SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

دليـــل نظام حمايـــة البيانات الشخصية

الإصدار 1.0

ديسمبر 2023

فهم النظام ولوائحه

ما المقصود بحماية البيانات الشخصية؟

هي مجموعة من المبادئ والممارسات والتدابير التي تهدف إلى حماية بيانات الأفراد وضمان الالتزام بالأنظمة واللوائح، كما يعد تخصيص برنامج للالتزام بأحكام النظام ولوائحه ضرورياً لتمكين الجهات من معالجة البيانات الشخصية مع احترام حقوق الأفراد المتعلقة ببياناتهم.

حماية البيانات الشخصية ترتبط ارتباطاً وثيقاً بأهداف رؤية 2030 المتمثلة في التحول والاقتصاد الرقمي والشفافية والابتكار وبناء اقتصاد قائم على البيانات.

يشمل هذا الدليل ثلاثة أقسام توضح متطلبات النظام للجهات المشمولة بأحكامه لاستخدامه كمرجع أثناء بناء برنامج الالتزام، حيث يتضمن نبذة عن المتطلبات الرئيسية من خلال أمثلة عملية وأفضل الممارسات العالمية.

ونود التنويه بأنه تم ربط بعض الأمثلة بقطاع محدد على سبيل المثال ولكن تنطبق الأمثلة على جميع الجهات المشمولة بأحكام النظام بغض النظرعن القطاع وطبيعة نشاط الجهة.

أهمية حماية البيانات الشخصية لرؤية المملكة 2030

ترتبط رؤية المملكة 2030 ارتباطاً وثيقاً بالتحول الرقمي وتطوير اقتصاد قائم على المعرفة، وفي هذا السياق تعد حماية البيانات الشخصية مهمة جداً لنمو المملكة وازدهارها، وفيما يلي توضيح لكيفية ارتباط حماية البيانات الشخصية برؤية المملكة 2030:

• تطوير الاقتصاد الرقمي:

تهدف رؤية المملكة 2030 إلى تعزيز نمو الاقتصاد الرقمي من خلال تعزيز الابتكار والتقدم التقني، ومع انتشار التقنيات الرقمية، تصبح الحاجة إلى حماية البيانات أمراً بالغ الأهمية لضمان حماية البيانات الشخصية وأمن وثقة الأفراد والشركات فيما يتعلق بهذه التقنيات.

• تعزيز الشفافية ضمن الأدوار الحكومية:

تؤكد رؤية المملكة 2030 على تطوير خدمات الحكومة الإلكترونية التي تتسم بالفاعلية والشفافية، وفي الوقت الذي تتولى فيه الجهات الحكومية جمع كميات كبيرة من البيانات الشخصية ومعالجتها، يصبح من الضروري تنفيذ تدابير وإجراءات صارمة لحماية هذه البيانات الشخصية.

• تعزيز ودعم ثقافة الابتكار وريادة الأعمال:

تعمل تدابير وإجراءات حماية البيانات الصارمة والمحكمة على تعزيز الثقة بالشركات الناشئة والجهات، مما يتيح التعامل الآمن مع البيانات الشخصية للعملاء ويحمي حقوق الملكية الفكرية.

• اتخاذ القرارات القائمة على البيانات:

تفترض رؤية المملكة 2030 الاستخدام المكثف لتحليل البيانات والرؤى من أجل إعداد السياسات والتخطيط الاقتصادي واستراتيجيات الأعمال؛ لذلك فإن الحماية الفعالة للبيانات ضرورية لضمان سلامة البيانات ودقتها واستخدامها على نحو أخلاقي.

يتم تنظيم معالجة البيانات الشخصية في المملكة من قبل الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، وهي الجهة المختصة فيما يتعلق بتطبيق نظام حماية البيانات الشخصية في المملكة.

يعد فهم نظام حماية البيانات الشخصية ضرورياً للالتزام بأحكامه، إذ يضمن النظام حقوق أصحاب البيانات الشخصية والتزامات جهة التحكم وجميع المتطلبات المتعلقة بمعالجة البيانات الشخصية، ويتيح للجهة فهم طرق ومتطلبات حماية البيانات الشخصية في المملكة، وتتضمن اللوائح التنفيذية تفاصيل حول كيفية تنفيذ أحكام النظام.

القسم 01

مبادئ نظام حماية البيانات الشخصية

على الرغم من أن نظام حماية البيانات الشخصية لم ينص على مبادئ حماية البيانات الشخصية صراحة، إلا أن هذه المبادئ توجد ضمنياً في أحكام النظام، ومعرفة تلك المبادئ يساعد الجهات على فهم المتطلبات النظامية.

يُوضح أدناه تفصيل لبعض المبادئ الرئيسية لحماية البيانات الشخصية:

- **المشروعية والإنصاف والشفافية:**

يجب على الجهة التأكد من معالجة البيانات الشخصية بطريقة عادلة ومشروعة وتتسم بالشفافية دائماً.

- **تقييد الغرض:**

يجب على الجهة تحديد الغرض من معالجة البيانات الشخصية وأن يكون الغرض مشروعاً ومعيناً.

- **الحد الأدنى من البيانات الشخصية:**

يجب على الجهة جمع ومعالجة البيانات الشخصية اللازمة لتحقيق الغرض من المعالجة.

- **الدقة:**

يجب على الجهة التأكد من تحديث البيانات الشخصية واتخاذ التدابير اللازمة لتصحيح البيانات الشخصية غير الدقيقة.

- **تقييد التخزين:**

يجب على الجهة عدم الاحتفاظ بالبيانات الشخصية بعد انتهاء الغرض من جمعها.

- **النزاهة والسرية:**

يجب على الجهة وضع تدابير أمنية كافية لحماية البيانات الشخصية من الفقد أو التلف.

- **المسؤولية:**

يجب على الجهة اتباع التدابير وإعداد السجلات اللازمة لإثبات التزامها بالنظام ولوائحه ومبادئه.

◄ ما هي حقوق أصحاب البيانات الشخصية بموجب النظام؟

أحد أهم أهداف نظام حماية البيانات الشخصية هو تمكين الأفراد من إدارة بياناتهم الشخصية، وتحديد حقوقهم تجاه معالجة بياناتهم الشخصية، علماً بأن هذه الحقوق ليست مطلقة وإنما يوجد بعض الاستثناءات على ممارسة تلك الحقوق في ظل ظروف محددة.

وفيما يلي توضيح للحقوق التي يتمتع بها أصحاب البيانات الشخصية بموجب النظام:

01 الحق في العلم:

يجب إحاطة أصحاب البيانات الشخصية علماً بالمسوغ النظامي لمعالجة بياناتهم الشخصية والغرض منها.

02 الحق في الوصول إلى البيانات الشخصية:

يحق لأصحاب البيانات الشخصية الوصول إلى بياناتهم، مع مراعاة استيفاء متطلبات نظام حماية البيانات الشخصية ولوائحه التنفيذية.

03 الحق في طلب الحصول على البيانات الشخصية:

يحق لأصحاب البيانات الشخصية طلب الحصول على بياناتهم بصيغة مقروءة وواضحة.

04 الحق في طلب التصحيح:

يحق لأصحاب البيانات الشخصية طلب تصحيح بياناتهم (إذا كانت غير دقيقة) أو إكمالها (في حال عدم اكتمالها) أو تحديثها (في حال كانت غير محدثة).

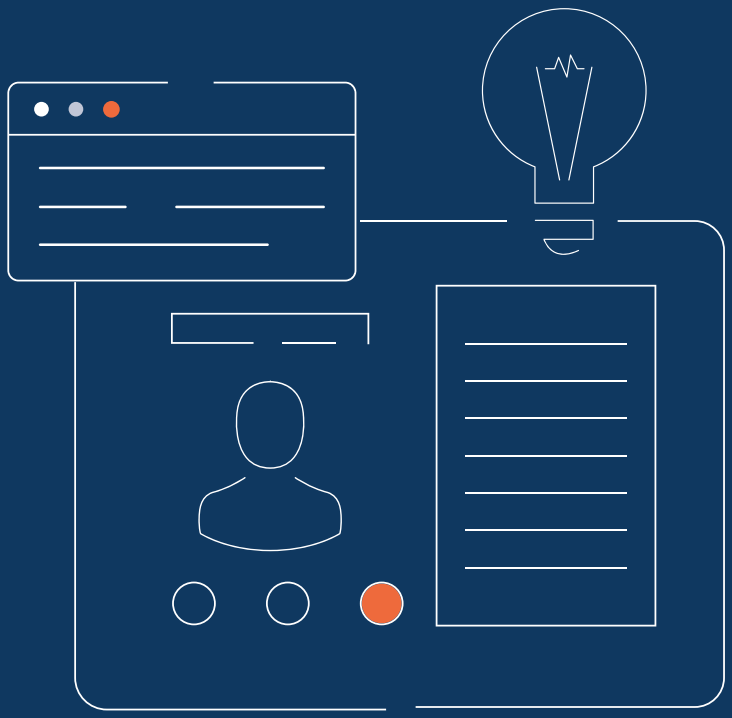
05 الحق في طلب الإتلاف:

يحق لأصحاب البيانات الشخصية طلب إتلاف (حذف) بياناتهم.

06 الحق في العدول عن الموافقة:

يحق لأصحاب البيانات الشخصية العدول عن موافقتهم على معالجة بياناتهم في أي وقت.

القسم 02
معرفة البيانات الشخصية التي يتم جمعها



من خلال معرفة أنواع البيانات الشخصية التي يتم جمعها ومعالجتها وتخزينها، يمكن إعداد تقويم للمخاطر المحتملة المتعلقة بمعالجة هذه البيانات ووضع التدابير اللازمة لحمايتها، كما يتيح تحديد الأغراض لمعالجتها والمسوغ النظامي وحقوق أصحابها، وتمكين الجهة من إعداد سجل أنشطة معالجتها والاستجابة لطلبات أصحاب هذه البيانات الشخصية بفاعلية.

2.1 إجراء عملية اكتشاف البيانات الشخصية

تنويه

يمكن للجهات بغض النظرعن القطاع الذي تعمل فيه الاستفادة من إجراء عملية اكتشاف البيانات الشخصية لمعرفة البيانات التي تحتفظ بها وفهم تدفقاتها وإنشاء سجل أنشطة معالجة البيانات وتقويم مخاطر معالجة البيانات الشخصية.

يتيح إجراء اكتشاف البيانات الشخصية للجهة فهم البيانات التي يتم جمعها ومعالجتها وتخزينها بشكل كامل، وتمكن هذه العملية من اتخاذ قرارات مدروسة أكثر بشأن البيانات الشخصية ومعالجتها كما يُتيح للجهة تحديد الثغرات المحتملة.

◄ مثال: إجراء عملية اكتشاف البيانات الشخصية

شركة تعمل في مجال تجارة التجزئة وتدير منصة للتجارة الإلكترونية، تنوي البدء بتنفيذ إجراءات الالتزام بأحكام نظام حماية البيانات الشخصية. لتحقيق ذلك يجب عليها أولاً فهم طبيعة البيانات الشخصية التي تتم معالجتها؛ لذا عليها القيام بتنفيذ عملية اكتشاف للبيانات الشخصية من خلال تشكيل فريق عمل متعدد التخصصات يتكون من ممثلين من قطاع تقنية المعلومات والشؤون القانونية والالتزام ووحدات الأعمال الأخرى، ويبدأ الفريق بتحديد وتخطيط جميع البيانات الشخصية داخل الشركة.

وفيما يلي الخطوات التي يجب أن يتخذها الفريق:

01 جرد البيانات الشخصية:

يحدد الفريق مصادر البيانات المختلفة، مثل قواعد بيانات العملاء وسجلات المعاملات وتحليلات الموقع الإلكتروني وسجلات الموظفين، كما يحدد الموردين أو الشركاء الخارجيين الذين يعالجون البيانات الشخصية بالنيابة عن الشركة العاملة بتجارة التجزئة.

02 تصنيف البيانات الشخصية:

يصنف الفريق أنواع البيانات الشخصية التي يتم جمعها، مثل أسماء العملاء ومعلومات الاتصال وتاريخ الشراء وتفاصيل الدفع، كما يتم تحديد البيانات الحساسة، مثل البيانات الصحية التي تتطلب حماية إضافية بموجب نظام حماية البيانات الشخصية.

03 تخطيط البيانات الشخصية:

يعمل الفريق بشكل دقيق مع فريق تقنية المعلومات لتتبع تدفق البيانات الشخصية عبر أنظمة شركة تجارة التجزئة، كما يتم تحديد نقاط الاتصال التي يتم بها جمع البيانات الشخصية ومعالجتها وتخزينها، سواء في قواعد البيانات الداخلية أو الأنظمة الخارجية.

04 الغرض من جمع البيانات الشخصية والمسوغ النظامي:

يتعاون الفريق مع خبراء الالتزام بالأنظمة وخبراء نظام حماية البيانات الشخصية لتحديد الأغراض التي جُمعت من أجلها البيانات الشخصية والمسوغ النظامي لمثل هذه المعالجة، ويحدد فترات الاحتفاظ بالبيانات وينفذ عمليات للتخلص الآمن من البيانات الشخصية.

05 الاحتفاظ بالبيانات الشخصية:

يقوم الفريق بتحديد البيانات الشخصية التي تم الانتهاء من غرض جمعها ومعالجتها، ووضع مدة للاحتفاظ بالبيانات الشخصية الأخرى وإجراءات التخلص منها بشكل آمن.

2.2 تحديد المسوغ النظامي للمعالجة

تنويه

يجب أن تستوفي الموافقة على جمع ومعالجة البيانات الشخصية ضمن معايير محددة لتعد موافقة صحيحة بموجب نظام حماية البيانات الشخصية، ويجب أن يكون قرار منحها أُخذ بحرية ودون استخدام أساليب مُضللة للحصول عليها، ويجب أن يعود هذا القرار بشكل كامل لأصحاب البيانات الشخصية.

تحديد المسوغ النظامي المناسب هو أساس الالتزام بنظام حماية البيانات الشخصية.

مثال: تحديد المسوغ النظامي للمعالجة

يتولى مقدم الرعاية الصحية الذي يقدم الخدمات الطبية للمرضى جمع البيانات الشخصية ومعالجتها، بما في ذلك البيانات الحساسة، مثل السجلات الطبية.

يتخذ مقدم الرعاية الصحية الخطوات التالية:

01 تحديد الغرض:

يُدرك مقدم الرعاية الصحية أن توفير رعاية طبية عالية الجودة وإدارة مواعيد المرضى بشكل صحيح يتطلب منه معالجة البيانات الشخصية للمرضى (بما في ذلك البيانات الحساسة)؛ لذلك يحدد مقدم الرعاية الصحية الغرض من المعالجة، مثل الوفاء بالتزاماته كمقدم للرعاية الصحية وضمان رفاهية مرضاه.

02 تحديد المسوغ النظامي:

بعد تحليل الغرض من معالجة البيانات، يحدد مقدم الرعاية الصحية المسوغ النظامي المناسب وهو "إبرام اتفاقية يكون صاحب البيانات الشخصية طرفاً فيها" كما أن معالجة البيانات الشخصية للمرضى ضرورية لتمكين مقدم الرعاية الصحية من الوفاء بالتزاماته التعاقدية مع المرضى، إذ إن تقديم الخدمات الطبية للمرضى يتطلب جمع بياناتهم الشخصية.

03 إبلاغ المرضى:

بلغ مقدم الرعاية الصحية مرضاه بأنشطة المعالجة والمسوغ النظامي المحدد ويوفر معلومات واضحة وشفافة حول طبيعة البيانات الشخصية التي سيتم جمعها ومبررات معالجتها وكيفية استخدامها.

04 الحصول على الموافقة لأغراض محددة:

على الرغم من أن المسوغ النظامي الذي ينص على "إبرام اتفاقية يكون صاحب البيانات الشخصية طرفاً فيها"، يتضمن جوانب عملية من معالجة البيانات الشخصية اللازمة لتقديم الخدمات الطبية، إلا أن مقدم الرعاية الصحية قد يحتاج إلى إجراء معالجة للبيانات الشخصية لأغراض محددة لا تتعلق مباشرة بالعقد، مثل إرسال النشرات الإخبارية والتقارير المتعلقة بالصحة في هذه الحالة يطلب مقدم الرعاية الصحية من المرضى تقديم موافقتهم على ذلك لاستيفاء معالجة البيانات الشخصية لأغراض إضافية.

وفي حال الاعتماد على (المصالح المشروعة) كمسوغ نظامي لمعالجة البيانات الشخصية، يجب إجراء تقويم للمصالح المشروعة للتأكد من أنها مسوغ نظامي مناسب لتنفيذ عمليات معالجة البيانات لدى الجهة، ويتم تحديد متطلبات هذا التقويم في اللوائح التنفيذية، ولا يمكن للجهة الاعتماد على (المصالح المشروعة) كمسوغ نظامي في حال كانت البيانات الشخصية التي تتم معالجتها بيانات حساسة (مثل: البيانات الصحية).

2.3 إنشاء سجلات أنشطة معالجة البيانات الشخصية

تنويه

يجب على الجهات بغض النظر عن القطاع الذي تعمل فيه وضع سجل لأنشطة معالجة البيانات، إذ تُعد مسألة الاحتفاظ بسجلات دقيقة متطلباً أساسياً بموجب نظام حماية البيانات الشخصية بغض النظر عن حجم عمليات المعالجة أو طبيعتها

يعتبر سجل أنشطة معالجة البيانات متطلباً أساسياً بموجب نظام حماية البيانات الشخصية، ويُعرّف بأنه قائمة شاملة بأنشطة معالجة البيانات الشخصية التي تقوم بها الجهة.

يتيح سجل أنشطة معالجة البيانات للجهة أيضاً توثيق مخاطر معالجة البيانات الشخصية وتدابير الحماية الأمنية المناسبة للتخفيف من مخاطر حماية البيانات الشخصية.

◄ مثال: إنشاء سجل أنشطة معالجة البيانات

أجرت شركة تقنية تقدم برامج تدريب مخصصة في مجال اللياقة البدنية لعملائها عملية اكتشاف البيانات التي تعالجها.

وفيما يلي الخطوات التي تتخذها شركة التقنية:

01 التوثيق:

توثق الشركة كل نشاط من أنشطة معالجة البيانات في سجل أنشطة معالجة البيانات بعناية بناءً على اكتشاف البيانات، بما في ذلك بيانات التواصل مع جهة التحكم، والغرض من المعالجة، وفئات البيانات الشخصية المعنية، والمسوغ النظامي للمعالجة، والمعلومات المتعلقة بمشاركة البيانات الشخصية داخل المملكة، وفترات الاحتفاظ بالبيانات، وأي عمليات نقل بيانات خارج المملكة.

02 الحفظ والإدارة والتحديث:

تعتمد الشركة عملية محددة لإجراء التحديثات الدورية لسجل أنشطة معالجة البيانات وحفظه وإدارتـه، ويتولى الشخص المسؤول، مثل مسؤول حماية البيانات الشخصية مهمة مراجعة السجلات وتحديثها بانتظام، مع ضمان دقتها وملاءمتها.

03 دعم الالتزام والتدقيق:

يجب استخدام سجل أنشطة معالجة البيانات لإجراء عمليات تقييم الالتـزام والتدقيق، ويجب أن تضمن الشركة إمكانية الوصول إلى السجلات بسهولة إلى جانب إمكانية معاينتها من قبل الجهة المختصة والمدققين، إذ يُعد ذلك بمثابة دليل على التزام الشركة بنظام حماية البيانات الشخصية.

2.4 إعداد إشعارات الخصوصية ونشرها

تنويه

إشعار الخصوصية هو وثيقة قابلة للتعديل والتحديث المستمر؛ لذا يجب تحديثها في حالة التغييرات على ممارسات معالجة البيانات الشخصية لدى الجهة.

يُعد إعـداد إشعـارات الخصوصية ونشرها من الممارسات الضرورية للغاية للجهات حيث تمكنها من الالتـزام بنظام حماية البيانات الشخصية، إذ تُعتبر هذه الإشعـارات بمثابة أدوات تواصل أساسية توضح كيفية جمع البيانات الشخصية واستخدامها وحمايتها، ومـن خلال تسهيل الـوصـول إلى إشعارات الخصوصية (على سبيل المثال إتاحتها في المواقع الإلكترونية وتطبيقات الهاتف المحمول) يمكن للجهة تمكين الأفراد من اتخاذ قرارات مدروسة بشأن بياناتهم الشخصية، ويحدد النظام بالتفصيل المعلومات التي يجب أن يتضمنها إشعار الخصوصية على سبيل المثال: المسوغ النظامي لجمع ومعالجة البيانات الشخصية والغرض من ذلك وغيرها.

مثال: إعداد إشعارات الخصوصية ونشرها

تقدم شركة برمجيات مقرها الرياض عديداً من المنتجات والخدمات التقنية لعملائها، بما في ذلك منصة تخزين البيانات السحابية، إذ أنشأت شركة البرمجيات سجلاً لأنشطة معالجة البيانات، ولتطبيق مبدأ الشفافية بموجب نظام حماية البيانات الشخصية تُقرر الشركة إعداد إشعارات الخصوصية ونشرها في موقعها الإلكتروني.

وفيما يلي الخطوات التي تتخذها الشركة في هذا الشأن:

01 صياغة إشعارات الخصوصية:

يعمل الفريق القانوني التابع للشركة على صياغة إشعارات الخصوصية الذي يوفر معلومات واضحة وموجزة عن أنشطة المعالجة ليتضمن على سبيل المثال: أقسام حول جمع البيانات الشخصية، وأغراض معالجة هذه البيانات والمسوغات النظامية ومشاركة البيانات الشخصية وفترة الاحتفاظ بالبيانات، وحقوق أصحاب البيانات الشخصية.

02 إمكانية الوصول واللغة:

تضمن الشركة سهولة الوصول إلى إشعارات الخصوصية في موقعها الإلكتروني انطلاقاً من إدراكها لأهمية تسهيل الوصول إلى هذه الإشعارات، كما توفر الشركة الإشعارات بلغات متعددة بما يلبي احتياجات قاعدة عملائها المتنوعين.

03 نشر إشعارات الخصوصية:

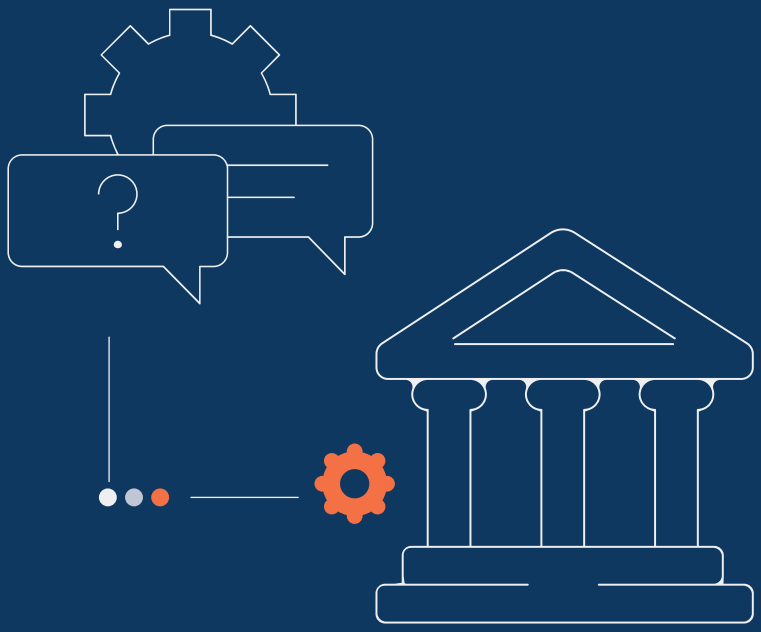
تنشر الشركة إشعارات الخصوصية في موقعها الإلكتروني، ما يجعلها متاحة بسهولة لجميع الزوار والعملاء، كما توفر الشركة روابط مباشرة لإشعارات الخصوصية تُتيح للمستخدمين الجُدد إمكانية الاستفادة منها أثناء عملية التسجيل.

04 تحديثات دورية:

تعمل الشركة على مراجعة وتحديث إشعارات الخصوصية بانتظام بما يتناسب مع التغييرات التي تتم في أنشطة معالجة البيانات الشخصية في الشركة.

القسم 03

إرساء مبادئ المسؤولية والحوكمة



من خلال إعداد إطار لحوكمة حماية البيانات الشخصية، يمكن للجهة إدارة مخاطر معالجة البيانات الشخصية بشكل فعال وتفعيل الضوابط اللازمة وتعزيز الالتزام بمعايير ومتطلبات نظام حماية البيانات الشخصية في الجهة، مما يعزز ثقة الأفراد والجهات المعنية بإمكانية الجهة من حماية البيانات الشخصية.

3.1 تقويم مدى إلزامية تعيين مسؤول حماية البيانات الشخصية

تنويه

ليس على جميع الجهات تعيين مسؤول حماية البيانات الشخصية بموجب النظام، إذ تُحدد اللوائح التنفيذية الحالات التي يكون فيها تعيين مسؤول حماية البيانات الشخصية إلزامياً.

لا يساعد تعيين مسؤول حماية البيانات الشخصية الجهة على الالتزام بمتطلبات نظام حماية البيانات الشخصية فحسب، بل يُتيح للجهة تنفيذ برنامج الالتزام بأحكام نظام حماية البيانات الشخصية بنجاح وفاعلية.

مثال: تعيين مسؤول حماية البيانات الشخصية

تتولى شركة تجارة إلكترونية متعددة الجنسيات تعمل في المملكة معالجة البيانات الشخصية لعملائها على نطاق واسع (مثل الأسماء والعناوين ومعلومات الدفع وتاريخ الشراء وما إلى ذلك) وذلك بحكم طبيعة عملها، ويتعيّن على الشركة بموجب نظام حماية البيانات الشخصية ولوائحه التنفيذية تعيين مسؤول حماية البيانات الشخصية.

لذا تتخذ شركة التجارة الإلكترونية الخطوات التالية:

01 الخبرات والمؤهلات:

تُحدد شركة التجارة الإلكترونية المؤهلات والخبرات اللازم توفرها لدى الشخص المُراد تعيينه كمسؤول حماية البيانات الشخصية، مثل: المعرفة بنظام حماية البيانات الشخصية وممارسات حماية البيانات الشخصية وإدارة المخاطر.

02 تعيين مسؤول حماية البيانات الشخصية:

تُقيّم الشركة المرشحين الداخليين والمهنيين الخارجيين والجهات المهنية التي توفر مسؤولي حماية البيانات الشخصية الذين يتمتعون بخبرة وإلمام بنظام حماية البيانات الشخصية.

03 التدريب والدعم:

توفر شركة التجارة الإلكترونية لمسؤول حماية البيانات الشخصية الموارد والتدريب والدعم الكافي لتمكينه من البقاء على اطلاع على نظام حماية البيانات الشخصية واللوائح وأفضل الممارسات في هذا الجانب، كما تشجع الشركة مسؤول حماية البيانات الشخصية على المشاركة في التطوير المهني المستمر.

04 الاتصال والتعاون:

تشجع شركة التجارة الإلكترونية مسؤول حماية البيانات الشخصية على التواصل والتعاون مع الإدارات المختلفة، بما في ذلك الشؤون القانونية وتقنية المعلومات والموارد البشرية والتسويق، ويعمل مسؤول حماية البيانات كمستشار داخلي ويساعد فرق العمل في التعامل مع مسائل تتعلق بالبيانات الشخصية.

3.2 وضع إطار لحوكمة حماية البيانات الشخصية

تنويه

تتطلب الحوكمة الفعالة لحماية البيانات الشخصية مشاركة الجهة بأكملها، وتتطلب اتباع نهج شامل يتضمن آليات وسياسات وإجـراءات وبرامج تدريبية تشمل جميع الموظفين والجهات/ الإدارات المعنية.

ويساعد اعتماد إطار محدد لحوكمة حماية البيانات الشخصية في وضع إطار عمل لوضع سياسات وإجراءات وضوابط فاعلة وتنفيذها بما يتماشى مع نظام حماية البيانات الشخصية، إذ من شأنه تعزيز الشفافية والمسؤولية والمساهمة في بناء ثقافة تهتم بحماية البيانات الشخصية داخل الجهة.

◄ مثال: إنشاء إطار لحوكمة حماية البيانات الشخصية

عيّنت شركة متعددة الجنسيات تعمل في قطاع التقنية مسؤول حماية بيانات شخصية نظراً إلى الكميات المتزايدة من البيانات الشخصية التي تتولى معالجتها، وترغب في إنشاء إطـار فعال لحوكمة حماية البيانات الشخصية لديها لضمان الالتزام المستمر بنظام حماية البيانات الشخصية.

وفيما يلي الخطوات التي يتخذها مسؤول حماية البيانات الشخصية في هذا الشأن:

01 تحديد الحوكمة:

يتعاون مسؤول حماية البيانات الشخصية مع الإدارة العليا للشركة لتشكيل لجنة توجيهية لحماية البيانات الشخصية مسؤولة عن الإشراف على مبادرات حماية البيانات الشخصية وإدارتها، وتضم اللجنة ممثلين من الإدارات الرئيسية، بما في ذلك الشؤون القانونية وتقنية المعلومات والموارد البشرية والتسويق، بالإضافة إلى ذلك تحديد إطار إدارة حماية البيانات الشخصية داخل الشركة.

02 ملاحظة:

في حال كانت الجهة عامة و يوجد لديها لجنة لحوكمة البيانات وفقاً للمواصفة رقم D.G.4.2 من وثيقة ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية يتم الاكتفاء بها عن طريق ضم هذه الأدوار لها.

03 الأدوار والمسؤوليات:

يحدد مسؤول حماية البيانات الشخصية أدوار ومسؤوليات الإدارة فيما يتعلق بمعالجة البيانات الشخصية، ويشمل ذلك مراقبة الالتزام بالنظام، وتقديم الاستشارات والتوجيه بشأن المسائل المتعلقة بمعالجة البيانات الشخصية، والعمل كجهة اتصال بين أصحاب البيانات الشخصية والجهة المختصة، ويجب على المسؤول التأكد من مراعاة اعتبارات حماية البيانات الشخصية في جميع العمليات التجارية والمشاريع. بالإضافة إلى إدارة أنشطة حماية البيانات الشخصية اليومية، مثل مراجعة سجل أنشطة معالجة البيانات الشخصية بشكل دوري.

04 الاستقلالية ورفع التقارير:

تضمن اللجنة التوجيهية بالتعاون مع مسؤول حماية البيانات عمل إدارة حماية البيانات الشخصية بشكل مستقل، وتُحدد الشركة تسلسلاً إدارياً لإعداد التقارير يضمن تمتع مسؤول حماية البيانات الشخصية بالاستقلالية والصلاحيات اللازمة لتنفيذ المسؤوليات المنوطة به بشكل فعال.

05 إطار حوكمة حماية البيانات الشخصية:

يتولى مسؤول حماية البيانات الشخصية وضع إطار لحوكمة حماية البيانات الشخصية يحدد فيه الأدوار والمسؤوليات والتسلسل الإداري داخل الجهة ليوضح هذا الإطار نطاق المسؤولية عن الالتزام بأحكام نظام حماية البيانات الشخصية ويضمن المراقبة المستمرة وإعداد التقارير ومراجعة ممارسات معالجة البيانات الشخصية في الشركة.

06 وضع السياسة:

يتولى مسؤول حماية البيانات الشخصية بالتشاور مع اللجنة

التوجيهية لحماية البيانات الشخصية وضع سياسات وإجراءات شاملة تتماشى مع النظام، وتتناول هذه السياسات أنشطة معالجة البيانات الشخصية وآليات الموافقة وحقوق أصحاب البيانات الشخصية وإجراءات الإبلاغ عن حوادث تسرب البيانات وإدارة مخاطر الموردين.

07 تقويم الأثر:

يتولى مسؤول حماية البيانات الشخصية ترتيب عمليات تقويم الأثر ومخاطر معالجة البيانات الشخصية المرتبطة على سبيل المثال: بالمشاريع أو الأنظمة أو العمليات الجديدة أو معالجة البيانات الحساسة، ويشارك مسؤول حماية البيانات الشخصية في تقويم المخاطر وتخفيفها وتنفيذ الضوابط المناسبة، ما يضمن مراعاة اعتبارات حماية البيانات الشخصية في مرحلة مبكرة من عملية صنع القرار، كما يعكس هذا النهج مبدأ الخصوصية بالتصميم وبشكل افتراضي.

08 المراقبة والتدقيق:

يُحدد مسؤول حماية البيانات الشخصية عمليات مراقبة وتدقيق أنشطة معالجة البيانات الشخصية داخل الشركة، إذ يتم إجراء عمليات تدقيق منتظمة لتحديد الفجوات أو مجالات التحسين المحتملة، وتُستخدم نتائج عمليات التدقيق هذه لتحسين الالتزام بمتطلبات حماية البيانات الشخصية في الجهة.

09 التدريب والتوعية:

يتولى مسؤول حماية البيانات الشخصية تصميم وتنفيذ برامج تدريبية تتعلق بحماية البيانات الشخصية لموظفي الشركة في جميع المستويات، وتساهم هذه البرامج في تثقيف الموظفين حول مسؤولياتهم المتعلقة بحماية البيانات الشخصية وفقاً للنظام وسياسات الجهة الداخلية، وتُعقد البرامج التدريبية بانتظام لاطلاع الموظفين على المتطلبات المتغيرة لحماية البيانات الشخصية.

10 مشاركة الجهات المعنية:

يتولى مسؤول حماية البيانات الشخصية مهمة تنسيق عمليات التواصل والتعاون المنتظم مع الجهات المعنية الداخلية، بما في ذلك الإدارة العليا ورؤساء الإدارات والموظفون، بهدف ترسيخ ثقافة الوعي بحماية البيانات الشخصية.

3.3 إعداد السياسات والإجراءات وتقديم البرامج التدريبية

تنويه

يجب مراجعة وتحديث السياسات والإجراءات بشكل مستمر لضمان توافقها مع الأنظمة واللوائح وأفضل الممارسات والاحتياجات التنظيمية.

تساهم السياسات والإجراءات في حال أُعدّت بشكل صحيح في توفير إرشادات واضحة حول كيفية معالجة البيانات الشخصية داخل الجهة، ويمكن الاستفادة من هذه السياسات والإجراءات لتمكين موظفي الجهة وتوجيههم بطرق الحد من مخاطر معالجة البيانات الشخصية.

◀ مثال: إعداد السياسات والإجراءات

شركة مالية تعالج بيانات شخصية على نطاق واسع، ولضمان الالتزام المستمر بنظام حماية البيانات الشخصية تُقرر الجهة وضع سياسات وإجراءات شاملة لحماية البيانات الشخصية.

وفيما يلي الخطوات التي تتخذها الشركة المالية في هذا الخصوص:

01 سياسة حماية البيانات الشخصية:

تعد الجهة سياسة داخلية لحماية البيانات الشخصية تُحدد فيها القواعد العامة لكيفية معالجة البيانات الشخصية، إذ تتناول السياسة مجالات مثل استراتيجية حماية البيانات الشخصية، ومبادئ حماية البيانات الشخصية، وحوكمة حماية البيانات الشخصية في الجهة وغيرها.

02 السياسات والإجراءات المتعلقة بمجالات محددة لحماية البيانات الشخصية:

تضع الجهة السياسات والإجـراءات لمختلف عمليات معالجة البيانات الشخصية، بما في ذلك سياسة وإجـراءات طلبات ممارسة الحقوق من قبل صاحب البيانات الشخصية، وسياسة وإجراءات تقويم الأثر، وسياسة الخصوصية بالتصميم وبشكل افتراضي، وسياسة مراقبة الأطراف الخارجية والإشراف عليها، وسياسة إجراءات الاستجابة لحوادث تسرب البيانات الشخصية، وسياسة الاحتفاظ بالبيانات وإجراءات إدارة الموافقات، تضمن هذه السياسات والإجـراءات معالجة جميع الموظفين للبيانات الشخصية بطريقة موحدة على مستوى الجهة بأكملها.

03 الشكاوى وطلبات أصحاب البيانات الشخصية:

تُنفذ الجهة إجـراءات محددة لإدارة الشكاوى والطلبات لتحديد خطوات تلقيها والتحقق منها والاستجابة لها وتوثيقها.

04 إدارة الموردين والأطراف الخارجية:

ضع الجهة إجراءات لإدارة مخاطر معالجة البيانات الشخصية من قبل الأطراف الخارجية، بما في ذلك الموردون ومقدمو الخدمات الممكن وصولهم إلى البيانات الشخصية، وتشمل الإجراءات إجراء تقويم العناية اللازمـة، وتحديد الالتزامات التعاقدية المتعلقة بحماية البيانات الشخصية والمراقبة المستمرة للالتزام من قبل الأطراف الخارجية من خلال عمليات التدقيق الدورية.

05 خطة الاستجابة لحوادث تسرب البيانات الشخصية:

تضع الجهة خطة للاستجابة للحوادث تُحدد فيها الخطوات التي يجب اتخاذها عند وقوع حادثة تسرب للبيانات الشخصية، إذ تتضمن الخطة إجـراءات تحديد الحوادث واحتوائها وإخطار مسؤول حماية البيانات الشخصية وأصحاب البيانات الشخصية (عند الحاجة) والتنسيق مع الجهات المعنية الداخلية والخارجية، مثل الجهة المختصة وأصحاب البيانات الشخصية المتأثرين.

3.4 تنفيذ طلبات ممارسة حقوق أصحاب البيانات الشخصية

تنويه

يتمتع أصحاب البيانات الشخصية بموجب النظام بحق العدول عن موافقتهم على معالجة بياناتهم، ويجب على الجهات المعنية إيقاف معالجة البيانات وعدم التأخر في ذلك دون مبرر.

احترام حقوق أصحاب البيانات الشخصية يساهم في تعزيز الثقة بينهم وبين الجهة، كما أن احترام وحماية حقوق الأفراد يساهم في تعزيز الالتزام بنظام حماية البيانات الشخصية.

◄ مثال | تنفيذ طلبات أصحاب البيانات الشخصية

شركة تجارة إلكترونية توفر منتجات صديقة للبيئة للعملاء في جميع أنحاء العالم، ويتضمن برنامجها للالتزام بحماية البيانات الشخصية ضرورة تنفيذ طلبات أصحاب البيانات الشخصية المتعلقة بممارسة حقوقهم.

ترسل إحدى العميلات رسالة إلكترونية إلى متجر الشركة الإلكتروني لطلب الوصول إلى بياناتها الشخصية التي تحتفظ بها الشركة، وتريد معرفة المعلومات المخزنة وكيفية استخدامها.

وفيما يلي الخطوات التي يتخذها مسؤول حماية البيانات الشخصية في هذا الشأن:

01 الرد الفوري:

فور استلام الطلب، يُؤكد مسؤول حماية البيانات الشخصية استلامه للطلب وتبلغ العميلة بأن طلبها قيد المعالجة.

02 التحقق من البيانات الشخصية:

يتحقق مسؤول حماية البيانات الشخصية من هوية العميلة للتأكد من أن مُقدمة الطلب هي صاحبة البيانات الشخصية (مثل: إرسال رمز تحقق لها)، مع مراعاة ألا يترتب على هذه الخطوة جمع بيانات شخصية حساسة.

03 جمع البيانات الشخصية:

يتعاون مسؤول حماية البيانات الشخصية مع الإدارات المعنية في شركة التجارة الإلكترونية لجمع البيانات الشخصية المطلوبة بصيغة واضحة ومفهومة.

04 توفير المعلومات:

توفر الشركة للعميلة إمكانية الوصول إلى بياناتها الشخصية المطلوبة، بما في ذلك فئات البيانات الشخصية التي تتم معالجتها وأي أطراف خارجية تتم مشاركة بياناتها الشخصية معها.

05 طلب التصحيح:

بعد مراجعة البيانات الشخصية المقدمة، لاحظت العملية بأن عنوانها قديم، لذا قامت بإرسال طلب آخر عبر البريد الإلكتروني إلى الشركة تطلب فيه تصحيح العنوان.

06 التصحيح الفوري:

تعمل الشركة على الفور على تحديث عنوان العميلة في سجلاتها، وإعلامها بالتصحيح الذي تم إجراؤه.

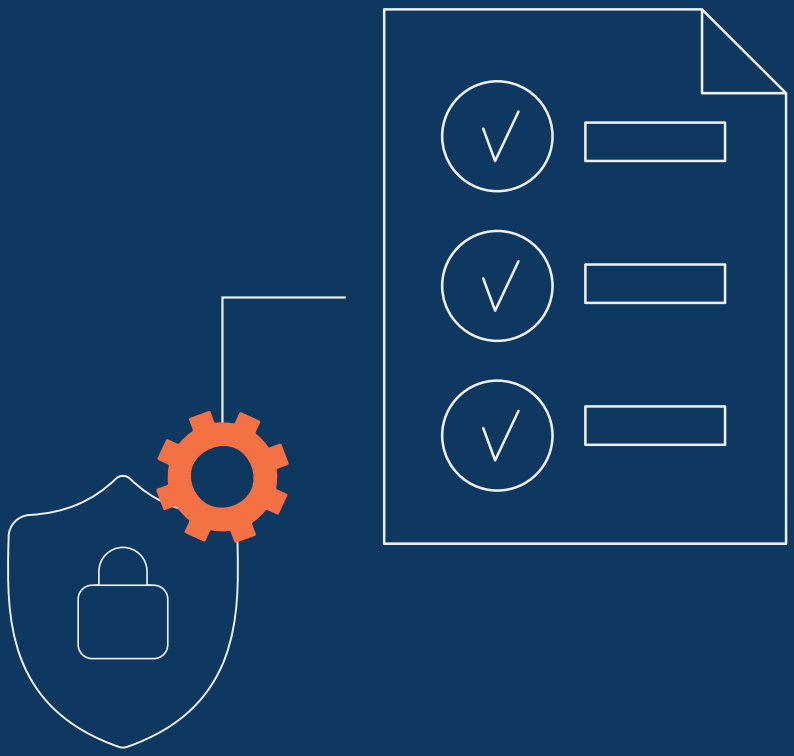
07 العدول عن الموافقة وحذفها:

قررت العميلة بعد بضعة أشهر عدم رغبتها في استقبال إحدى الحملات التسويقية، ولها الحق في العدول عن موافقتها وطلب حذف بياناتها المتعلقة بتلك الحملة من قائمة المستهدفين.

08 إيقاف عملية معالجة البيانات والالتزام بطلب حذف البيانات الشخصية:

تُراجع الشركة طلب العميلة وتُوقف عملية معالجة البيانات الشخصية وتحذف البيانات الشخصية للعميلة على النحو المطلوب.

القسم 04
إجراء تقويم الأثر



تنويه

يعد تقويم الأثـر إجـراءً هـاماً لتحديد مخاطر معالجة البيانات الشخصية.

يعد تقويم الأثرعملية منهجية تُستخدم لتقويم وإدارة المخاطرالمحتملة المتعلقة بمعالجة البيانات الشخصية وتنفيذ تدابير للتخفيف منها بشكل استباقي وحماية حقوق الأفراد وتحمّل مسؤولية معالجة البيانات الشخصية لدى الجهة.

كيف يمكنني إجراء تقويم الأثر؟

تقدم الهيئة السعودية للبيانات والذكاء الاصطناعي خدمة لتقويم الأثـر مُصممة لمساعدة الجهة على تقويم المخاطر المرتبطة بالمعالجة التي يُراد إجراؤها، وتمكن خدمة تقويم الأثـر الجهة من اتـخاذ قـرارات مدروسة للحد من مخاطر معالجة البيانات الشخصية.

وللقيام بإجراء تقويم الأثـر يرجى زيـارة خدمة تقويم الأثر في منصة حوكمة البيانات الوطنية، كما تم تحديد متطلبات عمليات تقويم الأثر باللوائح التنفيذية.

◀ مثال | إجراء تقويم الأثر

تخطط شركة تطوير برمجيات تعمل في المملكة لإطلاق تقنية جديدة قائمة على برمجيات لجمع وتحليل البيانات الشخصية من مصادر مختلفة للإعلانات المستهدفة، ونظراً إلى إدراك الشركة لاحتمالية تعرض حماية البيانات الشخصية للخطر بسبب هذه التقنية، ولمراعاة متطلبات نظام حماية البيانات الشخصية، تُقرر الشركة إجراء تقويم للأثر.

وفيما يلي الخطوات التي تتخذها الشركة في هذا الشأن:

01 النطاق والأهداف:

تحدد شركة البرمجيات نطاق تقويم الأثر والسمات والوظائف المحددة للتقنية المُراد تقويمها.

02 أنشطة معالجة البيانات الشخصية:

على شركة البرمجيات أن تقوم بحصر جميع أنشطة معالجة البيانات الشخصية المرتبطة بالتقنية وعليها أن تُوثق أنـواع البيانات الشخصية التي يتم جمعها وأغراض معالجة تلك البيانات والمسوغ النظامي وأي عمليات مشاركة أو إفصاح عن البيانات الشخصية مع أطراف خارجية.

03 تقويم المخاطر والحد منها:

تعمل شركة البرمجيات على تقويم مخاطر معالجة البيانات الشخصية المرتبطة بالتقنية من خلال دراسـة عـوامـل مثل: حساسية البيانات التي يتم جمعها، وحـوادث تسرب البيانات الشخصية المحتملة، والأثر المترتب على حقوق أصحاب البيانات الشخصية، ومبادئ النظام، ومدى ضرورة المعالجة وتوافقها مع الغرض، والوضع الحالي للتقنية، كما تحدد المخاطر المحتملة، مثل: الوصول غير المصرح به إلى البيانات الشخصية، والفترات الطويلة للاحتفاظ بالبيانات الشخصية بشكل غير مبرر.

بناءً على المخاطر المحددة، تُعد شركة البرمجيات مجموعة من الإجـراءات للحد من المخاطر المكتشفة وتضمن تطوير التقنية بما يتماشى مع مبدأ الخصوصية بالتصميم وبشكل افتراضي، وقد يشمل ذلك تنفيذ آليات التشفير، واعتماد ضوابط لحماية البيانات الشخصية وآليات الموافقة، وإجراء تقويم أمني منتظم، وتقديم إشعارات خصوصية واضحة وتتسم بالشفافية.

04 مشاركة الجهات المعنية:

تشارك شركة البرمجيات الجهات المعنية، مثل خبراء حماية البيانات الشخصية وتطوير البرمجيات لجمع الملاحظات والتأكد من أن عملية تقويم الأثر تساعد الشركة فعلاً على التعامل مع المخاطر على النحو المطلوب، كما تأخذ الشركة في الاعتبار وجـهـات نظر أصـحـاب البيانات الشخصية الـذيـن تتم معالجة بياناتهم والفرق الداخلية المسؤولة عن تطوير التقنية وإدارتها والشركاء الخارجيين المشاركين في معالجة البيانات الشخصية.

05 التوثيق واتخاذ القرارات:

تتولى شركة البرمجيات توثيق تقويم الأثر، بما في ذلك النتائج والتوصيات والقرارات المتخذة، بناءً على التقويم، كما تضمن أن يكون تقرير تقويم الأثر متاحاً للمراجعة من قبل الجهة المختصة أو الجهات الأخرى ذوات العلاقة.

06 المراجعة والتعديل:

على شركة البرمجيات إدراك أن عملية تقويم الأثر ليست نشاطاً يُنفذ لمرة واحـدة، بل تلتزم الشركة بمراجعته وتحديثه بشكل دوري أو عند إجراء تغييرات كبيرة على التقنية، ويُعد هذا النشاط بمثابة عملية متابعة وتقويم وتحسين مستمر لحماية البيانات

الشخصية بما يتماشى مع نتائج التقويم وتوصياته.

القسم 05
الخصوصية بالتصميم وبشكل افتراضي

تنويه

يُعد التعامل مع اعتبارات حماية البيانات الشخصية في المراحل المبكرة من عملية تطوير أنظمة المعلومات أكثر كفاءة وفاعلية من حيث التكلفة مقارنة بتنفيذ تدابير لحماية البيانات الشخصية في المراحل اللاحقة.

مبدأ الخصوصية بالتصميم وبشكل افتراضي في جميع مراحل دورة حياة معالجة البيانات الشخصية في الجهة، ليس متطلباً في النظام واللوائح بشكل مباشر ولكن يوصى بتطبيقه في جميع مراحل دورة الحياة لمعالجة البيانات الشخصية للالتزام بالنظام.

ويُقصد بتطبيق مبدأ الخصوصية بالتصميم وبشكل افتراضي مراعاة اعتبارات حماية البيانات الشخصية في كل مرحلة من مراحل عمليات ومنتجات وخدمات الجهة، ويشمل ذلك التعامل بشكل استباقي مع مخاطر معالجة البيانات الشخصية منذ البداية واعتماد ممارسات داعمة ومُعززة لحماية البيانات الشخصية، إذ يساهم هذا النهج في بناء الثقة بين الجهة والمستخدمين ويضمن الالتزام المستمر بنظام حماية البيانات الشخصية.

◄ مثال | تطبيق مبدأ الخصوصية بالتصميم وبشكل افتراضي

يعمل مركز طبي كبير في المملكة على تطوير بوابة إلكترونية للمرضى تتيح الوصول إلى السجلات الطبية وجدولة مواعيد المرضى بسهولة ويُسر، كما يسعى المركز إلى الاستفادة من هذه البوابة لتكون بمثابة منصة بحثية للأطباء لإجراء البحوث حول الأمراض التي تؤثر في سكان المملكة، قرر المركز الطبي تطبيق مبدأ الخصوصية بالتصميم وبشكل افتراضي لتطوير بوابة المرضى.

وفيما يلي الخطوات التي يتخذها المركز بهذا الخصوص:

ضوابط الوصول إلى البيانات الشخصية:

يُطبق المركز الطبي ضوابط صارمة للوصول أثناء تطوير بوابة المرضى إلى ضمان السماح لأخصائيي الرعاية الصحية المصرح لهم فقط بالوصول إلى سجلات المرضى، ويشمل ذلك تصاريح الوصول القائمة على الأدوار والمصادقة المتعددة العوامل.

01 الخصوصية في واجهة المستخدم:

يصمم المركز الطبي بوابة المريض مع الأخذ بالاعتبار خصوصية أصحاب البيانات الشخصية وحماية بياناتهم، لضمان عدم عرض البيانات الصحية الحساسة علناً أو عرضها على المستخدمين غير المصرح لهم، وتكشف البوابة عن البيانات الصحية ذوات الصلة بالمرضى عند تسجيل دخولهم بشكل آمن.

02 إدارة الموافقة:

ينفذ المركز الطبي نظام إدارة الموافقة وفقاً لنظام حماية البيانات الشخصية، إذ يتم إبلاغ المرضى بشكل صريح بأنشطة معالجة البيانات ويطلب موافقتهم قبل جمع بياناتهم الشخصية أو معالجتها.

03 إخفاء هوية أصحاب البيانات الشخصية:

يعمل المركز الطبي على إخفاء هوية المرضى قبل معالجة بياناتهم للأغراض البحثية، ويتيح ذلك للمركز وللأطباء الآخرين إجراء أبحاث قيمة حول صحة الأفراد مع الحفاظ على سرية البيانات الشخصية للمرضى.

04 تشفير البيانات:

يضمن المركز الطبي تشفير جميع البيانات الشخصية، في حال عدم معالجتها أوعند نقلها بين بوابة المريض وأنظمة المركز، وتقلل هذه العملية من خطر الوصول غير المصرح به أثناء ذلك، كما سيقوم المركز باستخدام ضوابط الترميز عند الاقتضاء.

05 عمليات التدقيق الدورية لحماية البيانات الشخصية:

يُجري المركز الطبي عمليات تدقيق منتظمة لتقويم الالتزام المستمر بمتطلبات نظام حماية البيانات الشخصية وتحديد مجالات التحسين، وذلك طوال عملية تطوير بوابة المرضى وبعد إطلاقها، وتساعد عمليات التدقيق هذه على تعامل المركز الطبي مع مخاطر معالجة البيانات الشخصية تعاملاً استباقياً.

06 برامج تدريبية لحماية البيانات الشخصية:

يتم إعـداد برامـج تدريبية لفريق تطوير البـوابـة والموظفين العاملين في المجال الطبي تختص بحماية البيانات الشخصية للاستزادة والإلمام بأهمية مبدأ الخصوصية بالتصميم وبشكل افتراضي، وكيفية التعامل مع بيانات المرضى وفقاً لنظام حماية البيانات الشخصية.

القسم 06

وضع إجراءات التعامل مع حوادث تسرب البيانات الشخصية

تنويه

يجب الإبلاغ عن حادثة تسرب البيانات الشخصية في الحالات التي تحددها اللوائح التنفيذية.

يعد تنفيذ إجـراءات التعامل مع حـالات تسرب البيانات الشخصية في غاية الأهمية لضمان الالتزام الفعال بأحكام نظام حماية البيانات الشخصية داخل الجهة، إذ تمكن هذه الإجراءات الجهة من الاستجابة الفورية وبالشكل المناسب في حالة تسرب البيانات الشخصية وفقاً للنظام، ومن خلال وجود إجراء واضح ومحدد للتعامل مع هذه الحالات، ويمكن للجهة الحد من آثارها بطريقة فعالة.

◄ مثال | وضع إجراءات التعامل مع حوادث تسرب البيانات الشخصية

تدرك الجهات المالية التي تعالج البيانات الشخصية على نطاق واسع بما في ذلك البيانات الائتمانية للعملاء مدى الحاجة إلى وجود إجراء للتعامل مع حوادث تسرب البيانات الشخصية.

وفيما يلي الخطوات التي تتخذها الجهة في هذا الخصوص:

01 تشكيل فريق الاستجابة للحوادث:

تشكل الجهة المالية فريقاً مختصاً للاستجابة لحوادث تسرب البيانات الشخصية على أن يشمل ممثلين من إدارات تقنية المعلومات والشؤون القانونية والالتزام والتواصل الخارجي، ويتولى الفريق مسؤولية إدارة أي حادثة تسرب بيانات شخصية مشتبه بها أو مؤكدة.

02 اكتشاف حوادث تسرب البيانات الشخصية وتقويمها:

ينفذ فريق الاستجابة للحوادث إجـراءات المراقبة والاكتشاف لتحديد حوادث تسرب البيانات الشخصية المحتملة على الفور، وفي حالة الاشتباه في الحادثة، يتم إجراء تقويم لتحديد طبيعة الحادثة ونطاقها.

03 تصنيف الحوادث:

بناءً على التقويم، يعمل فريق الاستجابة للحوادث على تصنيف حادثة تسرب البيانات الشخصية حسب مستوى جسامتها وخطورتها، ويأخذ في الاعتبار بعض العوامل مثل نوع البيانات المعرضة للخطر، وعدد أصحاب البيانات الشخصية المتضررين، والضرر المحتمل الذي قد ينشأ من الحادثة.

04 إشعار الجهة المختصة:

إذا كان من شأن تلك الحادثة الإضـرار بالبيانات الشخصية أوصاحب البيانات الشخصية أو كانت تتعارض مع حقوقه أو مصالحه، فيجب على الجهة المالية إشعار الجهة المختصة، مع الأخذ بالاعتبار تضمين جميع التفاصيل المطلوبة في الإشعار.

05 إشعار أصحاب البيانات الشخصية المتضررين:

يجب على الجهة المالية إشعـار أصحـاب البيانات الشخصية المتضررين إذا كان من شأن تلك الحادثة أن يترتب عليها ضرر على البيانات الشخصية للأفراد أو تتعارض مع حقوقهم أو مصالحهم.

06 التنسيق مع الجهات المختصة ذات العلاقة:

في حال كانت حادثة تسرب البيانات الشخصية تنطوي على نشاط إجرامي، يتعاون فريق الاستجابة للحوادث مع الجهات المختصة ذات العلاقة للتحقيق في الحادثة واتخاذ الإجـراءات النظامية اللازمة.

07 توثيق الحادثة وتحليلها:

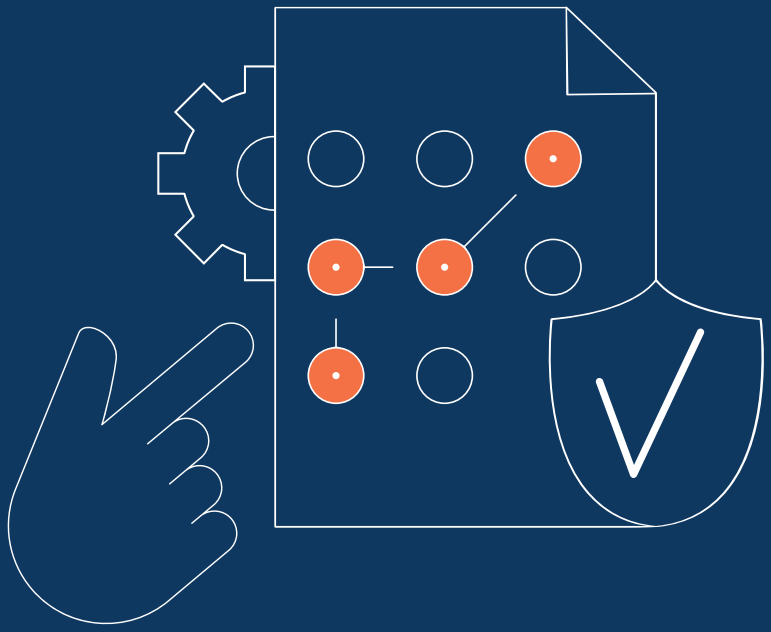
يعمل فريق الاستجابة للحوادث على توثيق جميع الإجـراءات المتخذة أثناء عملية الاستجابة لحادثة تسرب البيانات الشخصية، وانـطلاقاً من ذلك يُجري الفريق تحليل ما بعد الحادثة لتحديد الـدروس المستفادة وتنفيذ التحسينات اللازمـة لمنع وقـوع حوادث مماثلة في المستقبل.

قد تحتاج الشركة إلى إرسال إشعارات تسرب البيانات الشخصية إلى جهات تنظيمية أو هيئات أخرى حسب الاقتضاء.

كيف أتمكن من إشعار الجهة المختصة عن حادثة تسرب بيانات شخصية؟

إذا وقع لدى الجهة تسرب لبيانات شخصية، فمن الضروري الالتزام بمتطلبات الإبلاغ عن حوادث تسرب البيانات الشخصية، إذ إن هذه المتطلبات محددة في نظام حماية البيانات الشخصية واللوائح التنفيذية، وتقدم الهيئة السعودية للبيانات والذكاء الاصطناعي خدمة للإبلاغ عن حوادث تسرب البيانات الشخصية صممت لتقليل الوقت المستغرق في الإبلاغ، ويمكن إيجاد هذه الخدمة في منصة حوكمة البيانات الوطنية.

القسم 07
وضع تدابير تقنية وتنظيمية



تنويه

لا تقتصر التدابير التقنية والتنظيمية على تدابير الأمن السيبراني فحسب، بل تتجاوزها.

تعد التدابير التقنية والتنظيمية من العناصر الأساسية لأي برنامج فعال لحماية البيانات الشخصية، وتشمل التدابير التقنية ضوابط وتقنيات الأمن السيبراني، مثل تشفير البيانات وضوابط الوصول وأنظمة كشف الوصول غير المشروع للبيانات الشخصية، كما تتضمن التدابير التنظيمية السياسات والإجراءات والبرامج التدريبية لضمان معرفة الموظفين والجهات المعنية لمسؤولياتهم واتباع أفضل الممارسات لحماية البيانات الشخصية.

◄ مثال | وضع تدابير تقنية وتنظيمية

عملت شركة تقنية تقدم خدمات الحوسبة السحابية وتقنية المعلومات لعديد من العملاء، بما في ذلك الشركات والهيئات الحكومية، على تنفيذ التدابير التقنية والتنظيمية التالية لحماية البيانات الشخصية التي تتم معالجتها.

وفيما يلي الخطوات التي اتخذتها الشركة في هذا الشأن:

01 تشفير البيانات:
تستخدم الشركة بروتوكولات تشفير البيانات لضمان حماية جميع البيانات الشخصية المخزنة والمنقولة من خلال خدماتها السحابية بشكل آمن.

02 ضوابط الوصول المعقول:
لتقييد الوصول إلى البيانات للموظفين المصرح لهم فقط، تطبق الشركة ضوابط وصول مقيدة صارمة، إذ يُمنح الموظفون إمكانية الوصول بناءً على أدوارهم ومسؤولياتهم، ويتم استخدام التحقق من الهوية المتعدد العوامل لتعزيز الأمن.

03 ضوابط الوصول المادي:
لتقييد الوصول المادي إلى مراكز البيانات الخاصة بالشركة، تستخدم الشركة كاميرات الدوائر التلفزيونية المغلقة، والإضاءة والإنذارات الأمنية، وسجلات الزوار، وإشارات الهوية، وغيرها من التدابير المادية الصارمة التي تحمي مراكز البيانات من الوصول غير المصرح به.

04 ضوابط الأمن السيبراني:
تطبق الشركة ضوابط متقدمة للأمن السيبراني مثل جدران الحماية وعمليات المسح الدورية للبرمجيات الضارة والحماية من الفيروسات لتقليل احتمالية حوادث تسرب البيانات الشخصية وتحديد الثغرات.

05 تدريب الموظفين:
تقدم الشركة برامج تدريبية بشكل دوري لحماية البيانات الشخصية لجميع الموظفين، إذ يتم تثقيف الموظفين حول أفضل الممارسات للتعامل مع البيانات وسياسات حماية البيانات الشخصية والتهديدات الأمنية المحتملة.

06 خطة الاستجابة للحوادث:
في إطار مجموعة السياسات والإجراءات الخاصة بالشركة، فقد وضعت الشركة خطة استجابة للحوادث لتحديد الإجراءات الواجب إتباعها في حالات حوادث تسرب البيانات الشخصية أو أي حادث أمني.

07 الحد الأدنى من البيانات الشخصية:
تطبق الشركة مبدأ الحد الأدنى من معالجة البيانات الشخصية كجزء من إطار الخصوصية بالتصميم الخاص بها، إذ يتم جمع البيانات الشخصية اللازمة لتقديم خدماتها فقط وتحتفظ بها، مما يقلل من المخاطر المرتبطة بتخزين البيانات الشخصية بشكل مفرط.

08 إدارة المورّدين:
تتعاون الشركة مع موزّدين خارجيين ومتعاقدين من الباطن لتنفيذ الخدمات السحابية التي تقدمها لعملائها، ولضمان الالتزام بحماية البيانات الشخصية على مستوى سلسلة الإمداد، تضع الشركة متطلبات تعاقدية مقيدة فيما يتعلق بإجراءات معالجة البيانات الشخصية.

القسم 08

مشاركة البيانات الشخصية داخل المملكة

تنويه

يجب الالتزام بمتطلبات نظام حماية البيانات الشخصية واعتماد التدابير التقنية والتنظيمية المناسبة عند المشاركة أو الإفصاح عن البيانات الشخصية لجهة داخل المملكة.

ومن خلال مشاركة البيانات الشخصية داخل المملكة بمسؤولية وشفافية، يمكن للجهة ضمان خصوصية الأفراد وحماية بياناتهم ومعالجتها للأغراض المصرح بها فقط.

◄ مثال | مشاركة البيانات الشخصية داخل المملكة

يقدم البنك الذي يعمل داخل المملكة خدمات مالية مختلفة لعملائه، بما في ذلك إدارة الحسابات والقروض والاستثمارات، ويجمع البنك في إطار عملياته البيانات الشخصية لعملائه ويعالجها ويشاركها مع جهة المعالجة.

وفيما يلي الخطوات التي يتخذها البنك:

01 معالجة بيانات العملاء:

يجمع البنك البيانات الشخصية لعملائه ويعالجها، بما في ذلك الأسماء والعناوين والمعاملات المالية والمعاملات الائتمانية السابقة، وتُستخدم هذه البيانات الشخصية لتقديم الخدمات المصرفية وإدارة الحسابات وتقويم الجدارة الائتمانية.

02 مشاركة البيانات الشخصية:

لتسهيل تقديم الخدمات للعملاء ولتشغيل الحساب البنكي للعميل يشارك البنك بيانات العميل الشخصية المحددة مع جهة المعالجة لإجراءات معرفة العميل.

03 المراجعة القانونية ومراجعة مدى الالتزام:

قبل مشاركة البيانات الشخصية للعملاء مع جهة المعالجة، يراجع البنك ممارسات مشاركة البيانات وفقاً للنظام واللوائح التنفيذية للتأكد من وجود الضمانات اللازمة، على سبيل المثال: للتأكد من أن جهة المعالجة قد قدمت الضمانات اللازمة لحماية البيانات الشخصية، ووجود إجراءات متابعة بين الأطراف، وتحديد المسوغ النظامي للإفصاح عن البيانات، إلخ.

04 ضوابط الوصول:

يطبق البنك ضوابط وصول صارمة ضمن أنظمته الداخلية، إذ يُمنح الموظفون حق الوصول فقط إلى البيانات الشخصية اللازمة لأدوارهم، مما يقلل من مخاطر الوصول غير المصرح به ويضمن أمن البيانات الشخصية.

05 تدريب الموظفين:

لضمان الوعي بالتعامل النظامي مع البيانات الشخصية للعملاء، يقدم البنك برامج تدريبية لحماية البيانات الشخصية والإفصاح عنها.

06 التواصل بشفافية:

يتم تضمين معلومات حول ممارسات مشاركة البيانات الشخصية في إشعار الخصوصية، كما يتم إبلاغ العملاء بالغرض من مشاركة البيانات الشخصية والإدارات المعنية والضمانات المتخذة لحماية بياناتهم الشخصية.

07 المراقبة المستمرة:

يراقب البنك عمليات مشاركة البيانات الخاصة به بانتظام لضمان فاعلية ضوابط الوصول واستخدام البيانات الشخصية للأغراض الموثقة فقط، كما تتم معالجة أي محاولات وصول غير مصرح بها أو أنشطة مشبوهة.

08 إتلاف أو استعادة البيانات الشخصية:

بمجرد الانتهاء من المعالجة من قبل جهة المعالجة، يتم إتلاف البيانات الشخصية أو تمكين البنك من استعادتها.

القسم 09

نقل البيانات الشخصية خارج المملكة

تنويه

تخضع عمليات نقل البيانات الشخصية خارج المملكة لمتطلبات إضافية بموجب نظام حماية البيانات الشخصية واللوائح التنفيذية.

تتضمن عملية نقل البيانات الشخصية خارج المملكة نقلاً للبيانات الشخصية خارج الحدود الجغرافية للمملكة، وغالباً ما تكون هذه العملية ضرورية للعمليات التجارية أو لتقديم الخدمات على نطاق عالمي (مثلاً: أثناء استخدام حلول التخزين السحابي)، وتخضع هذه الترتيبات للمتطلبات المحددة المنصوص عليها في نظام حماية البيانات الشخصية واللوائح التنفيذية.

مثال | نقل البيانات الشخصية خارج المملكة

تقدم شركة تقنية دولية -غير مشمولة بقائمة دول الاعتماد للمملكة- حلولاً للبرمجيات وخدمات تقنية المعلومات للعملاء في جميع أنحاء العالم، بما في ذلك المملكة، وفي إطار عملياتها حول العالم، تعمل الشركة على جمع البيانات الشخصية من العملاء والموظفين والشركاء ومعالجتها.

وفيما يلي الخطوات التي تتخذها الشركة[1]:

01 التواصل مع العملاء الدوليين:

تبرم الشركة عقداً مع عميل في المملكة لتقديم خدمات تطوير برمجيات مخصصة، ويقدم العميل بيانات موظفيه الشخصية لفتح الحساب وإدارة المشروع.

02 ضرورة نقل البيانات الشخصية:

لتقديم الخدمات لعملائها بكفاءة، تحتاج الشركة إلى مشاركة بعض البيانات الشخصية لمواطنين سعوديين، بما في ذلك أسماء الموظفين ومعلومات الاتصال، مع فريق التطوير الموجودة في الدولة غير المعتمدة، ولذلك قررت الشركة نقل البيانات الشخصية خارج المملكة.

03 ضرورة نقل البيانات الشخصية:

نظراً إلى أن النقل إلى دولة غير معتمدة، فعلى الشركة مراجعة المادة التاسعة والعشرين من النظام ووسائل النقل والضمانات المذكورة في لائحة نقل البيانات الشخصية خارج المملكة لضمان الآتي، (على سبيل المثال):

- ما إذا كان النقل سيؤثر في الأمن الوطني أو مصالح المملكة الحيوية.
- ما إذا كان نقل البيانات الشخصية خارج المملكة سيقتصر على الحد الأدنى اللازم لتحقيق الغرض من النقل.
- ما إذا كان قد تم الأخذ بالاعتبار حقوق أصحاب البيانات الشخصية.
- ما إذا كان قد تم تحديد غرض نقل البيانات الشخصية وتقييده.
- وجود الضمانات المناسبة، على سبيل المثال: القواعد المشتركة الملزمة والبنود التعاقدية القياسية وغيرها.
- ما إذا كان قد تم إجراء تقويم أثر على عملية النقل.

04 إشعارات الخصوصية والشفافية:

تعمل الشركة وعميلها على تحديث إشعارات الخصوصية الخاصة بها لإعلام الجهات المعنية ذوات الصلة بنقل البيانات الشخصية خارج المملكة، بما في ذلك الأسس والضمانات النظامية المعمول بها.

05 الاحتفاظ بالبيانات الشخصية:

بمجرد اكتمال الاتفاق، تبادر الشركة بإتلاف أي بيانات شخصية يتم نقلها بشكل آمن، وفقاً لشروط اتفاقية مشاركة البيانات.

1 يرجى ملاحظة أن هذه الخطة مختصرة، يجب إجراء مراجعة تفصيلية لنظام واللوائح التنفيذية لضمان الامتثال لمتطلبات نقل البيانات الشخصية خارج المملكة.

القسم 10
مراقبة ومتابعة الالتزام

تنويه

تعد عملية مراقبة ومتابعة الالتزام عملية مستمرة يجب إجراؤها بانتظام لضمان الالتزام المستمر بنظام حماية البيانات الشخصية.

تعد عملية مراقبة ومتابعة الالتزام، من الجوانب الحيوية لتحقيق الالتزام الفعال لأحكام نظام حماية البيانات الشخصية داخل الجهة، وتتضمن إجراء تقييم مستمر لضمان الالتزام بنظام حماية البيانات الشخصية وسياسات حماية البيانات الشخصية الداخلية، إذ تساعد المتابعة المنتظمة في الكشف عن مخاطر معالجة البيانات الشخصية المحتملة ونقاط الضعف في الممارسات، وتوفر عمليات التدقيق تقييماً شاملاً لبرنامج الالتزام بأحكام حماية البيانات الشخصية في الجهة، ومن خلال المراقبة والمتابعة بشكل مستمر يمكن للجهة معالجة أي مشاكل بشكل استباقي وإجراء التحسينات اللازمة وإثبات الالتزام بنظام حماية البيانات الشخصية.

◄ مثال | مراقبة ومتابعة الالتزام

يتعامل أحد الفنادق الفاخرة الشهيرة مع بيانات شخصية على نطاق واسع لنزلائه، بما في ذلك بياناتهم الشخصية وتفاصيل الدفع ومفضلاتهم، وللحفاظ على مستوى عالٍ لحماية البيانات الشخصية والالتزام بالنظام، يطبّق الفندق برنامجاً متقدماً وصارماً للمراقبة و متابعة الالتزام.

وفيما يلي الخطوات التي يتخذها الفندق:

01 المراقبة المستمرة:

يجري الفندق عمليات مراقبة داخلية منتظمة لضمان اتباع موظفيه لسياسات وإجراءات حماية البيانات الشخصية المعمول بها، كما يتولى فريق الإدارة مراجعة ضوابط الوصول وممارسات التعامل مع البيانات الشخصية بشكل دوري لتحديد أي مشاكل محتملة فيما يتعلق بالالتزام.

02 المراقبة التنظيمية:

تعمل الإدارة القانونية في الفندق على متابعة أي تحديث يصدرعن الجهات التنظيمية المعنية بحماية البيانات الشخصية وتبقى على اطلاع بأحكام الاتفاقيات الدولية المتعلقة بحماية البيانات الشخصية.

03 مراقبة حوادث تسرب البيانات الشخصية:

يستخدم الفندق نظاماً لمراقبة أي حوادث لتسرب البيانات الشخصية، إذ ينبّه نظام المراقبة مسؤول حماية البيانات الشخصية وفريق الاستجابة لتسرب البيانات الشحصية في الوقت الفعلي في حال اكتشاف أي أنشطة غير اعتيادية.

04 عمليات المراجعة الخارجية:

يتعاقد الفندق مع مراجع خارجي لإجراء عمليات مراجعة منتظمة لبرنامج الالتزام بأحكام نظام حماية البيانات الشخصية، وفي هذا الصدد يعمل المدقق الخارجي على تقويم فاعلية ضوابط حماية البيانات الشخصية وممارسات معالجة هذه البيانات والالتزام بمتطلبات نظام حماية البيانات الشخصية.

05 سجلات الوصول إلى بيانات النزلاء:

يحتفظ الفندق بسجلات الوصول لتتبع وصول الموظفين إلى بيانات النزلاء، ويساعد ذلك على مراقبة وكشف أي وصول غير مصرح به أو حوادث محتملة لتسرب البيانات الشخصية.

اختبار الاستجابة للحوادث: لضمان الجاهزية في حوادث تسرب البيانات الشخصية، يُجري الفندق اختبارات الاستجابة للحوادث بشكل دوري، ويتضمن ذلك محاكاة سيناريوهات مختلفة لتقويم مدى فاعلية إجراءات الاستجابة المتبعة في الفندق.

06 إدارة المورّدين:

نظراً إلى طبيعة عمل الفندق في قطاع الضيافة، فيعتمد على عديد من المورّدين والشركاء لتقديم الخدمات، وانطلاقاً من ذلك، يطبق الفندق برنامج إدارة الموردين الذي يتضمن النص على متطلبات حماية البيانات الشخصية في العقود ويُجري عمليات تدقيق دورية للموردين فيما يتعلق بمعالجتهم للبيانات الشخصية لضمان التزامهم.

ما هي المصادر المتاحة للجهات لضمان الالتزام المستمر؟

تقدم الهيئة السعودية للبيانات والذكاء الاصطناعي خدمة للتقييم الذاتي للالتزام، وهي أداة مساعدة للجهات لمعرفة مدى التزامهم بأحكام النظام، تتضمن المجالات الأساسية لبرنامج الالتزام بأحكام نظام حماية البيانات الشخصية، ويمكن الاستفادة من الخدمة عن طريق زيارة خدمة التقييم الذاتي للالتزام في منصة حوكمة البيانات الوطنية.

وللإطلاع على النظام كاملاً ولوائحه التنفيذية الرجاء زيارة موقع سدايا الإلكتروني

منصة حوكمة البيانات الوطنية