف بشكل مباشر أو غير مباشر عن عرق الشخص، آرائه السياسية، آرائه الفلسفية، معتقداته الدينية، انتمائه النقابي، سجله الجنائي أو أي بيانات تتعلق بصحته وحياته الجنسية. يُرجى مراجعة الصفحة ٥ لمزيد من التفاصيل.

المبادئ الرئيسية لخصوصية البيانات

معظم قوانين خصوصية البيانات تستند إلى مجموعة من المبادئ الرئيسية، التي تؤسس قواعد جميع ما يتعلق بخصوصية وحماية البيانات الشخصية.

هناك سبعة مبادئ رئيسية لخصوصية البيانات تُشكّل الشروط الأساسية التي يجب على المؤسسات اتباعها عند معالجة البيانات الشخصية. تُشكّل معالجة البيانات الشخصية بالتوافق مع هذه المبادئ الرئيسية أمراً أساسياً من أجل الممارسة الجيدة لحماية البيانات.

وتتمثل تلك المبادئ فيما يلي:

تقليل البيانات

يلزم التأكد من معالجة البيانات الشخصية التي تحتاج إليها فعلياً دون سواها.

تقييد الغرض

يجب معالجة البيانات لغرض محدد وقانوني.

القانونية والعدالة والشفافية

يجب دائماً معالجة البيانات بصورة تتسم بالقانونية والنزاهة والشفافية.

النزاهة والسرية

يجب تطبيق ضوابط الأمن المناسبة للتأكد من حماية البيانات الشخصية من الفقدان، التلف أو الضرر.

تقييد التخزين

يجب عدم الاحتفاظ بالبيانات الشخصية بعد انتهاء احتياجك إليها.

الدقة

يجب التأكد من تحديث البيانات، والتأكد من وجود التدابير اللازمة لتصحيح وتحديث البيانات غير الدقيقة.

المساءلة

يجب وضع تدابير وسجلات مناسبة تُثبت الامتثال.

ما هي البيانات الشخصية؟

البيانات الشخصية هي اي معلومات يمكن من خلالها تحديد هوية شخص على قيد الحياة. قد تكون تلك المعلومات بسيطة مثل الاسم أو رقم الحساب أو قد تكون معرفاً رقمياً مثل عنوان بروتوكول الإنترنت، اسم مستخدم أو بيانات الموقع مثل إحداثيات نظام تحديد المواقع العالمي.

أمثلة على البيانات الشخصية

- الاسم واسم العائلة.
- رقم بطاقة الهوية.
- المعرفات عبر الإنترنت (مثل أسماء المستخدمين، عناوين بروتوكول الإنترنت).
- لقطات الدوائر التلفزيونية المغلقة.

أمثلة على البيانات غير الشخصية

- رقم التسجيل الخاص بإحدى المؤسسات.
- صناديق البريد مثل info@pwc.com.

من المهم أن نعي أنه يمكن تحديد هوية الفرد بإحدى الطريقتين التاليتين:

- بطريقة مباشرة، في حال القدرة على تحديد هوية فرد بعينه عن طريق البيانات التي تعالجها وحدها دون غيرها. على سبيل المثال: الاسم، رقم بطاقة الهوية أو عنوان البريد الإلكتروني.
- بطريقة غير مباشرة، في حال القدرة على تحديد هوية فرد بعينه عند دمج مجموعات مختلفة من البيانات من مصادر مختلفة. على سبيل المثال: الجنس، تاريخ الميلاد أو رقم لوحة المركبة.

ما هي البيانات الشخصية الحساسة؟

تشمل البيانات الشخصية بعض البيانات التي تُعتبر حساسة بحيث أن تسريبها أو إساءة استخدامها قد يؤدي إلى الإضرار بصاحب البيانات. وعلى الرغم من وجود فروقات ضئيلة بين كل قانون وآخر من القوانين التي تنظم خصوصية البيانات في تعريف البيانات الشخصية الحساسة، تُصنف البيانات الشخصية على أنها "حساسة" في حال ارتباطها بما يلي:

- الانتماء النقابي
- التوجهات السياسية أو المعتقدات الدينية
- الأصل العرقي
- المخالفات الجنائية والدعاوى القضائية
- الحياة أو الميول الجنسية
- الصحة البدنية أو العقلية

أمثلة على البيانات الشخصية الحساسة

من الضروري معرفة الفرق بين البيانات الشخصية والبيانات الشخصية الحساسة حيث تتطلب معالجة البيانات الشخصية الحساسة غالباً اتخاذ إجراءات حماية إضافية

الفرق بين ظابطي البيانات ومعالجي البيانات

تحدد قوانين خصوصية البيانات الفرق بوضوح بين "ظابطي البيانات" و"معالجي البيانات" لتوضيح أن ليست كل المؤسسات التي تمارس معالجة البيانات الشخصية تترتب عليها نفس المسؤوليات.

ظابطو البيانات " يقومون بتحديد الغرض من معالجة البيانات". هذا يعني أنهم هم من يتخذون القرارات بشأن ماهي المعلومات المسجلة والغرض منها.

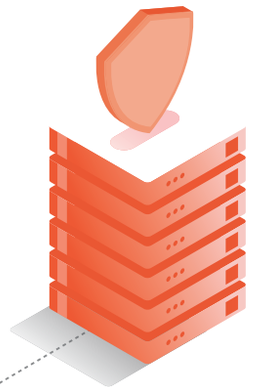
معالجو البيانات يقومون بمعالجة البيانات الشخصية بالنيابة عن ظابط البيانات حسب التعليمات الصادرة. في حال قيام المعالج بإسناد بعض أو كل إجراءات المعالجة لمؤسسة أخرى ، فيُشار إلى هذا المعالج باسم **المعالج من الباطن.**

الطريقة المبسطة للتفكر في ذلك هي على النحو التالي: تقوم شركة بيع بالتجزئة بإنشاء موقع للتجارة الإلكترونية عبر الإنترنت وتقرر المعلومات المطلوبة من العملاء لإنشاء الحساب. تستخدم هذه الشركة مزود خدمات سحابية لاستضافة الموقع وقاعدة البيانات. في هذه الحالة، تكون الشركة هي ظابط البيانات ومقدم الخدمات السحابية هو معالج البيانات.

هل أنا ظابط بيانات أم معالج بيانات؟

من المهم معرفة أن المؤسسات لا يجري تصنيفها بطبيعة الحال إما ظابط بيانات أو معالج بيانات، فقد تكون المؤسسة ظابطاً لبعض البيانات الشخصية وتقوم في الوقت ذاته بأنشطة معالجة لبيانات أخرى.

ما الذي يعنيه إن كنت..



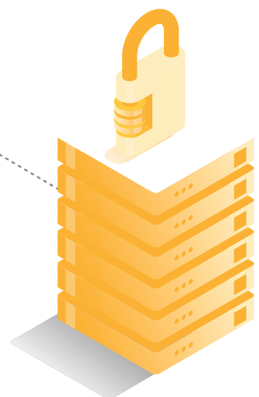
ضابطاً للبيانات

تكون أنت المسؤول في نهاية المطاف عن امتثالك وامتثال معالجي البيانات التابعين لك. وتتضمن المسؤوليات الواقعة عليك الامتثال لمبادئ خصوصية البيانات وخصوصية حقوق اصحاب البيانات واتخاذ التدابير الأمنية وإدارة اختراقات البيانات وعدم إشراك معالجين لمعالجة البيانات سوى هؤلاء المعالجين الذين يقدمون ضمانات كافية لخصوصية البيانات.

معالجاً للبيانات

تكون لديك درجة استقلالية أقل فيما يخص البيانات التي تقوم بمعالجتها، ولكن قد تظل عليك التزامات قانونية مباشرة. في حال استعانتك بمعالج بيانات من الباطن، فقد تكون مسؤولاً أمام ظابط البيانات عن امتثال هذا المعالج من الباطن.

وتتضمن المسؤوليات الواقعة عليك الامتثال لتعليمات ظابط البيانات حسبما هو منصوص عليه في العقود مع الأطراف الخارجية وتنفيذ التدابير الأمنية وإخطار ظابط البيانات بأي اختراق للبيانات الشخصية وعدم الاستعانة بأي معالج من الباطن دون موافقة ظابط البيانات.



معالج بيانات من الباطن

قد تكون مسؤولاً بصفتك معالج بيانات من الباطن عن أي ضرر يقع نتيجة معالجتك للبيانات في حال عدم امتثالك للالتزامات القانونية المترتبة عليك وفي حال عدم اتباعك لتعليمات ظابط البيانات. وتتشابه المسؤوليات الواقعة عليك أمام معالج البيانات للمسؤوليات المترتبة على معالج البيانات أمام ظابط البيانات.

حقوق الأفراد

واحد من الأهداف التي تنشدها قوانين خصوصية البيانات تمكين اصحاب البيانات ومنحهم القدرة على التحكم في بياناتهم الشخصية. لذلك تطرح معظم تلك القوانين مفهوماً تحت مسمى "حقوق اصحاب البيانات" والذي يختص بخصوصية البيانات الشخصية للأفراد. يجب التنويه الى أن هذه الحقوق ليست جميعها حقوقاً "مطلقة"، مما يعني أن هناك منها ما ينطبق فقط تحت ظروف معينة:

حق الوصول للبيانات الشخصية

يكون للأفراد الحق في الوصول إلى بياناتهم الشخصية وطلب نسخ منها.

حق تقييد معالجة البيانات الشخصية

يكون للأفراد الحق في طلب تقييد معالجة بياناتهم الشخصية.

حقوق ذات صلة بعمليات صناعة القرار والتصنيف بصورة مؤتمتة

يمكن للأفراد الاعتراض على القرارات المتخذة بشأنهم اعتماداً فقط على عمليات المعالجة المؤتمتة أو الميكانيكية.

حق الحذف*

يمكن للأفراد طلب حذف بياناتهم الشخصية دون أي تأخير غير مبرر.

حق الاعتراض

يمكن للأفراد الاعتراض على معالجة مؤسسة ما لبياناتهم الشخصية.

حق تصحيح البيانات الشخصية

يمكن للأفراد طلب تصحيح بياناتهم الشخصية في حال عدم دقتها أو طلب استكمالها في حال نقصانها.

حق نقل البيانات الشخصية

يكون للأفراد القدرة على استلام بياناتهم في شكل منظم وبتنسيق شائع الاستخدام قابل للقراءة الرقمية.

*ليست جميع حقوق أصحاب البيانات حقوقاً "مطلقة". غالباً ما يُساء فهم "حق الحذف"، ويعود السبب الرئيسي في ذلك إلى افتراض الكثيرين أن هذا الحق من "الحقوق المطلقة" بينما لا يمكن للأفراد في واقع الأمر طلب حذف بياناتهم إلا في ظروف معينة.

متى يمكن معالجة البيانات الشخصية؟

يتطلب المبدأ الأول من مبادئ خصوصية البيانات معالجة جميع البيانات الشخصية بصورة قانونية ونزيهة. لعمل ذلك، يجب على المؤسسات أن تعتمد على أساس واحد على الأقل من الأسس القانونية التالية لمعالجة البيانات:

ضرورة تعاقدية: لزوم معالجة البيانات من أجل إبرام عقد ما أو تنفيذه.

مصلحة مشروعة: للمؤسسة أو للأطراف الخارجية المشاركة.

موافقة: الفرد على معالجة بياناته الشخصية.

مصلحة عامة: وتكون خاصة للمؤسسات التي تمارس سلطات رسمية أو التي تُمارس مهاماً للمصلحة العامة.

مصلحة حيوية: للأفراد، حيث تكون معالجة البيانات ضرورية لحماية حياتهم.

التزام قانوني: حيث تكون المؤسسة ملزمة بمعالجة البيانات الشخصية.

نظراً إلى أن مختلف أنواع البيانات تتطلب مستويات مختلفة من الخصوصية، تُحدد قوانين خصوصية البيانات شروطاً مختلفة لمعالجة البيانات الحساسة والجنائية:

- **البيانات الحساسة** يمكن عادة معالجتها فقط بعد الحصول على موافقة محددة من صاحب البيانات، ما لم تكن البيانات مطلوبة لرفع إجراءات أو دعاوى قضائية، أو كان هناك أي مصلحة قانونية، مصلحة عامة أو متطلبات تنظيمية.
- البيانات الشخصية ذات الصلة **بأحكام الإدانة والمخالفات الجنائية** يمكن معالجتها طالما يتم تنفيذها تحت سيطرة سلطة حكومية معينة أو وفقا للقوانين المحلية.

أهم الإرشادات

- يجب تحديد الأساس القانوني قبل البدء في معالجة البيانات، كما يجب توثيقه.
- إنجاز الأمر بصورة صحيحة في أول مرة - يجب عدم التحول بين الأسس القانونية في تاريخ لاحق.
- في حال تغيير غرض معالجة البيانات، يجب إعادة تقييم الغرض الجديد وتحديد أساس قانوني فعال.

عشر خطوات لإنشاء برنامج فعال لخصوصية البيانات

1

18 تعيين مسؤول خصوصية البيانات

2

19 الاحتفاظ بسجل للبيانات الشخصية

3

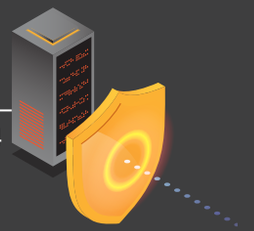
20 الإخطار بالغرض والحصول على الموافقة

4

21 الرد في حالة استفسار اصحاب البيانات عن بياناتهم الشخصية

5

22 فرض آليات أمن المعلومات

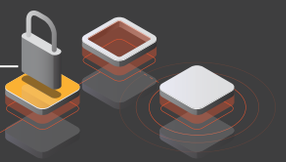


6

24 تضمين خصوصية البيانات في الأنظمة والعمليات والخدمات

7

26 الإخطار عن اختراقات البيانات



8

27 إدارة الأطراف الخارجية

9

28 خصوصية البيانات الشخصية عند نقلها إلى الخارجية

10

30 التعريف بسياسات وممارسات وعمليات خصوصية البيانات الخاصة بكم

1 تعيين مسؤول خصوصية البيانات

الكثير من القوانين التابعة لخصوصية البيانات تطرح مفهوم "مسؤول خصوصية البيانات"، وهو دور قيادي جديد يتولى المسؤولية عن الإشراف على برنامج خصوصية البيانات بالمؤسسة وضمان الامتثال للقوانين الواجب تطبيقها.

من يمكن أن يتولى منصب مسؤول خصوصية البيانات؟

يمكنكم إسناد منصب مسؤول خصوصية البيانات لموظف حالي داخل المؤسسة أو تعيين شخص معين لهذا المنصب.

يجب أن يكون مسؤول خصوصية البيانات مستقلاً، خبيراً في خصوصية البيانات، مزوداً بالموارد الكافية، ويجب أن يقدم تقارير الى الإدارات العليا.

ما هو دور مسؤول حماية البيانات:

يساعدكم مسؤول حماية البيانات في مراقبة الامتثال الداخلي لقوانين حماية البيانات واجبة التطبيق، يقدم المشورة للمؤسسة بشأن التزاماتها الخاصة بحماية البيانات، يقدم مشورة الخبراء عند الحاجة ويقوم بمهام التواصل للأفراد وسلطات حماية البيانات.

2 الاحتفاظ بسجل للبيانات الشخصية

لكي تتمكنوا من حماية البيانات الشخصية عليكم معرفة ماهي البيانات التي تجمعونها، كيفية استخدامها ومكان تخزينها. تتمثل الخطوة الأولى لتحقيق ذلك في تحديد جميع أنشطة المعالجة داخل المؤسسة التي تدخل فيها البيانات الشخصية، وتوثيق كيفية استخدام البيانات والغرض من ذلك فيما يُسمى باسم "سجل البيانات الشخصية".

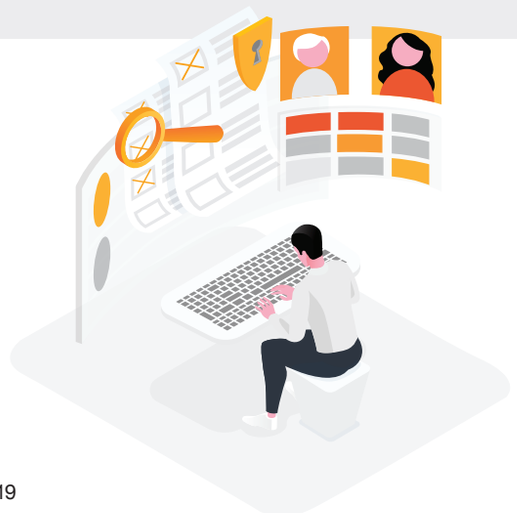
كيف يمكن تحديد البيانات الشخصية التي تجري معالجتها؟

يُعد الاحتفاظ بسجل للبيانات الشخصية من بين المتطلبات الرئيسية في معظم اللوائح المعنية بخصوصية البيانات في جميع أنحاء العالم. كخطوة أولى، نوصي بإجراء استكشاف للبيانات داخل المؤسسة لتوثيق البيانات الشخصية التي تحتفظون بها وتعالجونها، توثيق مكان تخزينها، توثيق الاطراف ذو الصلاحية على الاطلاع عليها وتوثيق مدة الاحتفاظ بها.

ما هي التفاصيل التي يجب إدراجها في السجل؟

تتطلب معظم قوانين خصوصية البيانات تحديد وتوثيق النقاط التالية لجميع أنشطة معالجة البيانات التي تجري داخل المؤسسة:

- الأسماء وبيانات الاتصال الخاصة بمسؤول خصوصية البيانات وأي طرف خارجي آخر (حسب الاقتضاء)
- الأساس القانوني لمعالجة البيانات والغرض من تلك المعالجة.
- الفئات المختلفة للبيانات الشخصية المستخدمة.
- الأنظمة والمواقع التي تجري بها معالجة البيانات الشخصية.
- الجهات الخارجية التي تُنقل إليها البيانات وقائمة بمتلقيها.
- فترة الاحتفاظ بالبيانات والتدابير الفنية والأمنية المنفذة (يُرجى مراجعة الصفحة ٢٤ لمزيد من التفاصيل).



3 الإخطار بالغرض والحصول على الموافقة

تمثل الشفافية مبدأ أساسياً في قوانين خصوصية البيانات. عند جمع البيانات الشخصية للأفراد يجب عليكم تزويدهم بمعلومات واضحة تشرح ما هي البيانات التي تريدون معالجتها وما هو سبب وكيفية معالجتها.

ما هي المعلومات التي يوجب علي أن أقدمها؟

يجب تضمين ما يلي في المعلومات الخصوصية التي تجري مشاركتها مع الأفراد:

- بيانات الاتصال بمؤسستكم وبمسؤول خصوصية البيانات.
- غرض المعالجة والأساس القانوني لها، بما في ذلك التفاصيل المتعلقة بالمصالح المشروعة إذا كان ينطبق ذلك.
- مستلمو البيانات الشخصية وتفاصيل عمليات نقل البيانات إلى الخارج.
- مدة الاحتفاظ بالبيانات الشخصية والوجود لعملية اتخاذ قرار بصفة مؤتمتة.
- التفاصيل المتعلقة بحقوق الأفراد، إجراءات سحب الموافقة وكيفية تقديم الشكاوى.

كيف تقدم المعلومات؟

يجب تقديم معلومات عن خصوصيات البيانات للأفراد في وقت جمع بياناتهم الشخصية أو خلال إطار زمني معقول في حال جمعها من مصادر أخرى. يجب أن تكون معلومات الخصوصية دقيقة، شفافة، مفهومة ويسهل الوصول إليها، كما يجب استخدام لغة واضحة وبسيطة لها. لتحقيق هذة المتطلبات، يمكن أن تأخذوا بعين الاعتبار استخدام مجموعة من التقنيات، منها منهج الاقسام القابلة للتوسع، لوحات المعلومات والإخطارات المرسلة في الوقت المناسب.

ما هي الموافقة؟

الموافقة هي القبول الذي يبديه الأفراد بحرية بشكل محدد ومتطلع، يوفره الفرد عن طريق بيان أو إجراء تأكيدي واضح لمعالجة بياناتهم الشخصية. الموافقة تعني السماح للأفراد بالتحكم في كيفية معالجة بياناتهم الشخصية واختيارها. تمثل أحد الأسس القانونية لمعالجة البيانات الشخصية بطريقة قانونية، ومع ذلك توجد شروط يتعين استيفاؤها للتأكد من أنها صحيحة.

كيف يمكنني الحصول على الموافقة؟

- يمكن لأصحاب البيانات تقديم موافقتهم كتابياً أو بأي شكل آخر. في حال تقديم الموافقة كتابياً، فيجب أن تكون مستقلة عن أي اتفاق آخر (مثل الشروط والأحكام) ويجب كتابتها بلغة واضحة وبسيطة.
- يمكن للأفراد سحب موافقتهم في أي وقت، ويجب أن تكون إجراءات السحب بنفس مستوى سهولة تقديمها.

4 الرد في حالة استفسار اصحاب البيانات عن بياناتهم الشخصية

ما هي طلبات أصحاب البيانات؟

تقدم قوانين خصوصية البيانات حقوقاً جديدةً للأفراد بحيث تتيح لهم التحكم بشكل أكبر في الكيفية التي تُستخدم بها بياناتهم. وعليه، يحق للأفراد التقدم بطلبات لممارسة حقوق اصحاب البيانات، ويجب على المؤسسات الرد في وقت محدد، وذلك بحسب قوانين خصوصية البيانات التي تخضع لها.

كيف يمكنني الاستعداد؟

للالتزام بالجدول الزمني المحدد، يتعين على مؤسستك تنفيذ إجراءات فعالة للتحقق من هوية مقدم الطلب وتقييم الطلب وصياغة الرد الملائم.

ما هي المعلومات التي يجب علي تقديمها في الرد الرسمي؟

- ما هي البيانات الشخصية الخاضعة للمعالجة. يُرجى مراجعة الصفحة ٩ لمزيد من التفاصيل.
- أغراض معالجة البيانات.
- من في داخل المؤسسة بحوزته البيانات الشخصية ولمن سيُفصح عنها.
- إذا كانت البيانات الشخصية للفرد تُستخدم في أي عملية صنع قرار بصفة مؤتمتة (مثل االاستحقاق الائتماني) وكيفية سير عملية صنع القرار هذه بشكل آلي.
- إلى متى سيُحتفظ بالبيانات، أو على الأقل ذكر المعايير المستخدمة لتحديد هذه المدة.

ما هي خطوات الرد على طلب صاحب البيانات؟

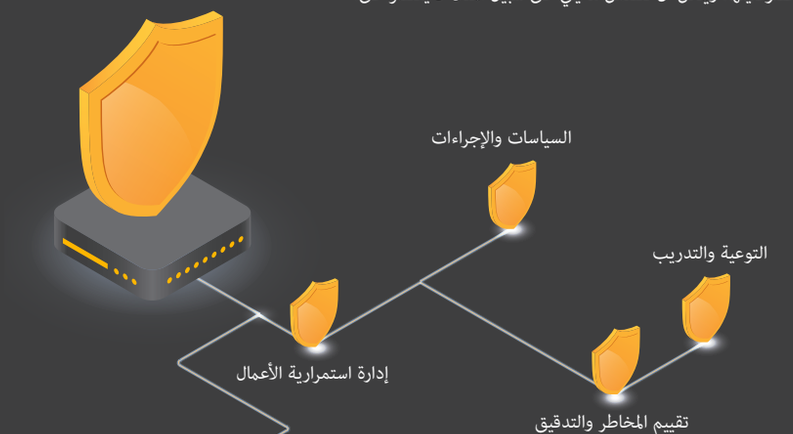
1. استلام الطلب المقدم من صاحب البيانات وإرساله إلى الإدارة المعنية.
2. تحديد ما إذا كان الطلب مقدم من الشخص نفسه أو بالنيابة عن آخرين، ثم التحقق من هوية الفرد.
3. تقييم الطلب والتأكيد على ما إذا كان سيُطبق تمديد أو رسوم، وذلك بحسب قوانين خصوصية البيانات التي تخضع لها. وإذا كانت هذه هي الحال، فيُقدم الرد للفرد مع توضيح التمديد الزمني والرسوم الإدارية أو إحداهما.
4. تحديد مكان تخزين البيانات الشخصية للفرد، سواءً كانت في أنظمة أو مستندات ورقية.
5. اتخاذ الإجراء الملائم بحسب نوع الطلب المقدم من صاحب البيانات (أي نسخ البيانات أو حذفها أو تقييد عملية معالجتها وما إلى ذلك).
6. تقديم التفاصيل الملائمة لمسؤول خصوصية البيانات لإيصالها إلى صاحب البيانات والرد عليه.
7. إرسال وتوثيق الرد المناسب للفرد.

5 فرض آليات أمن المعلومات

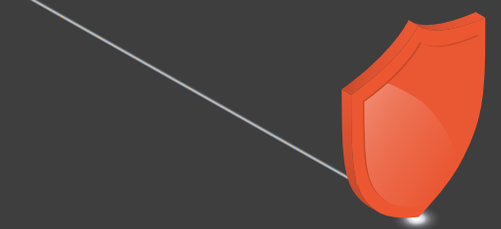
تُلزِم معظم قوانين خصوصية البيانات المؤسسات بالتأكد من وجود "تدابير مؤسسية وفنية" لخصوصية البيانات الشخصية. يعني هذا عادةً أنه يتعين على المؤسسات اتخاذ خطوات معقولة لخصوصية البيانات الشخصية. ما هو "معقول" يصل عادةً إلى اتخاذ أحد قرارات العمل بدعم من مستشار قانوني، ويعتمد على حجم المؤسسة وكم ونوع البيانات الشخصية الخاضعة للمعالجة.

بشكل عام، تكون التدابير المؤسسية والفنية هي وظائف، عمليات، ضوابط، أنظمة، إجراءات و تدابير مأخوذة لخصوصية المعلومات الشخصية التي تعالجونها.

التدابير المؤسسية هي المنهج المطبق في تقييم، إعداد، وتنفيذ الضوابط التي تؤمن البيانات الشخصية وتؤكد خصوصيتها. ويمكن أن تتضمن ما يلي على سبيل المثال لا يقتصر على:



التدابير الفنية هي التدابير والضوابط المطبقة على الأنظمة من ناحية تقنية. تشكل خصوصية هذه الجوانب أهميةً لأمن البيانات، ولكن تتعدى مرحلة تأمين الوصول إلى الأجهزة والأنظمة. يمكن أن تتضمن ما يلي على سبيل المثال غير مقتصرة على:

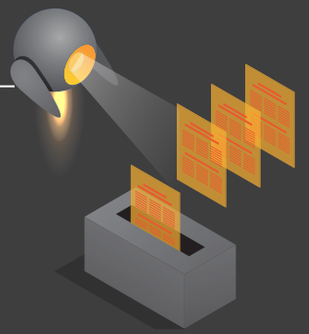


- الأمن البدني وامن الأنظمة
- تشفير البيانات الشخصية أو إخفاء هوية صاحبها
- تدابير فعالة للتخلص من البيانات
- كلمات السر ومصادقة ثنائية العناصر
- جلب الأجهزة الشخصية وآليات الدخول عن بعد

ما هي التدابير الأمنية التي يجب علي تنفيذها؟

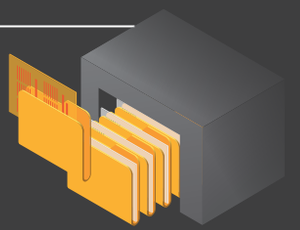
بحسب حجم مؤسستك وأنشطة المعالجة المجراة، توجد مجموعة واسعة من التدابير الفنية والمؤسسية التي يمكن أن تساعد في تأمين البيانات الشخصية وحمايتها. ونقترح أيضاً استخدام أطر عمل مثبتة مثل ISO27001 لاعداد وتقييم التدابير المناسبة .

ونظراً لعدم وجود حل "شامل مناسب للجميع" عندما يتعلق الأمر بأمن المعلومات، نوصي بأن تتبع الخطوات الواردة أدناه لتحديد أي التدابير التي يجب عليكم تنفيذها:



خطوة ١

إجراء تقييم لمخاطر أمن المعلومات عن طريق مراجعة البيانات الشخصية التي تحتفظ بها، الطريقة التي تستخدمها والمخاطر التي تشكلها عملية المعالجة.



خطوة ٢

إجراء تقييمات نقاط الضعف التقنية (مثل اختبار الاختراق) على الأجهزة والأنظمة التي تشكل خطراً كبيراً على عملية معالجة البيانات الشخصية.

خطوة ٣

تقييم اختيار التدابير الأمنية الأكثر ملاءمةً للتخفيف من المخاطر المحددة.

خطوة ٤

الحرص على إبقاء الموظفين لديك مطلعين على برنامج أمن المعلومات وافضل الممارسات الأمنية.

6 تضمين خصوصية البيانات في الأنظمة والعمليات والخدمات لديكم

نصت أحدث القوانين بخصوصية البيانات على متطلبات تفصيلية بشأن خصوصية البيانات المتنضمنة بالتصميم والمتضمنة افتراضياً. الخطوة الأولى لتحويل هذين المفهومين الواسعين إلى متطلبات وظيفية هي تحديد مبادئها كما يلي:

1. تضمين خصوصية وحماية البيانات في تصميم عملية أو تطبيق جديد: (مثل: إنشاء ثقافة مؤسسية تكون فيها الخصوصية وحماية البيانات هما الاساس الذي تتبعه الإدارة العليا).

2. الابلاغ عن المماسئلة ودعمها (مثل: إجراء عمليات مراجعة للتدقيق الداخلي على برامج خصوصية البيانات وممارساتها).

3. إنشاء الشفافية والحفاظ عليها (مثل: التحديث المستمر لإشعارات الخصوصية لتعكس أنشطة المعالجة وممارسات الخصوصية).

4. وضع وتمكين التدابير الوقائية (مثل: فرض آليات التشفير وتقليل البيانات على البيانات الشخصية).

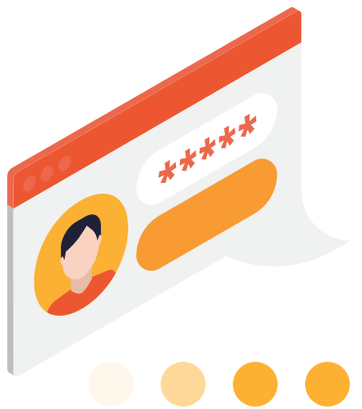
في حين تساعد هذه المبادئ في اعلام المنهج العام للمؤسسة، أن نجاح خصوصية البيانات المتنضمنة بالتصميم والمتضمنة افتراضياً تيسره الحوكمة والإشراف العالم، تطبقه القوى العاملة الداعمة وتحدده المخاطر والامتثال.

ما هي "خصوصية البيانات المتضمنة افتراضياً"؟

تتعلق خصوصية البيانات المتضمنة افتارضياً بالمبادئ الأساسية لخصوصية البيانات والمتمثلة في تقليل البيانات وتقييد الغرض.

تتطلب منكم الخصوصية الافتراضية التأكد من انه يتم فقط معالجة البيانات اللازمة لتحقيق هدفكم المحدد، مع الأخذ بعين الاعتبار أمور مثل ما يلي:

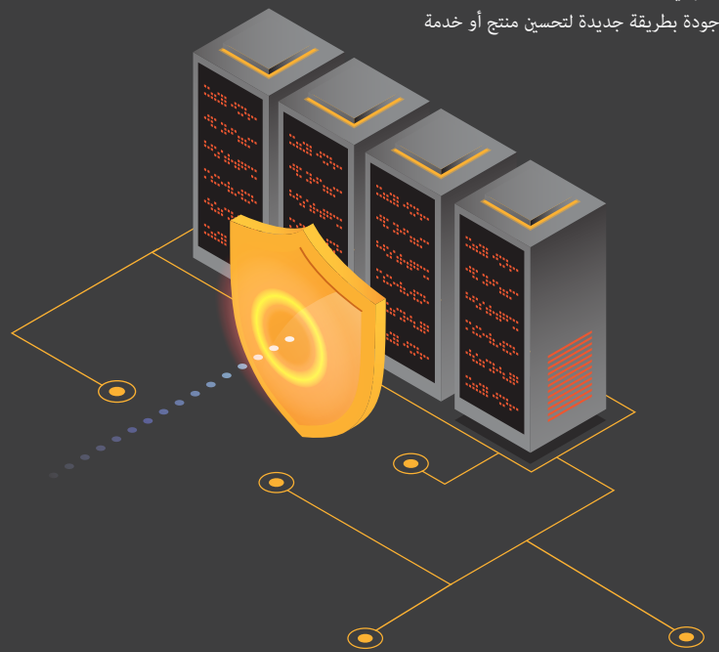
- تطبيق إعدادات الخصوصية الافتراضية على الأنظمة؛
- الالتزام بالشفافية مع عملائكم وموظفيكم بشأن أنشطة معالجة البيانات وممارساتها؛
- معالجة البيانات التي تتناسب مع الغرض؛
- إتاحة المعلومات والخيارات للأفراد لممارسة حقوقهم.



ما هي "خصوصية البيانات المتضمنة بالتصميم"؟

تلتزم المؤسسات بتوفير بيئة تحمي البيانات الشخصية ويجب عليها أن تُضمِّن خصوصية البيانات في التصميم ودورة الحياة الكلية لأي تكنولوجيا، إجراء، منتج أو خدمة، مثل:

- استخدام طريقة جديدة لتخزين البيانات (أي السحابة)
- تعيين طرف خارجي لإدارة وصيانة نظم تكنولوجيا المعلومات
- نقل البيانات إلى طرف خارجي جديد
- إنشاء عمليات جديدة للأعمال أو تعديل العمليات الحالية
- طرح مجموعة منتجات جديدة
- استخدام البيانات الموجودة بطريقة جديدة لتحسين منتج أو خدمة



تتطلب منكم خصوصية البيانات المتضمنة بالتصميم التالي:

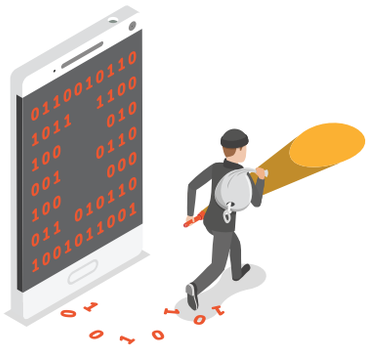
- وضع تدابير فنية ومؤسسية ملائمة مصممة لتنفيذ مبادئ خصوصية البيانات؛
- تضمين ضوابط في أنشطة المعالجة لديكم حتى تتمكنوا بالوفاء بالمتطلبات القانونية وخصوصية حقوق الأفراد.

تتألف خصوصية البيانات المتضمنة بالتصميم من عنصرين:

1. تحليل تأثير خصوصية البيانات: أداة تُستخدم لتحديد مخاطر الخصوصية المتعلقة بأنشطة المعالجة، وتقييم أثرها وتصميم ضوابط للتخفيف من المخاطر المحددة وتنفيذ متطلبات الخصوصية.
2. إدارة تغيير البيانات الشخصية: عملية تحدد المراحل الخمس العامة التي يتعين دمجها داخل دورة حياة تنفيذ المشروع، من مرحلة البداية وحتى مرحلة الإنجاز.

7 الإخطار عن اختراقات البيانات

يمكن أن تحدث اختراقات البيانات لأسباب متعددة، على الرغم من جميع الاحتياطات التي قد تتخذونها. في حين تنص لوائح خصوصية البيانات على أطر زمنية دقيقة للإبلاغ ، فمن المهم لكل مؤسسة أن تكون مستعدةً بشكل جيد في حالة وجود اختراق للبيانات.



ما هي كيفية الاستجابة لحالة اختراق البيانات؟

- تقييم طبيعة الاختراق والتأكيد على ما إذا كان يشمل بيانات شخصية.
- تحديد البيانات الشخصية التي تأثرت بالاختراق وكيف تأثرت به.
- تقييم تأثير الاختراق للوقوف على ما إذا كان يشكل خطراً كبيراً على حقوق الأفراد وحرياتهم.
- تحديد ما إذا كان يتعين عليك إخطار السلطة والأفراد المعنيين.
- إجراء تحقيق دقيق لتحديد مصدر الاختراق السلطات.

إبلاغ السلطة

يجب أن يتضمن بلاغكم عن الاختراق المعلومات التالية بحد أدنى:

- طبيعة الاختراق:
  - من اخترق أي معلومات ومتى؟
  - من تسبب في حدوث الاختراق؟
  - كيف استُخدمت البيانات؟
  - من هم الأفراد المتضررين؟
- بيان التأثير المقدر ونتائجه المحتملة.
- بيانات الاتصال بمشرف خصوصية البيانات.
- الإجراءات التي اتخذتها مؤسستك للتحقيق في الحادث وتداركه.

أفضل النصائح لإنجاز الإجراءات قبل الموعد المحدد

- التحلي بالهدوء وأخذ وقت للتحقيق بدقة قبل استئناف العمل ومواصلته.
- تنفيذ خطة استجابة وإبلاغ جميع الموظفين والأطراف الأخرى بها.
- إسناد مسؤولية إدارة الاختراقات لشخص أو فريق مخصص لذلك.
- إجراء اختبار للخطة بشكل منتظم للحد من الخلل والتعطيل الذي عادةً ما يتبع حادث الاختراق.

8 إدارة الأطراف الخارجية

تضيف قوانين خصوصية البيانات متطلبات جديدة ترفع مستوى الالتزامات المتعلقة بإدارة المخاطر ذات الصلة بالأطراف الخارجية. في حال الاستعانة بطرف خارجي لمعالجة البيانات الشخصية، فقد تتحملون المسؤولية إذا انتهك مقدم الخدمة قوانين خصوصية البيانات المطبقة أثناء تقديم الخدمة لكم.

عند إبرام اتفاق تعاقدي مع مقدم الخدمة، احرصوا على التأكد من وجود بنود تلزمه باتخاذ تدابير ملائمة لضمان الامتثال للمتطلبات التي تنص عليها قوانين خصوصية البيانات المطبقة.

ما الذي يجب تضمينه في العقد؟

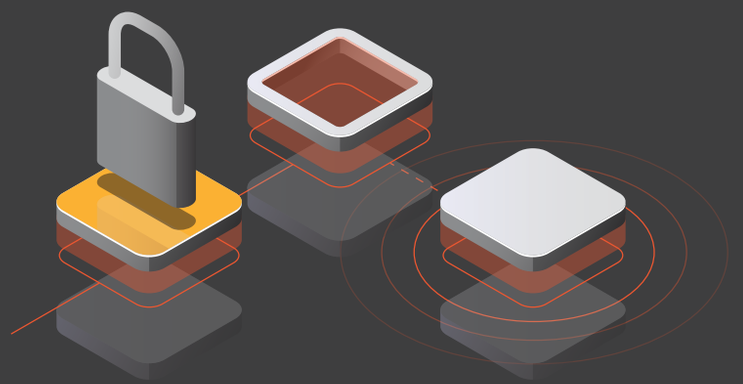
يجب أن تتضمن الاتفاقيات التعاقدية المبرمة مع الأطراف الخارجية التفاصيل التالية بحد أدنى:

- موضوع عملية المعالجة ومدتها
- طبيعة عملية المعالجة وغرضها
- نوع البيانات الشخصية وفئات موضوعات البيانات
- الحد الأدنى من الشروط أو البنود المطلوبة من معالج البيانات
- التزامات وحقوق ظابط البيانات

تحسين برنامج إدارة المخاطر ذات الصلة بالأطراف الخارجية

العقود وحدها لا تكفي لإدارة المخاطر ذات الصلة بالأطراف الخارجية. ترد أدناه خطوات إضافية يمكنكم أن تأخذوها بعين الاعتبار لتحسين برنامجكم لإدارة المخاطر ذات الصلة بالأطراف الخارجية:

- إجراء تقييم للعناية الواجبة للتأكد من أن الطرف الخارجي يطبق ضوابط ملائمة لخصوصية البيانات الشخصية.
- تحديث العقود الموجودة وصياغة عقود جديدة تحدد بشكل واضح أدوار كل طرف ومسؤولياته والتزاماته.
- مواصلة تحسين المراقبة المستمرة عن طريق تقييم المخاطر والتدقيق للتأكد من أن الأطراف الأخرى تواصل تنفيذ ضوابط ملائمة لخصوصية البيانات الشخصية.



9 خصوصية البيانات الشخصية عند نقلها إلى الخارج

في ظل وجود عدد كبير من عمليات المؤسسات تمتد عبر العديد من الدول والمناطق، أصبحت عمليات نقل البيانات تشكل جزءاً لا يتجزأ من الاقتصاد العالمي اليوم. تتضمن الكثير من قوانين خصوصية البيانات "قائمة بيضاء" بالدول التي يمكن نقل البيانات الشخصية إليها بحرية، حيث إنها تطبق مستويات ملائمة من خصوصية البيانات الشخصية. بالنسبة للدول غير المدرجة على القوائم البيضاء أو "الدول العالم الثالث" كما تُعرف أيضاً، تتطلب قوانين خصوصية البيانات تدابير وقائية متى نُقِلت البيانات إلى هذه الأماكن. يعني هذا في كثير من الأحيان استخدام آلية معترف بها لنقل البيانات.

ما يُعتبر عملية نقل بيانات إلى دولة أخرى؟

عملية نقل البيانات إلى دولة أخرى هي نقل البيانات الشخصية إلى دولة أو بلد حيث لا يفرض قانون خصوصية البيانات في بلد المرسل اليه مستوى ملائماً لخصوصية البيانات مقارنةً بموطن المرسل.

تجري عملية نقل بيانات للخارج في حال ما يلي:

- إذا كانت البيانات الشخصية التي تعتزم نقلها تقع ضمن نطاق قانون أو أكثر من قوانين خصوصية البيانات.
- إذا كانت البيانات الشخصية تُنقل إلى دولة أخرى.
- إذا كان المرسل إليه مؤسسة مستقلة أو فرد. ويشمل هذا أيضاً عمليات النقل إلى شركة أخرى ضمن مجموعة الشركات نفسها.

متى يمكنني نقل البيانات الشخصية؟

يمكن ان تشكل عملية نقل البيانات الشخصية إلى الخارج مخاطر أكبر للمؤسسة. ففي بعض الحالات، تقيد قوانين خصوصية البيانات عمليات نقل البيانات الشخصية خارج الدول إلا في حال وجود تدابير وقائية معينة.

ما هي التدابير الوقائية الملائمة لعمليات نقل البيانات الشخصية؟

يوجد عدد من الآليات يمكن لمؤسستكم تبنيها لخصوصية البيانات الشخصية عند نقلها إلى دول أخرى. فيما يلي بعض التدابير الوقائية التي تقرها اللائحة العامة لخصوصية البيانات:

لوائح الشركات الملزمة:

قواعد وسياسات داخلية ملزمة وقابلة للتنفيذ قانونياً لعمليات نقل البيانات داخل الشركات العالمية التي تسمح بعمليات نقل البيانات داخل المجموعة إلى دول لا توفر مستوى ملائماً لخصوصية البيانات الشخصية. يتطلب موافقة السلطة على لوائح الشركات الملزمة.

البنود التعاقدية الاساسية:

مجموعة من البنود الاساسية تقدمها السلطة المعنية ذات الصلة لتُستخدم في العقود.

مدونات قواعد السلوك:

تشبه هذه المدونات برامج التنظيم الذاتي لإظهار التزام الشركة بمعايير معينة لخصوصية البيانات للجهات التنظيمية والمستهلكين.

الاعتماد:

يُمنح الاعتماد للمرسل إليه، وفقاً لسياسات توافق عليها السلطة. ويجب أن تشمل سياسة الاعتماد تدابير وقائية ملائمة لخصوصية الأفراد الذين تُنقل بياناتهم الشخصية، والتي يمكن تنفيذها بشكل مباشر.

ماذا لو كانت عملية نقل البيانات إلى الخارج غير خاضعة لتدابير وقائية ملائمة؟

إذا كانت عملية نقل البيانات غير خاضعة لتدابير وقائية ملائمة، فيتعين تقدير ما إذا كان أحد الاستثناءات المحددة في قوانين خصوصية البيانات المعمول بها مطبق. هذه الاستثناءات خاصة بكل قانون من قوانين خصوصية البيانات ويمكن أن تشمل الاعتماد على الموافقة المحددة لصاحب البيانات أو إبرام عقد معه.

10 التعريف بسياسات وممارسات وعمليات خصوصية البيانات الخاصة بكم

لا يمكن ترك قضية الامتثال لقوانين خصوصية البيانات لأقسام الشئون القانونية والامتثال للتعامل معها بمفردها. يتطلب الامتثال لقوانين خصوصية البيانات ادراك وفهم جميع العاملين بالمؤسسة لمسؤولياتهم تجاه خصوصية البيانات الشخصية. من الضروري التعريف بسياسات وممارسات خصوصية البيانات المطبقة بالمؤسسة للعملاء والموظفين لضمان إلمامهم بالكيفية التي تقوم بها المؤسسة بمعالجة البيانات الشخصية وحمايتها.

الموظفون

- إبلاغ الموظفين بالسياسات والإجراءات الخاصة بخصوصية البيانات لضمان إلمامهم بما يقع عليهم من أدوار ومسؤوليات في معالجة البيانات الشخصية.
- إنشاء ثقافة من الوعي بخصوصية البيانات داخل المؤسسة عن طريق المواءمة بين أهمية خصوصية البيانات والقيم التي تقوم عليها المؤسسة وعن طريق تنفيذ منهجيات عملية تستهدف تحويلها إلى ممارسات معتادة بالمؤسسة.
- استخدام الملصقات ورسائل البريد الإلكتروني وأدوات اتصال أخرى لرفع مستوى الوعي بشأن أهمية خصوصية البيانات الشخصية بين الموظفين.
- إرسال الموظفين المعنيين لديكم الذين يتعاملون مع البيانات الشخصية لحضور تدريب دوري على خصوصية البيانات لضمان بقائهم على اطلاع بأحدث العمليات الداخلية والتطورات في مجال الخصوصية.

العملاء

- تأكد من سهولة توفر معلومات الاتصال الخاصة بمسؤول خصوصية البيانات لديكم حتى يستطيع العملاء معرفة الشخص الذي يوجهون إليه أي استفسارات أو شكاوى.
- تأكد من جاهزيتكم لتقديم المعلومات عن السياسات والممارسات وإجراءات الشكاوى عند الطلب.
- تحديث إشعار الخصوصية لديكم لضمان معرفة العملاء بالبيانات التي تقوموا بمعالجتها وكيفية معالجتها، وذلك لتمكينهم من اتخاذ قرارات مستنيرة بشأنها. يجب أن يكون إشعار الخصوصية:
  - متسماً بالاختصار والشفافية
  - مكتوباً بلغة واضحة ومباشرة
  - مقدماً في الوقت المناسب
  - متوفراً بصورة عامة وسهل الوصول إليه

كيف يمكن لبرايس وترهاوس كوبرز تقديم المساعدة؟

باعتبارنا خبراء في مجال خصوصية البيانات، فإننا نعد في وضع ملائم لتقديم الدعم لمؤسستكم في رحلتها نحو الامتثال لمعايير خصوصية البيانات. لقد أعددنا منهجية مكونة من خمس خطوات لبرامج التحول في مجال خصوصية البيانات مع وجود الأدوات والمسرعات التي تُسهم في تحقيق ذلك.

تقييم القدرات الحالية

تحليل المخاطر واستكشاف البيانات

ما ستحصلون عليه
- خطة إشراك أصحاب المصلحة والتواصل معهم
- مخزون البيانات الشخصية
- خرائط تدفق البيانات التي توضح حركة البيانات الشخصية بداية من جمعها وحتى التخلص منها

تقييم الفجوات

ما ستحصلون عليه
- تحليل الفجوات الرقابية
- تقييم للمخاطر استناداً إلى استخدامات البيانات الشخصية الحالية والمستقبلية المقررة

تصميم الوضع المستقبلي

تصميم النموذج التشغيلي والبرنامج المستهدفين

ما ستحصلون عليه
- خطة مشروع تفصيلية لتدارك الأوضاع غير الصحيحة مع تحديد أثرها على مؤسستك
- إنشاء مجموعة عمل متعددة التخصصات

تنفيذ البرامج

مجالات التركيز
- الاستراتيجية والحوكمة
- إدارة السياسات
- استراتيجية البيانات العابرة للحدود
- إدارة دورة حياة البيانات
- معالجة حقوق الأفراد
- حماية البيانات المتضمنة بالتصميم
- أمن المعلومات
- إدارة حوادث الحماية
- مساءلة معالج البيانات

التشغيل والمداومة

العمليات التشغيلية والمراقبة المستمرة

ما ستحصلون عليه
- برنامج مراقبة مستمرة محدد
- تتبع حالات عدم الامتثال وإعادة فحصها
- البروتوكلات المتبعة في حالات إضافة تغييرات على السياسات والإجراءات

تواصل معنا

يُرجى التواصل معنا لمناقشة كيف يمكن لبرايس وترهاوس كوبرز المساعدة في تنفيذ برنامج خصوصية البيانات لديكم.

أوليفر سايكس
شريك، الثقة الرقمية
+974 4419 2777
oliver.sykes@pwc.com
linkedin.com/in/osykes
@oraclesykes

فيل ميني
شريك، الثقة الرقمية
+974 4419 2909
phil.mennie@pwc.com
linkedin.com/in/philmennie
@philmennie

عيسى حبش
شريك، قائد خدمات التأمين الأخرى، قطر
+974 3302 4594
issa.habash@pwc.com
linkedin.com/in/issa-habash

ناكول سريفاستافا
مدير، الثقة الرقمية
nakul.srivastava@pwc.com
linkedin.com/in/nakul-srivastava
@NakulSrivastav6

ريتشارد تشودزينسكي
شريك، مدير أول، الشؤون القانونية في بي دبليو سي
richard.chudzynski@pwc.com
linkedin.com/in/richardchudzynski

CDC 1872 082019