جمعية إدارة البيانات

الدليـــل الإرشـادي لنظـام حماية البيانات الشخصية للأفـــراد والمنظمـــات

نسخـــة 1

سبتمبر ٢٠٢٤

المحتويات

مقدمة عن الدليل

1.1 مقدمة

في خطوة ممكنة نحو الحماية الشاملة لبيانات الأفراد، صدر نظام حماية البيانات الشخصية بالمرسوم الملكي رقم (م/19) وتاريخ 9 /2/ 1443هـ والمعدل بموجب المرسوم الملكي رقم (م/148) وتاريخ 5 /9/ 1444هـ والذي **دخل حيز النفاذ في 14 سبتمبر 2024م**. ويعتبر النظام تطورًا هامًا في المشهد التشريعي في المملكة، حيث يتوافق مع أهداف رؤية 2030 لدعم التحول الرقمي والابتكار وتنمية الاقتصاد الرقمي والمعرفي.

1.2 نظرة عامة

تهدف جمعية إدارة البيانات "داما السعودية" من خلال إصدار هذا الدليل إلى مساعدة الأفراد والجهات على فهم مبادئ نظام حماية البيانات الشخصية لتعزيز تدابير وإجراءات الحماية والتعريف بكيفية تحقيق الامتثال الكامل لمتطلبات نظام حماية البيانات الشخصية السعودي.

1.3 الغرض من الدليل

- توضيح مفهوم البيانات الشخصية وأنواعها
- إلقاء الضوء على نظام حماية البيانات الشخصية السعودي وأهم ملامحه
- التعريف بحقوق الأفراد وكيفية ممارستها
- التعريف بخطة الامتثال للإيفاء بمتطلبات النظام

مقدمة عن النظام وقواعده

2.1 ماهي البيانات الشخصية؟ وما أنواعها؟

يركز نظام حماية البيانات الشخصية على البيانات الشخصية والبيانات الشخصية الحساسة وفيما يلي تعريف كلاً منهما:

البيانات الشخصية: هي أي بيان -مهما كان مصدره أو شكله- يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكنًا بصفة مباشرة أو غير مباشرة، ومن ذلك: الاسم، ورقم الهوية الشخصية، والعناوين، وأرقام التواصل، وأرقام الرُّخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي.

البيانات الشخصية الحساسة: هي نوع خاص من البيانات الشخصية تتطلب حماية إضافية نظرًا لطبيعتها الحساسة واحتمالية تأثيرها الكبير على حياة الأفراد إذا تم إساءة استخدامها أو الكشف عنها دون إذن. ويشمل ذلك كل بيان شخصي يتعلق بأصل الفرد العرقي، أو أصله الإثني، أو معتقده الديني، أو السياسي أو حالته الصحية وتاريخه المرضي. وكذلك البيانات الجنائية والأمنية، أو بيانات السمات الحيوية التي تحدد الهوية، أو البيانات الوراثية، أو البيانات الائتمانية، أو بيانات تحديد الموقع، والبيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهما.

وبحسب التصنيفات العالمية، يتم تصنيف البيانات الشخصية بحسب درجة الحساسية أو بحسب مجال البيان. وفيما يلي أبرز تصنيفات البيانات الشخصية مع أمثلة عليها:

ملخص لأنواع البيانات الشخصية

نوع البيانات	نوع التصنيف	التعريف	الأمثلة
البيانات الشخصية (أو كما تعرف بالبيانات الشخصية التعريفية) Personally Identifiable Information (PII)	عام	أي بيان يمكن استخدامه لتحديد هوية الفرد، سواء بمفردها أو بدمجها مع بيانات أخرى	الاسم، الأسماء السابقة، الجنس، الجنسية، تاريخ ومكان الميلاد، البريد الإلكتروني، الحالة الاجتماعية، الهوية الوطنية/الإقامة، رقم جواز السفر وأي مستندات أخرى مماثلة، عنوان السكن أو العمل، رقم الهاتف المحمول، سجل التوظيف، تفاصيل العائلة، التعليم، بروتوكول الإنترنت.
البيانات الشخصية الحساسة Sensitive Personal Information (SPI)	بحسب الحساسية	نوع خاص من أنواع (PII) والتي تعتبر أكثر حساسية وتتطلب مستويات أعلى من الحماية بسبب طبيعتها الحساسة والتي يمكن أن تؤثر بشكل بالغ على الأفراد، ويشمل ذلك السمات الحيوية والبيانات الوراثية والصحية.	الأصل العرقي أو القبلي، الآراء السياسية، المعتقدات الدينية، حالة الإعاقة، الصور أو مقاطع الفيديو، السجل الجنائي، محادثة هاتفية مسجلة، بصمات الأصابع أو أنماط الصوت أو التعرف على الوجه، أي بيان يدل على أن الفرد مجهول الأبوين أو أحدهما.
البيانات الصحية Protected Health Information (PHI)	بحسب الموضوع/ المجال	أي بيان شخصي يتعلق بحالة الفرد الصحية، سواءً الجسدية، أو العقلية أو النفسية أو متعلقة بالخدمات الصحية المقدمة له.	السجلات الطبية، التاريخ المرضي، التفاصيل الجينية، التفاصيل البيومترية، نتائج الفحوصات والتحاليل، فصيلة الدم، الأدوية التي تم أخذها.
البيانات الائتمانية والمالية Personal Financial and Credit Information (PFI)		كل بيان شخصي يتعلق بطلب الفرد الحصول على تمويل، أو حصوله عليه، سواءً لغرض شخصي أو عائلي، من جهة تُمارس التمويل، بما في ذلك أي بيان يتعلق بقدرته على الحصول على ائتمان أو بقدرته على الوفاء به أو بتاريخه الائتماني.	الراتب، العمليات المالية، الدخل، مصادر الدخل، الأصول، قيمة الأصول، الإيرادات، معلومات بطاقة الائتمان، أرقام الحسابات المصرفية، كشف الحساب، معلومات القروض الشخصية، معلومات الاستثمارات، درجة الائتمان، التاريخ الائتماني في سمة، تفاصيل حول المدفوعات من وإلى الحسابات الشخصية بما في ذلك سداد أي قرض أو تسهيل ائتماني وأسماء المستفيدين وعناوينهم وتفاصيل المعاملات.

البيانات الوراثية (Genetic Data)		كل بيان شخصي يتعلق بالخصائص الوراثية أو المكتسبة لشخص طبيعي، يحدد بشكل فريد السمات الفيسيولوجية أو الصحية لذلك الشخص ويستخلص من عينة بيولوجية للشخص مثل تحليل الحمض النووي أو تحليل أي عينة أخرى تؤدي إلى استخلاص بيانات وراثية.	الجينوم، الجينات، تسلسل البروتين، التركيب الوراثي، الصفات الوراثية، التغيرات الوراثية، الكروموسومات، البصمات الوراثية.

2.2 تصنيف البيانات الشخصية، أين تتقاطع ومتى تفترق؟

التصنيف قد يتم على حسب نوع الحساسية أو المجال (مالي، صحي، جنسي، عرقي الخ) وقد تختلف بعض العوامل فيختلف تصنيف نفس البيان.

لكن البيانات الشخصية التعريفية يمكن أن تشير إلى أي من الأنواع أعلاه بينما البيانات الشخصية الصحية -على سبيل المثال- تشير إلى البيانات المتعلقة بالمجال الصحي فقط) وقد ينتقل بيان محدد من نوع لأخر بتغير بعض المعطيات.

مثال رقم 1: عنوان المريض بحد ذاته يعتبر من البيانات الشخصية التعريفية (PII). لكن عندما يتم تقديم **عنوان المريض** مع بيانات حول تنويم المريض وتاريخه المرضي يتحول **عنوان المريض** لبيان صحي (PHI).

مثال رقم 2: أجوبة اختبار (الأجوبة بحد ذاتها كبيان وليس بيانات المُمتحن التعريفية) بشكلها الالكتروني (بدون بيانات الممتحن التعريفية) قد لا تعتبر من البيانات الشخصية. لكن الأجوبة المكتوبة بخط اليد قد تعتبر من البيانات الشخصية لإمكانية تمييز صاحبها.

2.3 ماهي أبرز ملامح نظام حماية البيانات الشخصية السعودي؟

يعد النظام إطارًا شاملًا لحماية البيانات الشخصية للأفراد في المملكة العربية السعودية. وقد خضع لعدة مراجعات لاستيعاب موجات التطور التقني وموائمته مع الحقوق التي كفلها القانون السعودي والمعايير الدولية. يهدف النظام إلى تنظيم معالجة البيانات الشخصية داخل المملكة العربية السعودية وحماية خصوصية الأفراد المقيمين داخل المملكة.

1. **نطاق تطبيق النظام**
يتمتع النظام بنطاق واسع للغاية خارج الحدود الإقليمية، فينطبق على جميع المؤسسات العامة والخاصة العاملة في المملكة العربية السعودية، بغض النظر عن مكان معالجة البيانات. بالإضافة إلى المنظمات خارج المملكة التي تقوم بمعالجة البيانات الشخصية والبيانات الشخصية الحساسة للمواطنين وللأفراد المقيمين داخل المملكة "بما في ذلك الأشخاص المتوفيين" بأي وسيلة كانت.
2. **أخذ الإذن والموافقات**
يتطلب نظام حماية البيانات الشخصية الحصول على موافقة صريحة ومحددة وحرة من أصحاب البيانات الشخصية وتوثيقها عند معالجة بياناتهم، باستثناء بعض الحالات كأن تُحقق المعالجة مصلحة معينة لصاحب البيانات وصعوبة الوصول له، أو مطلوبة بموجب القانون أو اتفاقية أو لأغراض عامة علمية أو أمنية وتلبية متطلبات قضائية. كما ويجوز لأصحاب البيانات سحب الموافقة في أي وقت.
3. **تقييد وتحديد الغرض**
يجب ألا تحيد المعالجة لاحقًا عن الأغراض الأولية التي تم من أجلها جمع البيانات.
4. **مدة الاحتفاظ بالبيانات**
يجب إتلاف البيانات التي تم جمعها إذا اتضح أنها لم تعد ضرورية لتحقيق الغرض من جمعها.
5. **حقوق أصحاب البيانات**
يمنح النظام أصحاب البيانات عدة حقوق فيما يتعلق ببياناتهم الشخصية. وتشمل حق العلم بغرض وطرق الاستخدام وحق الوصول للبيانات وحق طلب تصحيحيها أو تحديثها وحق طلب إتلافها وحق الاعتراض ورفض أو تقييد معالجتها. كما ولأصحاب البيانات الحق في تقديم شكوى فيما يتعلق بعدم تطبيق النظام للجهات المختصة.
6. **آمن البيانات**
يجب على المنظمات ضمان أمن وسرية البيانات الشخصية من خلال تنفيذ التدابير التنظيمية والإدارية والفنية المناسبة.
7. **عمليات نقل البيانات عبر الحدود**
يحتوي النظام على متطلبات تفصيلية لنقل البيانات الشخصية خارج المملكة العربية السعودية، فباستثناء حالات حماية حياة أو المصلحة الحيوية لصاحب البيانات، أو للوقاية من مرض أو علاجه، أو الوفاء بالتزامات تعاقدية تشمل المملكة كطرف فيها، لا يمكن نقل البيانات إلى أطراف خارج المملكة إلا إذا كان ذلك يخدم مصالح المملكة. وحتى في مثل هذه الحالات، يجب أن يستوفي نقل البيانات الشروط التالية:
    أ. يجب ألا يضر بالأمن الوطني أو المصالح الحيوية للمملكة.
    ب. يجب حماية البيانات لمنع تسربها أو الكشف عنها.
    ج. يقتصر النقل على الحد الأدنى من البيانات المطلوبة.
    د. موافقة الجهات المختصة وفق ما تحدده اللوائح

وقد يتم إعفاء المنظمة من هذه الشروط إذا كانت الدولة أو المنظمة المتلقية للبيانات توفر مستوى مناسبًا من الحماية للبيانات الشخصية، على ألا تكون بيانات حساسة.

8. **الاحتفاظ بالسجلات**
يجب على المنظمات الاحتفاظ بسجلات أنشطة معالجة البيانات الشخصية، وإتاحة هذه السجلات للجهة المختصة عند الطلب، على أن تتضمن السجلات: تفاصيل الاتصال والغرض من المعالجة والأفراد والأطراف التي يتم الكشف لها عن البيانات والمدة التي يتم خلالها الاحتفاظ بالبيانات.

9. **الجهة المسؤولة**

الهيئة السعودية للذكاء الاصطناعي والبيانات "سدايا" هي الجهة التنظيمية الرئيسية التي ستشرف على تطبيق نظام حماية البيانات الشخصية وضمان الامتثال والتحقق من الشكاوى وفرض العقوبات عند الانتهاكات. بالإضافة إلى ذلك ستقوم سدايا بتقديم المشورة للمنظمات فيما بتعلق بعمليات نقل البيانات، و تتبع طلبات حقوق أصحاب البيانات التي تتلقاها المنظمات، خلال العاميين الأوليين. وبعد ذلك، سيتولّى "مكتب إدارة البيانات الوطنية" الإشراف على تنفيذ النظام.

10. **عقوبات عدم الامتثال**

مخالفة أحكام نقل البيانات تؤدي إلى إمكانية السجن لمدة لا تزيد عن سنة و/أو غرامة لا تزيد عن مليون. كما وأن عدم الامتثال فيما لم يرد في شأنه نص خاص قد يؤدي إلى فرض غرامات تصل إلى 5 ملايين، يمكم مضاعفتها في المخالفات المتكررة. بالإضافة إلى ذلك، إمكانية السجن لمدة تصل لسنتين و/أو غرامة لا تتجاوز 3 ملايين في حال الكشف عن بيانات شخصية أو نشرها بقصد الإضرار بصاحب البيانات أو لتحقيق منفعة الشخصية.

11. **إشعار خرق البيانات**

بموجب أحكام نظام حماية البيانات الشخصية، يتعين على المنظمات إخطار السلطات التنظيمية على الفور (لمدة لا تتجاوز 72 ساعة) بمجرد علمهم بأي خروقات للبيانات. وفي حال كان الانتهاك سيتسبب بضرر جسيم فيجب إبلاغ الشخص المتضرر على الفور.

حقوق أصحاب البيانات الشخصية وكيفية ممارستها

3.1 ماهي الحقوق التي كفلها لك النظام؟

كصاحب بيانات شخصية، كفل لك النظام عدد من الحقوق أهمها **حقك** في:

1 - **العلم:** يشمل ذلك تزويدك بمعلومات حول الأساس القانوني لجمع بياناتك الشخصية، والغاية من جمعها، بالإضافة إلى تحديد هوية الجهة التي تجمع البيانات الشخصية وعنوانها، وكذلك الجهات التي سيتم الإفصاح لها عن هذه البيانات وصفاتها. كما يجب توضيح ما إذا كانت البيانات ستُنقل أو تُفصح عنها أو تُعالج خارج المملكة، بالإضافة إلى توضيح الآثار والمخاطر المحتملة التي قد تنجم عن عدم إتمام عملية الجمع.
2 - **الوصول لبياناتك الشخصية:** يشمل ذلك طلب الحصول على نسخة من بياناتك الشخصية المتاحة لدى الجهة المسؤولة بصيغة مفهومة وقابلة للقراءة.
3 - **طلب تصحيح بياناتك الشخصية:** يشمل ذلك تحديث بياناتك أو اكمالها في حال النقص.
4 - **طلب إتلاف بياناتك الشخصية:** يشمل ذلك التخلص منها وتعذر الاطلاع عليها أو استعادتها مرة أخرى.
5 - **الرجوع عن الموافقة على معالجة بياناتك:** في حال موافقتك على طلب معالجة لبياناتك الشخصية وأردت العدول عن ذلك، فالنظام يكفل لك حقك في الرجوع عن الموافقة فيما عدا بعض الأحوال المنصوص عليها في نظام حماية البيانات الشخصية ولائحته التنفيذية.

3.2 بياناتك هي حق لك، فكيف تمارس هذا الحق؟

يمكنك معرفة كيفية يمكنك ممارسة حقوقك عن طريق قراءة سياسة الخصوصية لدى الجهة (والتي تكون منشورة بالبوابة الداخلية للجهات والمنظمات أو المواقع الإلكترونية للمتاجر والمواقع) والتي يجب أن توضح ذلك حيث قد قد تمارس بعض الحقوق عن طريق خصائص يتم بنائها بالنظام (مثل التعديل والحذف وتحديث الرغبات) وقد تكون عن طريق التواصل عبر نموذج أو ايميل مخصص. وفيما يلي بعض الأمثلة:

حق العلم:

وبعدها بإمكانك معرفة كيف سيتم جمع ومعالجة وتخزين بياناتك الشخصية:

الخصوصية

إن stc تحترم خصوصيتك ويتمثل هدفنا في تقديم خدمة ممتازة لجميع عملائنا. حيث تمت صياغة إشعار الخصوصية هذا وفقًا لقانون ولوائح حماية البيانات الشخصية في المملكة العربية السعودية وذلك لغرض مساعدتك على فهم طبيعة البيانات التي نجمعها منك وكيف سيتم التعامل مع هذه البيانات من قبل stc
ينطبق إشعار الخصوصية هذا على جميع القطاعات ووحدات الأعمال في الشركة. ويلتزم جميع موظفي الشركة والمقاولين والمتعاقدين الذين يعملون إما على أساس دائم أو مؤقت باتباع المعايير المحددة

لماذا نجمع بياناتك الشخصية ونستخدمها:
لتقديم أعلى مستوى من الخدمة والمنتجات، نجمع بياناتك الشخصية ونستخدمها.

الأساس القانوني لمعالجة بياناتك الشخصية هو:
• تعاقدي - للوفاء بالتزامات الخدمة تجاهك.
• الموافقة - للأنشطة الأخرى مثل المعلومات والمبيعات والتسويق.
• الالتزام القانوني - للامتثال للمتطلبات الحكومية بما في ذلك على سبيل المثال لا الحصر، الأمن القومي وحماية الصحة العامة.

تشمل أغراض جمع هذه البيانات ما يلي:
• تمكيننا من تطوير المنتجات والخدمات وتحسينها و/ أو تسويقها و/ أو توصيلها لعملاء stc .
• تمكين ودعم عملياتنا وأنظمتنا لضمان استمرارية خدماتنا وجودتها وتقديم فواتير دقيقة وتمكيننا من معالجة مدفوعات المنتجات والخدمات.

حق الوصول لبياناتك الشخصية:

حق تصحيح البيانات الشخصية:

حق الرجوع عن الموافقة على معالجة بياناتك:

5. الحق في الرجوع عن الموافقة: يمكن لأصحاب البيانات الرجوع عن موافقتهم على معالجة بياناتهم الشخصية في أي وقت، ما لم تكن هناك أسباب مشروعة تستدعي استمرار المعالجة. البريد الإلكتروني: Data_Statistics@

الأساس النظامي لجمع ومعالجة البيانات الشخصية :

البيانات الشخصية تُجمع وتُعالج بناءً على موافقة من صاحب البيانات. يحتفظ صاحب البيانات بحق سحب موافقته في أي وقت، ما لم يكن هناك أساس نظامي يستلزم الاحتفاظ بهذه البيانات. لسحب الموافقة أو لأي استفسارات أخرى متعلقة بالبيانات، يمكن التواصل مع مكتب إدارة البيانات في أمانة المدينة عبر البريد الإلكتروني Data_Statistics@.

3.3 كيف يمكنك تقديم شكوى لمخالفة النظام؟

يمكن للأفراد تقديم الشكاوى والبلاغات عن تسرب البيانات الشخصية من خلال منصة حوكمة البيانات (اضغط هنا) حيث يتم النظر بالشكاوي من قبل الجهة المشرعة (سدايا) واتخاذ العقوبات الواردة في النظام في حال ثبوت ذلك والتي تصل إلى السجن لمدة تصل لسنتين و/أو غرامة لا تتجاوز 5 ملايين ريال.

دور الجهات التي تتعامل مع البيانات الشخصية وكيف تحقق الامتثال

4.1 أدوار الجهات فيما يتعلق بالبيانات الشخصية

ينص نظام حماية البيانات الشخصية على دورين للجهات فيما يتعلق بمعالجة البيانات:

1.**المتحكم:** الجهة التي تتخذ القرارات حول أغراض وطرق معالجة البيانات الشخصية، والجهة المتحكمة ملزمة بالتأكد من أن أصحاب البيانات قادرون على ممارسة حقوقهم بموجب النظام.

2.**المعالج:** الكيان الذي يعالج البيانات الشخصية لمصلحة المتحكم ونيابةً عنه، فالمعالج لا يتخذ أي قرارات وانما يتلقى التوجيه من المتحكم.

على سبيل المثال:

جهة "أ" متحكم بالبيانات وشركة "ب"معالج البيانات.

جهة "أ" (المتحكم):

شركة "أ" هي شركة تأمين صحية. تتخذ القرارات بشأن جمع البيانات الشخصية لعملائها، مثل معلومات الصحة والتأمين. تحدد شركة "أ" الأغراض والطرق التي تُجمع بها البيانات الشخصية، وتضمن أن عملاءها يمكنهم ممارسة حقوقهم المتعلقة بالبيانات، مثل طلب الوصول إلى بياناتهم أو طلب حذفها. الشركة مسؤولة عن تحديد سبب وكيفية معالجة البيانات (مثل تحسين خدمات التأمين الصحية، إدارة المطالبات، إلخ) وهي ملزمة بتوفير حقوق البيانات للأفراد وفقاً للقوانين.

شركة "ب" (المعالج):

شركة "ب" هي مزود خدمة سحابية تقوم بتخزين بيانات العملاء لشركة "أ" وتقديم خدمات النسخ الاحتياطي. على الرغم من أن شركة "ب" تتعامل مع البيانات وتخزنها، إلا أنها لا تتخذ أي قرارات بشأن كيفية جمع أو استخدام البيانات. بدلاً من ذلك، تتبع شركة "ب" التوجيهات التي تقدمها شركة "أ" بشأن كيفية معالجة وتخزين البيانات. الشركة تعمل تحت إشراف شركة "أ" ولا تقرر كيف تُستخدم البيانات أو لماذا تُجمع. وظيفتها تقتصر على تنفيذ الإجراءات التقنية التي تتطلبها شركة "أ" لحفظ ومعالجة البيانات وفقاً للتوجيهات المحددة.

لذلك يجب عليك تحديد ما إذا كانت جهتك جهة تحكم أو جهة معالجة (أو كلاهما) وتطبيق المواد الواردة بالنظام اتجاه جهتك.

4.2 خطوات الامتثال الرئيسية؟

البيانات ذات قيمة استراتيجية مهمة، لذا فإن فهم الأنظمة والامتثال لها ليس خيار، بل ضرورة وخطوة أساسية للنجاح. فلذلك على الجهات القيام بالعديد من الخطوات لتحقيق الامتثال للنظام ومنها:

1. التسجيل في السجل الوطني لجهات التحكم (من خلال منصة حوكمة البيانات) في أي من الأحوال التالية:
   أ. إذا كانت جهة التحكم جهة عامة
   ب. إذا كان النشاط الرئيسي لجهة التحكم قائماً على معالجة البيانات الشخصية
   ج. إذا كانت جهة التحكم تعالج بيانات حساسة
   د. إذا كان الفرد يقوم بمعالجة البيانات الشخصية لأغراض تتجاوز الاستخدام الشخصي أو العائلي

2. بناء إطار تنظيمي قوي لضبط ومراقبة الخصوصية من خلال:
   أ. فرز وفهرسة وتصنيف البيانات الشخصية
   ب. تطوير وتنفيذ سياسات وإجراءات معالجة البيانات الشخصية بما يتوافق مع نظام حماية البيانات الشخصية
   ج. التأكد من وجود أساس مشروع وقانوني لجمع البيانات واستخدامها
   د. التأكد من جمع ومعالجة البيانات بما يتوافق مع سياسات ولوائح الخصوصية
   هـ. تضمين خصوصية البيانات في الأنظمة والعمليات والخدمات التابعة للجهة
   و. الحفاظ على أمان البيانات الشخصية من خلال اتخاذ التدابير المناسبة، وعدم الكشف عنها لأي طرف ثالث دون الحصول على موافقة من صاحب البيانات
   ز. ضمان إمكانية ممارسة أصحاب البيانات الشخصية لحقوقهم كافة بكل يسر وسهولة (مثل حق التعديل والإتلاف والوصول والرجوع عن الموافقة)

3. اعتماد سياسة للخصوصية وتكون متاحة لأصحاب البيانات الشخصية للاطلاع عليها عند جمع بياناتهم على أن تشمل السياسة العناصر التالية:
   أ. الغرض من جمع البيانات
   ب. محتوى البيانات الشخصية المطلوب جمعها
   ج. طريقة جمعها
   د. وسيلة حفظها
   هـ. كيفية معالجتها
   و. كيفية إتلافها
   ز. حقوق صاحبها فيما يتعلق بها وكيفية ممارسة هذه الحقوق (على سبيل المثال: يمكنك طلب إتلاف بياناتك الشخصية من خلال بوابة ... الخ).

وبالإمكان الاطلاع على الدليل الإسترشادي لإعداد وتطوير سياسة الخصوصية (من هنا) و تحميلنموذج سياسة الخصوصية (docx/pdf) المطور من قبل الجمعية .

4. تعيين مسؤول حماية البيانات للإشراف وضمان الامتثال لنظام حماية البيانات الشخصية داخل المنظمة وذلك في أي من الأحوال التالية:

أ. إذا كانت الجهة تقدم خدمات أو منتجات تتضمن معالجة بيانات شخصية على نطاق واسع
ب. أن تقوم الأنشطة الأساسية لجهة التحكم على عمليات المعالجة التي تتطلب بطبيعتها مراقبة منتظمة وممنهجة لأصحاب البيانات الشخصية
ج. أن تقوم الأنشطة الأساسية لجهة التحكم على معالجة بيانات حساسة

ويمكن التأكد من مدى إلزامية تعيين مسؤول حماية البيانات الشخصية من عدمه من منصة حوكمة البيانات الشخصية .والاطلاع على قواعد تعيين مسؤول حماية البيانات الشخصية.

5. خلق ثقافة خصوصية البيانات داخل المنظمة عبر:

أ. التواصل وتوعية الموظفين على جميع المستويات لفهم كيف يمكن للنظام أن يؤثر على أدوارهم في المنظمة
ب. نشر ومشاركة السياسات والإجراءات مع أصحاب المصلحة
ج. تزويد أصحاب البيانات بالمعلومات حول حقوقهم وكيفية ممارستها بموجب نظام حماية البيانات الشخصية
د. توفير ورش عمل تثقيفية ودورات تدريبية من خلال برامج مصممة وفقًا لاحتياجات المنظمة

6. إدارة المخاطر بنهج استباقي:

أ. إجراء تقييمات خصوصية البيانات لأنشطة المعالجة بشكل دوري لتحديد المخاطر المحتملة والتوصية بالتدابير المناسبة.
ب. الاستجابة لطلبات أصحاب البيانات الشخصية
ج. الإخطار للجهات المختصة في حالة حدوث خروقات للبيانات الشخصية
د. الالتزام بقواعد نقل البيانات الشخصية خارج المملكة

7. الاحتفاظ بسجل أنشطة معالجة البيانات الشخصية لمدة خمس سنوات من الانتهاء، ومشاركتها مع سدايا عند الطلب

8. تنظيم التعاقدات مع المعالجين الخارجيين لضمان تأمين حماية للبيانات الشخصية بين جميع الأطراف وفق نظام حماية البيانات الشخصية

9. مراقبة امتثال المعالجين الخارجيين حيث لا يخل وجود جهة معالجة لدى جهة التحكم بمسؤولياتها اتجاه صاحب البيانات الشخصية أو الجهة المختصة.

10. الالتزام بالقواعد المنظمة لنقل البيانات الشخصية خارج المملكة (لائحة نقل البيانات الشخصية إلى خارج المملكة).

ولمعرفة ملخص لنقاط الالتزام بقانون حماية البيانات الشخصية كما وردت في التقييم الذاتي للالتزام بنظام حماية البيانات الشخصية ولوائحه التنفيذية، يرجى الرجوع للملحق **(١).**

كيف يمكن لجمعية إدارة البيانات (داما السعودية) مساعدتكم؟

ستقوم الجمعية بطرح عدد من النماذج التي يمكن إعادة استخدامها في المكتبة الرقمية واللقاءات مع الخبراء في المجال وذلك لتمكين الجهات من تحقيق الالتزام بالنظام.

تواصل معنا على: Info@DAMASaudi.org في حال وجود أي استفسار أو في حال رغبتكم بمشاركة المعرفة حول نظام حماية البيانات الشخصية مع مجتمع الجمعية.

إعداد: إدارة البحث والابتكار – داما السعودية

آلاء السياري
دعاء العوفي
نوف الجارالله
د. عبدالعزيز المنيع

ملحق (١): فيما يلي ملخص لنقاط الالتزام بقانون حماية البيانات الشخصية كما وردت في التقييم الذاتي للالتزام بنظام حماية البيانات الشخصية ولوائحه التنفيذية:

المجال	التفاصيل	هل تم التطبيق		مستندات خاصة ذات علاقة
		نعم	لا	
1. الإجراءات التنظيمية	هل تم اعتماد خطة لحوكمة البيانات الشخصية وفقاً لنظام حماية البيانات الشخصية ولوائحه، على سبيل المثال: أدوار ومسؤوليات واضحة وحدود مرسومة لضمان الالتزام بنظام حماية البيانات الشخصية ولوائحه في الجهة، ومعالجة الحالات التي قد تكون متعارضة داخلياً؟			
2. سياسة الخصوصية	هل تم نشر سياسة الخصوصية وإتاحتها لاطلاع أصحاب البيانات الشخصية قبل أو أثناء جمع بياناتهم الشخصية؟			- الدليل الاسترشادي لإعداد وتطوير سياسة الخصوصية - نموذج سياسة الخصوصية (docx/pdf) المطور من قبل الجمعية
3. مسؤول حماية البيانات الشخصية	هل تم الأخذ بالاعتبار ما إذا كان يتطلب على الجهة تعيين مسؤول حماية البيانات الشخصية وهل تم تحديد أدواره ومسؤولياته؟			- قواعد تعيين مسؤول حماية البيانات الشخصية - أداة استرشادية للتعرف على مدى إلزامية التعيين
4. التوعية	هل تم تطوير وتدريب جميع الموظفين لضمان فهم مبادئ حماية البيانات الشخصية والمسؤوليات والمخاطر المحتملة (وفقاً لنظام حماية البيانات الشخصية ولوائحه)؟			
5. البيانات الحساسة	هل تم الأخذ بالاعتبار ما إذا كانت الجهة تعالج بيانات حساسة والتأكد من تلبية متطلبات معالجة هذا النوع من البيانات؟			
6. البيانات الصحية	هل تم الأخذ بالاعتبار ما إذا كانت الجهة تعالج أي بيانات صحية والتأكد من تلبية متطلبات معالجة هذا النوع من البيانات؟			
7. البيانات الائتمانية	هل تم الأخذ بالاعتبار ما إذا كانت الجهة تعالج أي بيانات ائتمانية والتأكد من استيفاء متطلبات معالجة هذا النوع من البيانات؟			
8. دقة البيانات الشخصية وحداثتها	هل تم إعداد سياسة أو إجراءات لضمان دقة واكتمال وحداثة البيانات الشخصية واستخدامها للغرض الذي جمعت من أجله مع استيفاء مبدأ الحد الادنى من البيانات؟			- الدليل الاسترشادي لتحديد الحد الأدنى من البيانات الشخصية
9. تقويم الأثر	هل تم وضع إجراءات لتقويم الأثر على معالجة البيانات الشخصية؟			
10. الأسس النظامية لمعالجة البيانات الشخصية	هل تمت مراجعة الأسس النظامية الحالية لمعالجة البيانات الشخصية والتأكد من أنها متوافقة ومتوائمة مع نظام حماية البيانات الشخصية (على سبيل المثال: هل بإمكانك الاعتماد على الموافقة في ضوء المتطلبات الجديدة، أو المصلحة المشروعة؟) مع توضيح الأساس النظامي للمعالجة في سياسة الخصوصية.			

11. الولي الشرعي	هل يتم التعامل مع بيانات شخصية لناقصي أو عديمي الأهلية، وهل تم الأخذ بالاعتبار ما إذا تم استيفاء جميع المتطلبات المتعلقة بالولي الشرعي؟			- سياسة حماية البيانات الشخصية للأطفال ومن في حكمهم
12. الإفصاح عن البيانات الشخصية	هل تم وضع إجراءات للإفصاح عن البيانات الشخصية لأي طرف آخر؟			- الدليل الاسترشادي لحالات الإفصاح عن البيانات الشخصية
13. حقوق أصحاب البيانات الشخصية	هل تم وضع آلية لتنفيذ طلبات أصحاب البيانات الشخصية المتعلقة بممارسة حقوقهم المنصوص عليها في نظام حماية البيانات الشخصية ولوائحه؟			
14. تسرب البيانات الشخصية	هل تم وضع إجراءات داخلية للإبلاغ عن حوادث تسرب البيانات الشخصية، ويشمل ذلك ضوابط الإشعار الإلزامية للجهة المختصة وصاحب البيانات الشخصية؟			
15. التدابير التقنية	هل تم وضع التدابير التقنية المناسبة، بما في ذلك النسخ الاحتياطية والتشفير والاختبارات التجريبية المنتظمة لضمان الحماية التقنية والفنية للبيانات الشخصية؟			
16. نقل البيانات الشخصية	هل تم وضع إجراءات تنظم عملية نقل البيانات الشخصية خارج المملكة؟			-لائحة نقل البيانات الشخصية إلى خارج المملكة - دليل إعداد القواعد المشتركة الملزمة لنقل البيانات الشخصية - البنود التعاقدية القياسية لنقل البيانات الشخصية
17. الأغراض الدعائية / التوعوية / التسويق المباشر	هل تم استيفاء متطلبات عملية معالجة البيانات الشخصية لأغراض دعائية أو توعوية أو لأغراض التسويق المباشر؟			
18. تصوير الوثائق الرسمية	هل تم وضع إجراءات لتجنب تصوير الوثائق الرسمية أو نسخها؟			
19. سجلات أنشطة معالجة البيانات الشخصية	هل تم حصر جميع أنشطة معالجة البيانات الشخصية لتضمينها بسجل مفصل يبين أنشطة معالجة البيانات؟ (على سبيل المثال: توثيق أنوع البيانات الشخصية التي تحتفظ بها الجهة، ومصدر جمعها، ومع من تتم مشاركتها)			- الدليل الاسترشادي لسجلات أنشطة معالجة البيانات - نموذج سجل أنشطة معالجة البيانات الشخصية (xlsx) المطور من قبل الجمعية.
20. المتابعة	هل تم القيام بأعمال التدقيق والمراجعة الداخلية وتوثيق ذلك للتأكد من فعالية تطبيق السياسات والضوابط والإجراءات المتعلقة بحماية البيانات الشخصية؟			

المراجع

- نظام حماية البيانات الشخصية.
- اللائحة التنفيذية لنظام حماية البيانات الشخصية.
- دليل نظام حماية البيانات الشخصية.
- دليل نظام حماية البيانات الشخصية لجهات التحكم والمعالجة.
- الدليل الاسترشادي لتحديد الحد الأدنى من البيانات الشخصية.
- قواعد تعيين مسؤول حماية البيانات الشخصية.

إخلاء مسؤولية: هذا المستند يعتبر دليل استرشادي اجتهادي لتوضيح قانون حماية البيانات الشخصية للأفراد والجهات وقد تم الاعتماد بشكل أساسي على قانون حماية البيانات الشخصية الصادر في المملكة العربية السعودية والاستزادة ببعض النقاط التوضيحية من مصادر علمية في المجال وأنظمة أخرى مشابهة كاللائحة العامة لحماية البيانات في الإتحاد الأوروبي. وتعد الهيئة السعودية للبيانات والذكاء الاصطناعي هي الجهة المختصة والمشرعة كما أوضح النظام والتي يجب الاعتماد على الأنظمة والأدلة الصادرة منها.

DAMA SAUDI

جمعية إدارة البيانات (داما السعودية)