SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

دليل نظام حماية البيانات الشخصية
لجهات التحكم والمعالجة

الإصدار 1.0

ديسمبر 2023م

الفهرس

3 المقدمة

- الغرض 3
- الهدف 3

4 حماية البيانات الشخصية في المملكة

- نطاق النظام 4
- النطاق الموضوعي: ما هو نطاق النظام؟ 5
- ما المقصود بالبيانات الشخصية؟ 5
- كيف يمكن تحديد هوية الفرد؟ 6
- ما المقصود بالبيانات الحساسة؟ 7
- ماهي الأحكام الخاصة بمعالجة البيانات الحساسة؟ 8
- ما هي أشكال معالجة البيانات الشخصية؟ 8
- ما هي مصادر البيانات الشخصية؟ 9
- هل تعد الآراء والاستنتاجات من البيانات الشخصية؟ 9
- معالجة بيانات المتوفى 10
- هل تعد البيانات التي خضعت للترميز بيانات شخصية؟ 10
- هل تعد البيانات التي خضعت لإخفاء الهوية من البيانات الشخصية؟ 12
- ما هو المقصود بمعالجة البيانات الشخصية؟ 12

14 النطاق المكاني: أين تسري أحكام النظام؟

- الحالة (1): ما الذي يُعتبر معالجة للبيانات داخل المملكة؟ 14
- الحالة (2): من هم الأفراد المقيمون في المملكة؟ 15
- الحالة (3): ما المقصود بـ «جهة خارج المملكة»؟ 15

17 ما هو الدور الذي تؤديه جهات التحكم وجهات المعالجة بموجب النظام؟

18 متى لا تسري أحكام النظام؟

- ما المقصود بالاستخدام الشخصي أو العائلي؟ 18

19 متى يدخل النظام حيز التنفيذ؟

- ما الذي ينبغي فعله خلال الفترة التصحيحية؟ 19

20 من هي الجهة المختصة؟

20 حقوق الأفراد

21 مبادئ حماية البيانات الشخصية

22 الملحق (1) أمثلة للممارسات المخالفة للنظام عند التعامل مع البيانات الشخصية

SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

المقدمة

الغرض

يتمثل الغرض من هذه الوثيقة (الدليل الإرشادي) التعريف بنظام حماية البيانات الشخصية (النظام) في المملكة العربية السعودية (المملكة)، الذي تمت الموافقة عليه بموجب المرسوم الملكي رقم م/ 19 وتاريخ 1443/2/9 وشرح كيفية تطبيقه.

الهدف

يهدف هذا الدليل الإرشادي إلى توضيح أحكام النظام وتقديم إرشادات للأفراد والجهات لمساعدتهم على الالتزام بأحكامه، ولا يتضمن هذا الدليل الإرشادي أي قواعد ملزمة أو التزامات، ولا يعد هذا الدليل بديلاً عن أي أنظمة أو تشريعات في المملكة.

حماية البيانات الشخصية في المملكة

أحد أهم الركائز للمملكة التي تقوم عليها رؤية 2030 إنشاء اقتصاد رقمي مزدهر، وتمثل البيانات الأساس الذي يُبنى عليه الاقتصاد الرقمي الحديث؛ لذلك يجب تنظيم استخدام البيانات الشخصية في المملكة بما يضمن خصوصية الأفراد.

يتضمن الإطار التنظيمي لحماية البيانات الشخصية في المملكة ما يلي:

1. نظام حماية البيانات الشخصية.
2. اللوائح التنفيذية للنظام بما في ذلك اللائحة التنفيذية للنظام ولائحة نقل البيانات الشخصية خارج المملكة.
3. اللوائح والمعايير والسياسات والوثائق النظامية الأخرى المتعلقة بحماية البيانات الشخصية الصادرة من الهيئة السعودية للبيانات والذكاء الاصطناعي (الهيئة، سدايا).
4. المعاهدات الدولية الخاصة بالمملكة حول حماية البيانات الشخصية.

يعد نظام حماية البيانات الشخصية النظام الرئيسي لحماية البيانات الشخصية في المملكة، وبناءً عليه عند استخدام أي بيانات شخصية يجب الالتزام به، باستثناء الحالات المحدودة عند وجود وثيقة نظامية رسمية تصدر من السلطات المختصة تنص على غير ذلك.

لمزيد من المعلومات عن الجهة المختصة لحماية البيانات الشخصية، يُرجى الاطلاع على قسم (من هي الجهة المختصة) من هذا الدليل الإرشادي.

نطاق النظام

يتضمن التالي:

المادة (الثانية) من النظام

1. يُطبق النظام على أي عملية مُعالجة لبيانات شخصية تتعلق بالأفراد تتم في المملكة بأي وسيلة كانت، بما في ذلك معالجة البيانات الشخصية المتعلقة بالأفراد المقيمين في المملكة بأي وسيلة كانت من أي جهة خارج المملكة، ويشمل ذلك بيانات المتوفى إذا كانت ستؤدي إلى معرفته أو معرفة أحد أفراد أسرته على وجه التحديد.
2. يُستثنى من نطاق تطبيق النظام قيام الفرد بمعالجة البيانات الشخصية لأغراض لا تتجاوز الاستخدام الشخصي أو العائلي، ما دام أنه لم ينشرها أو يفصح عنها للغير، وتحدد اللوائح التنفيذية للنظام المقصود بالاستخدام الشخصي والعائلي المنصوص عليهما في هذه الفقرة.

النطاق الموضوعي: ما هو نطاق النظام؟

يشمل تنظيم معالجة البيانات الشخصية التالي:

1. البيانات الشخصية من أي نوع بما في ذلك البيانات الحساسة.
2. البيانات الشخصية مهما كان مصدرها أو شكلها.
3. البيانات التي خضعت للترميز.
4. بيانات المتوفى (في حالات محدودة).

ما المقصود بالبيانات الشخصية؟

يُعرف النظام البيانات الشخصية بأنها:

الفقرة (4) من المادة (الأولى) في النظام

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

يُقصد من ذلك أن البيانات الشخصية هي أي بيانات يمكن من خلالها تحديد الفرد مثلاً: رقم الهاتف الشخصي للفرد أو اسمه أو عنوان بريده الإلكتروني.

إذا تعذر تحديد هوية الفرد من البيانات، فإن هذه البيانات لا تعد من البيانات الشخصية ولن يخضع استخدامها للنظام.

مثال | البيانات الشخصية

تقوم إدارة الموارد البشرية لشركة بتخزين بيانات الموظفين بما في ذلك الاسم، وتاريخ الميلاد، والدرجة الوظيفية، ورقم الهاتف الشخصي، والمؤهلات التعليمية، وتُعد هذه البيانات التي تخزنها إدارة الموارد البشرية بيانات شخصية ويخضع استخدامها للنظام.

مثال | البيانات غير الشخصية

تحلل إدارة التسويق في الشركة سلوك الشراء الخاص بعملائها الذين تتراوح أعمارهم بين 30-20 عاماً، وتتعامل إدارة التسويق فقط مع بيانات إحصائية عن المنتجات التي تشتريها هذه الفئة العمرية، ولن تتمكن إدارة التسويق من تحديد هوية المشتري.

ولذلك لا تعد هذه البيانات بيانات شخصية ولا يخضع استخدامها للنظام.

مثال | البيانات غير الشخصية

تمتلك إحدى شركات السيارات قاعدة بيانات عن الموزعين المعتمدين لديها (الجهات التجارية)، وتتضمن قاعدة البيانات بيانات عن عدد السيارات التي باعها كل موزع خلال العام الحالي، وتتضمن كذلك أسعار شراء الموزعين للسيارات بغرض بيعها.

لا تعد البيانات عن حجم المبيعات وسعر السيارات بيانات شخصية ولا يخضع استخدامها للنظام

كيف يمكن تحديد هوية الفرد؟

يمكن تحديد هوية الفرد:

1. بشكل **مباشر**: من خلال البيانات التي تُجرى معالجتها، مثل: المعرفات المميزة بما في ذلك رقم الهاتف الشخصي أو الاسم أو عنوان البريد الإلكتروني الشخصي، وتخضع معالجة هذه البيانات للنظام.
2. بشكل **غير مباشر**: عن طريق ربط قواعد بيانات مختلفة ببعضها مما قد ينتج عنه بيانات تحدد هوية الفرد، وعليه تعد هذه البيانات بيانات شخصية تخضع للنظام، لكن إن لم ينتج عن عملية الربط بين البيانات تحديد هوية الفرد فلا تعد هذه البيانات بيانات شخصية ولا تخضع لأحكام النظام.

يُرجى العلم أنه يلزم النظر في كل حالة على حدة لمعرفة إذا كان من الممكن التعرف على هوية الفرد.

مثال | البيانات الشخصية | تحديد هوية الفرد بشكل مباشر

يعمل متجر بيع بالتجزئة على جمع أرقام الهواتف الخاصة بكل عميل قبل بيع المنتجات له بغرض إرسال رسائل ترويجية عن عروض جديدة إلى العملاء، ولكنه لا يجمع أسماء عملائه.

ترتبط أرقام الهواتف بأسماء العملاء في قاعدة بيانات شركات الاتصالات؛ لذلك يمكن اعتبار أرقام الهواتف من البيانات الشخصية بالنسبة إلى شركات الاتصالات.

ستعد أرقام الهواتف من البيانات الشخصية أيضاً بالنسبة إلى المتجر حتى إن لم يكن مخولاً له الوصول إلى قاعدة البيانات الخاصة بشركات الاتصالات وذلك لأن كل رقم هاتف يُخصص لفرد بعينه، ويمكن للمتجر أن يميز الفرد عن العملاء الآخرين من رقم هاتفه ويستخدم هذا الرقم في التواصل معه وتوجيه عروض البيع له وحده.

لذلك سيحتاج كل من المتجر وشركات الاتصالات إلى حماية أرقام الهواتف وفقاً للنظام.

مثال | البيانات الشخصية | تحديد هوية الفرد بشكل غير مباشر

تخزن إدارة الأمن في الشركة التالية في أنظمة منفصلة:

قاعدة البيانات رقم (1): تتضمن هذه القاعدة الأسماء، وأرقام الهواتف، وأرقام الموظفين، التي تُستخدم لأغراض تحديد الهوية، وإدارة الرواتب.

قاعدة البيانات رقم (2): تتضمن هذه القاعدة بيانات عن السيارات التي تدخل إلى مقرات الشركة وتخرج منها، وتُستخدم هذه البيانات في توجيه إنذار عن مخالفات الوقوف.

مثال | البيانات الشخصية | تحديد هوية الفرد بشكل غير مباشر

في هذه الحالة، تُخزن **قاعدة البيانات رقم (1)** البيانات التي يمكن من خلالها تحديد هوية الفرد بشكل مباشر؛ لذلك تحتوي على بيانات شخصية.

ولا يُخزن في **قاعدة البيانات رقم (2)** بيانات يمكن من خلالها تحديد هوية الفرد بشكل مباشر، لكن يمكن للشركة الربط بين **قاعدة البيانات رقم (1) وقاعدة البيانات رقم (2)** معاً لتحديد هوية مالك السيارة، لذلك ستُعد البيانات في **قاعدة البيانات رقم (2)** من البيانات الشخصية وسيخضع استخدامها للنظام أيضاً.

مثال | البيانات الشخصية | يتعذر تحديد هوية الفرد منها

اتخذت إحدى الصيدليات قراراً بتحليل بياناتها التجارية عن العام الماضي، قبل إجراء هذا التحليل قامت بحذف البيانات من سجل المشتريات التي يمكن ربطها بالعملاء بما في ذلك أرقام الهواتف، وأرقام البطاقات المصرفية، وبعد حذف هذه البيانات، لم يكن لدى الصيدلية سوى البيانات التالية:

1. اسم المنتج ونوعه.
2. البيانات الخاصة بالمنتجات التي تم بيعها خلال العام الماضي.
3. سعر المنتج.

لا تعد هذه البيانات بيانات شخصية ولا يخضع استخدامها للنظام.

ما المقصود بالبيانات الحساسة؟

يحدد النظام نوعاً خاصاً من البيانات وهي (البيانات الحساسة) ويتطلب هذا النوع من البيانات فرض مزيد من الإجراءات الوقائية وإجراءات الحماية إذ إن الوصول غير المصرح به لهذه البيانات قد يسفر عنه إلحاق ضرر جسيم بالفرد.

تتضمن البيانات الحساسة ما يلي:

1. البيانات الشخصية التي تكشف عن أصل الفرد العرقي أو أصله الإثني (مثلاً لون بشرة الفرد، إلخ).
2. البيانات الشخصية التي تكشف عن معتقد الفرد الديني أو الفكري أو السياسي.
3. البيانات الشخصية التي تشير إلى الجرائم الجنائية أو الأمنية السابقة التي ارتكبها الفرد.
4. بيانات السمات الحيوية الخاصة بالفرد (التي تحدد الهوية).
5. بيانات الفرد الوراثية.
6. البيانات الشخصية المتعلقة بصحة الفرد.
7. البيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهما.

ماهي الأحكام الخاصة بمعالجة البيانات الحساسة؟

عند معالجة البيانات الحساسة، يجب الالتزام بجميع المتطلبات المنصوص عليها في النظام التي تسري على معالجة أي بيانات شخصية أخرى. وإضافة إلى ذلك ينص النظام على متطلبات خاصة تتعلق بمعالجة البيانات الحساسة، على سبيل المثال لا الحصر:

1. لا يعتد بالمصلحة المشروعة كمسوغ نظامي لمعالجة البيانات الحساسة المنصوص عليها في الفقرة 4 من المادة السادسة من النظام.
2. في حالة وجود الموافقة من قبل صاحب البيانات الشخصية كمسوغ نظامي لمعالجة البيانات الحساسة، فيجب أن تكون الموافقة صريحة وفقاً للمادة الحادية عشرة من اللائحة التنفيذية للنظام.
3. في جميع الأحوال، لا يجوز معالجة البيانات الحساسة لأغراض تسويقية حتى وإن تم الحصول على موافقة الفرد وذلك وفقاً للمادة السادسة والعشرين من النظام.
4. ينص النظام على قيود استخدام البيانات الحساسة لأغراض علمية أو بحثية أو إحصائية وفقاً للمادة السابعة والعشرين من النظام.

ما هي أشكال معالجة البيانات الشخصية؟

ينطبق النظام على معالجة البيانات الشخصية بجميع أشكالها.

البيانات الشخصية في شكل غير إلكتروني (مثل: البيانات الشخصية المتضمنة في وثيقة ورقية ملموسة مثلاً) تخضع أيضاً لأحكام النظام.

من الناحية العملية ونظراً إلى مدى التطور التكنولوجي في المملكة، فإن معظم البيانات الشخصية تتم معالجتها بشكل إلكتروني.

مثال | البيانات الشخصية | البيانات الشخصية في شكل إلكتروني

تخزن إدارة الموارد البشرية البيانات الشخصية عن الموظفين في أنظمة التخزين السحابية، إذاً تكون هذه البيانات الشخصية في شكل إلكتروني ويخضع استخدامها للنظام.

مثال | البيانات الشخصية | البيانات الشخصية في شكل غير إلكتروني

تخزن الجامعة أوراق اختبارات طلابها، وتتضمن أوراق الاختبار بيانات الطلاب الشخصية (على سبيل المثال: الأسماء الكاملة، والأرقام الجامعية للطلاب)، إذاً تكون هذه البيانات الشخصية في شكل غير إلكتروني ويخضع استخدامها للنظام.

تسري أحكام النظام على معالجة البيانات الشخصية بغض النظر عن حجمها أو نوعها، بالإضافة إلى أن النظام لا يفرق بين الأشكال التي تتخذها البيانات الشخصية سواء كانت بيانات منظمة (مثلاً بيانات مخزنة في قاعدة البيانات)، أو غير منظمة (مثلاً بيانات شخصية في وثائق مختلفة)، وما إلى ذلك طالما أنه يمكن التعرف على هوية الفرد باستخدام هذه البيانات فتُعد هذه البيانات بيانات شخصية ويخضع استخدامها للنظام.

ما هي مصادر البيانات الشخصية؟

يمكن الحصول على البيانات الشخصية من مصادر عديدة إما مباشرة من الفرد ذاته أو من جهات أخرى مثلاً من مصادر عامة (من قواعد البيانات الموجودة في الإنترنت والمتاحة للعموم)، يحدد النظام في المادة العاشرة شروطاً معينة للحصول على البيانات الشخصية من وسائل أخرى غير مقدمة من صاحبها مباشرة.

هل تعد الآراء والاستنتاجات من البيانات الشخصية؟

يمكن أن تعتبر الآراء والاستنتاجات الخاصة بالأفراد بيانات شخصية في حال كان من الممكن تحديد هوية الفرد باستخدام هذه الآراء أو الاستنتاجات سواء بشكل مباشر أو غير مباشر، عندئذ إذا نسبت إحدى الجهات الآراء أو الاستنتاجات إلى فرد معين، فهي تعتبر من البيانات الشخصية بغض النظر عن مدى صحتها.

مثال | البيانات الشخصية | الآراء

تجري إدارة الموارد البشرية استطلاعاً لمعرفة مدى رضا الموظفين عن بيئة العمل، واستناداً إلى هذا الاستطلاع، تعد الإدارة تقريراً عن كيفية تحسين بيئة العمل، في هذه الحالة تعد آراء الموظفين بيانات شخصية.

مثال | البيانات الشخصية | الاستنتاجات

تحتفظ الصيدلية ببياناتها في قاعدة البيانات الخاصة بها وتتضمن بيانات المشتريات الخاصة بعملائها، وتربط قاعدة البيانات العملاء بالأدوية التي يشترونها وبناء على بيانات سجل المشتريات، تستنتج الصيدلية الحالة الصحية لعملائها.

تُعد الاستنتاجات التي تتوصل إليها الصيدلية عن الحالة الصحية لعملائها من البيانات الشخصية، فضلاً عن أنها بيانات حساسة حتى إن لم يُقدم بعض العملاء على شراء الأدوية لأنفسهم (على سبيل المثال: يشترون هذه الأدوية لأقاربهم).

ملاحظة: في هذا المثال تتضمن قاعدة بيانات العملاء هذه سجل المشتريات الخاص بالأفراد ولا تستطيع الصيدلية التفريق بين مشتريات العملاء التي يشترونها لأنفسهم أو للآخرين.

معالجة بيانات المتوفى

وفقاً للفقرة (1) من المادة (الثانية) من النظام

يُطبق النظام على معالجة بيانات المتوفى إذا كانت ستؤدي إلى معرفته أو معرفة أحد أفراد أسرته على وجه التحديد.

لا يُقصد من هذا الحكم من النظام أن استخدام بيانات المتوفى يخضع دائماً للمتطلبات التي تنطبق على استخدام البيانات الشخصية الخاصة بالفرد الحي، بل يُقصد منه أنه إذا كان من شأن بيانات المتوفى إلحاق الضرر بأحد أعضاء أسرته الذين هم على قيد الحياة (مثل: الضرر بسمعته)، عندئذ يلزم حماية بيانات المتوفى بالأسلوب ذاته المتبع لحماية البيانات الشخصية الخاصة بالفرد الحي.

ويجب أن يؤخذ في الاعتبار كل حالة معينة على حدى لتحديد متطلبات النظام التي يجب أن تنطبق على بيانات الفرد المتوفى.

مثال | البيانات الشخصية | بيانات المتوفى

تقدم إحدى الشركات خدمات البحث عن التاريخ العائلي للفرد، وعند إجراء هذا البحث، تمكنت الشركة من معرفة أن والد الفرد المتوفى كان يعاني من مرض معدٍ خطير، وقد أوضح الفرد الذي طلب إجراء هذا البحث أن هذه البيانات قد تلحق الضرر بسمعته، وأبلغ الشركة التي تجري البحث بهذا الأمر وأوضح لهم أسباب ذلك.
في هذه الحالة تلتزم الشركة التي تجري البحث بحماية بيانات الأب المتوفى متبعة الأسلوب ذاته كما لو كانت بيانات شخصية تخص فرداً على قيد الحياة.

هل تعد البيانات التي خضعت للترميز بيانات شخصية؟

تنص اللائحة التنفيذية للنظام على تعريف (الترميز):

الفقرة (7) من المادة (الأولى) من اللائحة التنفيذية للنظام

تحويل المعرفات الرئيسية التي تدل على هوية صاحب البيانات الشخصية إلى رموز تجعل من المتعذر تحديد هوية صاحب البيانات الشخصية بشكل مباشر دون استخدام بيانات أو معلومات إضافية، وأن يتم الاحتفاظ بتلك البيانات أو المعلومات الإضافية بشكل منفصل ووضع الضوابط الفنية والإدارية اللازمة لضمان عدم ربطها بصاحب البيانات بالشكل المحدد.

يُستخدم الترميز (إيجاد الأسماء المستعارة) لاستبدال البيانات التي تحدد هوية الفرد بشكل مباشر، وتظل البيانات التي خضعت للترميز من البيانات الشخصية ويمكن اعتبار الترميز إجراءً أمنياً فعالاً لحماية البيانات، ويتضمن الترميز إخفاء البيانات التي تحدد الهوية، على سبيل المثال: من خلال استبدال البيانات التي تحدد الهوية بشكل مباشر (مثل الأسماء) بمعرف فريد، ولا يمكن أن يرتبط هذا المعرف بفرد معين دون استخدام بيانات إضافية.

يعد الترميز من الإجراءات التي تُتخذ بغرض تعزيز حماية البيانات الشخصية وأمنها، ويمكن أن يساعد في الحد من المخاطر، كما أنه يُستخدم في عديد من المجالات، على سبيل المثال لا الحصر: التجارب السريرية، والأبحاث الطبية، والقطاع المالي، وما إلى ذلك.

مثال | الترميز | الخدمات المصرفية

يرغب أحد المصارف في تقديم عروض خاصة إلى عملائه، وتعتمد هذه العروض على حجم المعاملات التي يجريها العملاء.

واتخذ المصرف الخطوات التالية:

1. فصل أسماء عملائه عن معاملاتهم في قاعدتي بيانات منفصلتين:
   - تتضمن قاعدة البيانات الأولى أسماء العملاء.
   - وتتضمن قاعدة البيانات الثانية حجم معاملاتهم.
   - استبدل المصرف أسماء العملاء برموز في قاعدة البيانات الثانية.
2. قُدمت القاعدتان إلى فريقين منفصلين في المصرف لإجراء التحليل.
3. أعد كل فريق لقاعدة البيانات الخاصة به كلمة مرور حيث لا يستطيع أي من الفريقين الوصول إلى قاعدة الفريق الآخر.
4. وبهذا قام المصرف بإجراء الترميز لبيانات عملائه.

وفي هذه الحالة تعد البيانات عن حجم المعاملات من البيانات الشخصية، وذلك للأسباب التالية:

- من الممكن ربط حجم المعاملات بعملاء معينين عند جمع قاعدتي البيانات معاً.
- احتفظ المصرف ذاته بقاعدتي البيانات وهناك احتمالية لجمع قاعدتي البيانات معاً إذا ما اقتضى الأمر ذلك.

مثال | الترميز | قطاع التربية والتعليم

تحتفظ الجامعة بقاعدة بيانات تتضمن بيانات طلابها وحددت لكل طالب رقماً خاصاً به.

عند إجراء الاختبارات، يجب على كل طالب أن يذكر في أوراق الاختبار الرقم الخاص به فقط، لذا عندما تطلع لجنة الاختبارات على أوراق الاختبار لن ترى سوى رقم كل طالب، وسيتعذر عليها معرفة اسم الطالب الذي أجرى الاختبار، وعلاوة على ذلك لا يحق للجنة الاختبارات الوصول إلى قاعدة البيانات التي تتضمن أرقام الطلاب وأسماءهم. وبناءً عليه، فقد حرصت الجامعة في هذه الحالة على ترميز أسماء الطلاب، وستعد أرقام الطلاب من البيانات الشخصية لأنه يمكن للجامعة أن تربط بين أرقام الطلاب في قاعدة البيانات بأسمائهم.

هل تعد البيانات التي خضعت لإخفاء الهوية من البيانات الشخصية؟

الفقرة (8) من المادة (الأولى) من اللائحة التنفيذية للنظام

إزالة المعرفات المباشرة وغير المباشرة التي تدل على هوية صاحب البيانات الشخصية بشكل نهائي يتعذر معه تحديد هوية صاحب البيانات الشخصية.

تنص اللوائح على تعريف (إخفاء الهوية):

يُقصد من إجراء إخفاء الهوية إزالة أي بيانات تدل على هوية صاحب البيانات الشخصية من قاعدة البيانات حيث يتعذر تحديد هويته بأي وسيلة، لذا لا تعد البيانات التي خضعت لإخفاء الهوية من البيانات الشخصية ولن استخدامها للنظام، وبناءً عليه:

1. لا تخضع البيانات الشخصية التي تم إخفاء هوية أصحابها للنظام.
2. لا يمكن للأفراد ممارسة الحقوق المنصوص عليها في النظام فيما يتعلق باستخدام بياناتهم الشخصية التي خضعت لإخفاء الهوية.

عندما يتم إخفاء الهوية بشكل صحيح، سيحد ذلك من المخاطر المتعلقة بحماية البيانات الشخصية لأنه يتعذر في هذه الحالة التعرف على الفرد بشكل مباشر أو غير مباشر، وتحدد المادة التاسعة من اللائحة التنفيذية للنظام شروطاً معينة لعملية إخفاء هوية البيانات الشخصية.

ومع ذلك يُرجى العلم أن إجراء إخفاء هوية البيانات الشخصية لا يزال ضمن إجراءات معالجة البيانات الشخصية؛ لذلك تخضع هذه العملية لأحكام النظام.

ما هو المقصود بمعالجة البيانات الشخصية؟

يحدد النظام التعريف التالي لمعالجة البيانات الشخصية.

الفقرة (5) من المادة (الأولى) من النظام

أي عملية تجرى على البيانات الشخصية بأي وسيلة كانت يدوية أو آلية، ومن ذلك: عمليات الجمع، والتسجيل، والحفظ، والفهرسة، والترتيب، والتنسيق، والتخزين، والتعديل، والتحديث، والدمج، والاسترجاع، والاستعمال، والإفصاح، والنقل، والنشر، والمشاركة في البيانات، أو الربط البيني، والحجب، والمسح، والإتلاف.

تتضمن المعالجة اتخاذ أي إجراء يتعلق بالبيانات الشخصية، فعلى سبيل المثال: الاحتفاظ بالبيانات الشخصية فقط (تخزينها) يعد من إجراءات المعالجة حتى وإن لم يُتخذ أي إجراء آخر بشأنها.

ويُقصد من ذلك أن أي استخدام للبيانات الشخصية يعد بمثابة معالجة لها ويخضع للنظام.

مثال | معالجة البيانات الشخصية | جمع البيانات الشخصية

يطلب متجر إلكتروني من عملائه التسجيل في موقعه من أجل شراء المنتجات، ويلزم العملاء بتقديم: الاسم، وعنوان البريد الإلكتروني، وبيانات الدخول للحساب الشخصي، وكلمة المرور، بالإضافة إلى عنوان التسليم.
عندما يدخل العميل البيانات الشخصية أعلاه في الموقع، فإن المتجر الإلكتروني يعمل على جمع هذه البيانات الشخصية وذلك بمثابة معالجة للبيانات الشخصية وتخضع هذه المعالجة للنظام.

مثال | معالجة البيانات الشخصية | تخزين البيانات الشخصية

تمتلك شركة التصنيع قاعدة بيانات كبيرة التي تتضمن البيانات الشخصية عن الموظفين مثل: (أسمائهم، وبيانات التواصل معهم، ومؤهلاتهم التعليمية)، ولقد تعاقدت الشركة مع مقدم الخدمات السحابية لتخزين قاعدة البيانات للموظفين سحابياً.
يُعد تخزين هذه البيانات الشخصية سحابياً من إجراءات معالجة البيانات الشخصية ويخضع للنظام.

يجب التأكد من إجراء المعالجة بأسلوب عادل، وقانوني وبما يتوافق مع مبادئ النظام، ولمزيد من المعلومات عن مبادئ النظام، يُرجى الاطلاع على قسم (مبادئ حماية البيانات الشخصية) من هذا الدليل الإرشادي.

النطاق المكاني: أين تسري أحكام النظام؟

يُقصد بالنطاق المكاني المنطقة الجغرافية التي تسري عليها أحكام النظام، ويتضمن النطاق المكاني للنظام معالجة البيانات الشخصية ضمن حالتين:

الحالة (1): معالجة البيانات الشخصية داخل المملكة.

الحالة (2): معالجة البيانات الشخصية الخاصة بالأفراد المقيمين في المملكة من قبل أي جهة بما في ذلك الجهات خارج المملكة.

الحالة (1): ما الذي يُعتبر معالجة للبيانات داخل المملكة؟

تسري أحكام النظام على معالجة البيانات الشخصية في جميع الأراضي التي تخضع لسلطة المملكة بما في ذلك المنطقة الجغرافية للمملكة وسفاراتها في الولايات القضائية الأجنبية، وتندرج ضمن نطاق النظام أي جهة تقوم بمعالجة البيانات الشخصية مثل الجهات العامة أو الخاصة أو الأشخاص ذوي الصفة الطبيعية أو الاعتبارية داخل الولاية القضائية للمملكة.

مثال | النطاق المكاني | المعالجة داخل المملكة | جهة خاصة

يقوم مستشفى داخل المملكة بمعالجة البيانات الشخصية الخاصة بموظفيه ومرضاه.

تتم جميع إجراءات المعالجة داخل المملكة، وتتضمن معالجة بيانات المرضى الشخصية الذين يرتادون هذا المستشفى من أجل العلاج من دول أخرى؛ لذلك يجب على المستشفى الالتزام بأحكام النظام.

مثال | النطاق المكاني | المعالجة داخل المملكة | جهة عامة

تقوم وزارة التعليم في المملكة بمعالجة البيانات الشخصية الخاصة بموظفيها، والأطفال الذين يرتادون المدارس، والمعلمين في المملكة، وتندرج إجراءات المعالجة التي تجريها الوزارة في المملكة ضمن نطاق النظام.

الحالة (2): من هم الأفراد المقيمون في المملكة؟

لا يقتصر تعريف الأشخاص المقيمين في المملكة على جنسية الفرد أو وضع إقامته، بل تسري أحكام النظام على معالجة البيانات الشخصية الخاصة بجميع الأفراد المقيمين في المملكة أياً كانت جنسيتهم أو مدة إقامتهم، ومن هؤلاء الأشخاص، على سبيل المثال لا الحصر:

1. مواطني المملكة.
2. المقيمين بالمملكة مثل العمال المؤقتين والدائمين.
3. الزوار المؤقتين بما في ذلك السياح والزوار لأي سبب.
4. أي فرد آخر مقيم في المملكة لأي سبب ولأي مدة زمنية، بغض النظر عن الأساس النظامي للإقامة.

يُرجى العلم أنه حتى إذا غادر الفرد المملكة، ستكون بياناته الشخصية خاضعة للنظام إذا ما زالت بياناته مخزنة في المملكة.

مثال | النطاق المكاني | الإقامة في المملكة لأغراض العمل

تمارس إحدى الشركات التجارية نشاطها في المملكة، ويعمل معظم موظفيها في مكتبها بمدينة الرياض بطريقة دائمة، وتخضع معالجة بياناتهم الشخصية للنظام.

بينما يعمل بعض موظفيها في مكتبها بمدينة دبي ويزورون مكتب الرياض مرة في الشهر.

تخضع معالجة البيانات الشخصية للموظفين العاملين في مكتب دبي للنظام عند إقامتهم في مدينة الرياض.

مثال | النطاق المكاني | زيارة المملكة من أجل السياحة

قدمت عائلة من اليابان إلى المملكة لأغراض السياحة، وتقيم هذه العائلة في أحد الفنادق بمدينة الرياض، ويسجل الفندق بياناتها الشخصية بما في ذلك الأسماء، وأرقام الهواتف، وأرقام البطاقات المصرفية، وعناوين البريد الإلكتروني، كما أنه يخزن بياناتها الشخصية لشهور عديدة بعد عودتها إلى اليابان، وتخضع البيانات الشخصية الخاصة بأفراد العائلة اليابانية للحماية بموجب النظام طوال فترة تخزين الفندق بالرياض لهذه البيانات حتى إن لم تعد العائلة مقيمة في المملكة.

الحالة (3): ما المقصود بـ «جهة خارج المملكة»؟

أي جهة مثل الجهات العامة أو الخاصة أو الأشخاص ذوي الصفة الطبيعية أو الاعتبارية مهمتهم القيام بمعالجة البيانات الشخصية الخاصة بالأفراد (المقيمين في المملكة) حيث إن عمليات المعالجة التي تقوم بها هذه الجهات تخضع للنظام حتى إذا تمت المعالجة خارج الولاية القضائية للمملكة.

مثال | النطاق المكاني | الجهات خارج المملكة

1. تقدم إحدى الشركات الاستشارية في ألمانيا الخدمات إلى عملائها المقيمين في مدينة جدة، وتتضمن هذه الخدمات معالجة البيانات الشخصية الخاصة بالموظفين العاملين لدى عملائها لأغراض تحسين العمل، وتقع معالجة البيانات هذه ضمن نطاق النظام ويجب على الشركة الاستشارية الالتزام بأحكام النظام على الرغم من أنها ليست جهة في المملكة.

2. يمارس متجر إلكتروني نشاطه في المملكة، ويعد عملاء المتجر أفراداً يقطنون في المملكة ويعملون فيها، ويستخدم المتجر الإلكتروني الحلول السحابية لتخزين البيانات الشخصية الخاصة بعملائه، وتستضيف شركة تكنولوجيا أمريكية في الولايات المتحدة الأمريكية الحل السحابي.

يخضع جميع الأفراد، في **الحالة (1)** و**الحالة (2)**، بغض النظر عن جنسيتهم أو وضع إقامتهم، للحماية بموجب النظام.

ما هو الدور الذي تؤديه جهات التحكم وجهات المعالجة بموجب النظام؟

يتضمن النظام دورين أساسيين في معالجة البيانات: دور جهة التحكم ودور جهة المعالجة.

ويقع على عاتق كل منهما مستويات مختلفة من المسؤولية فيما يتعلق بالمعالجة، ونص النظام على تعريفهما كما يلي:

الفقرة (18) من المادة (الأولى) من النظام

جهة التحكم: أي جهة عامة، وأي شخصية ذات صفة طبيعية أو اعتبارية خاصة؛ تحدد الغرض من معالجة البيانات الشخصية، وكيفية ذلك؛ سواء أباشرت معالجة البيانات بوساطتها أم بوساطة جهة المعالجة.

الفقرة (19) من المادة (الأولى) من النظام

جهة المعالجة: أي جهة عامة، وأي شخصية ذات صفة طبيعية أو اعتبارية خاصة؛ تعالج البيانات الشخصية لمصلحة جهة التحكم ونيابةً عنها.

جهة التحكم هي الجهة التي تتخذ القرارات بشأن أغراض المعالجة وكيفية إجراء ذلك، ويمكن أن تتحمل جهة التحكم وحدها المسؤولية عن اتخاذ هذه القرارات أو يتحملها عديد من جهات التحكم (مثلاً إذا كانت هناك عدة جهات تحكم لنفس المعالجة للبيانات الشخصية)، وتتولى جهة التحكم مسؤولية أكبر عن المعالجة التي أُجريت ويُفرض عليها عديد من الالتزامات بموجب النظام مقارنة بجهة المعالجة.

تؤدي جهة المعالجة دوراً آخر يخضع للنظام إذ إنها تعالج البيانات الشخصية نيابة عن جهة التحكم، وعلى عكس جهة التحكم، لا تتخذ جهة المعالجة قرارات عن أغراض المعالجة وكيفيتها.

وبغض النظر عن الدور الذي ستقوم به الجهة، سواء جهة التحكم أو جهة المعالجة، سينطبق النظام على معالجة البيانات الشخصية في كل الجهات، وقد يلزم عليها بناءً على القطاع الذي تعمل فيه، والامتثال لقواعد حماية البيانات الشخصية الأخرى المنصوص عليها في الأنظمة التي تسري على القطاع التابعة له (على سبيل المثال: قطاع الرعاية الصحية وقطاع البنوك والقطاع المالي).

وفي جميع الأحوال يجب على جهة التحكم التأكد من الالتزام بالنظام من قبل جهة المعالجة التي تتعامل معها.

متى لا تسري أحكام النظام؟

لا يسري النظام وأحكامه في حالة معالجة البيانات الشخصية لأغراض عائلية أو شخصية.

الفقرة (2) من المادة (الثانية) من النظام

يُستثنى من نطاق تطبيق النظام، قيام الفرد بمعالجة البيانات الشخصية لأغراض لا تتجاوز الاستخدام الشخصي أو العائلي، ما دام أنه لم ينشرها أو يفصح عنها للغير.

ما المقصود بالاستخدام الشخصي أو العائلي؟

يقصد بالاستخدام الشخصي أو العائلي معالجة البيانات الشخصية من قبل فرد داخل نطاق أسرته أو دائرته الاجتماعية المحدودة، ولا يتعلق ذلك بأي استخدام ذي طابع مهني أو تجاري، كما أنه لا يتضمن نشر البيانات الشخصية للجمهور أو الإفصاح عنها إلى أي فرد خارج النطاق العائلي أو الشخصي، ويُقصد من ذلك أنه لا يجب الالتزام بأحكام النظام عند استخدام البيانات الشخصية لأغراض شخصية أو عائلية خالصة، وقد تتضمن، على سبيل المثال لا الحصر:

1. التواصل مع الأقارب، والأصدقاء، وزملاء العمل، والأشخاص الآخرين لأغراض شخصية لا تتعلق بالعمل.
2. التقاط الصور أو تسجيل مقاطع الفيديو لأغراض شخصية.
3. تسجيل بيانات التواصل الخاصة بأفراد آخرين ومشاركتها لأغراض شخصية.

مثال | الاستخدام الشخصي أو العائلي | المعالجة غير الخاضعة للنظام

يقوم مجموعة من الأصدقاء بالاحتفال بتخرج أحدهم من الجامعة في مطعم في مدينة الدمام، وقد قام الأصدقاء أثناء الاحتفال بالتقاط صور لهم وتسجيل مقاطع فيديو أثناء الاحتفال، وفيما بعد نشر الأصدقاء هذه الصور ومقاطع الفيديو في منصات التواصل الاجتماعي لأغراضهم الشخصية، وتعتبر الصور ومقاطع الفيديو بيانات شخصية للأفراد الموجودين في الصور ومقاطع الفيديو.
في هذه الحالة لن يقع أخذ الصور وتسجيل مقاطع الفيديو ونشرها في منصات التواصل الاجتماعي ضمن نطاق النظام ويجب التنويه أنه قد ينطبق عليها أنظمة أخرى على سبيل المثال لا الحصر (مكافحة الجرائم المعلوماتية، حماية الملكية الفكرية وغيرها).

مثال | الاستخدام الشخصي أو العائلي | المعالجة الخاضعة للنظام

يسافر مدون شهير إلى جميع أنحاء العالم باستمرار وينشر القصص عن رحلاته، وفي بعض الأحيان ينشر صوراً عن الفنادق والمطاعم التي يزورها في المملكة والتي تتضمن كذلك صوراً لأشخاص آخرين (على سبيل المثال: العاملين بالفنادق والمطاعم)، ثم يتلقى هذا المدون مقابلاً مادياً من هذه الفنادق والمطاعم نظير نشر هذا المحتوى في منصات التواصل الاجتماعي، وفي هذه الحالة يتعلق نشر الصور بالأنشطة المهنية والتجارية التي يمارسها المدون، لذا سيقع نشاط أخذ هذه الصور ونشرها ضمن نطاق النظام.

متى يدخل النظام حيز التنفيذ؟

دخل النظام حيز التنفيذ في **14 سبتمبر 2023م**.

وفقاً للبند (ثالثاً) من المرسوم الملكي رقم م/ **19** (الذي اعتمد النظام)، توجد فترة تصحيحية لمدة عام من تاريخ دخول النظام حيز التنفيذ لضمان الالتزام به.

ما الذي ينبغي فعله خلال الفترة التصحيحية؟

لن تقوم الجهة المختصة خلال الفترة التصحيحية بفرض العقوبات، وعلى الرغم من ذلك يجب على جهات التحكم خلال هذه الفترة القيام بتعديل أوضاعها لضمان الالتزام بأحكام النظام بحلول **14 سبتمبر 2024م**.

وفقاً للبند (ثالثاً) من المرسوم الملكي رقم **م/ 19** وتاريخ **1443/2/9** يجوز للجهة المختصة تمديد الفترة التصحيحية في حالة تقديم أسباب معقولة تستدعي تمديدها، وستحدد الجهة المختصة طبيعة الأسباب المعقولة في كل حالة على حدة وفقاً لتقديرها، ولا تعفي الفترة التصحيحية الجهات من وجوب الالتزام بالأنظمة واللوائح الأخرى المعمول بها في مجال حماية البيانات الشخصية (على سبيل المثال: في القطاع المالي وقطاع الرعاية الصحية).

من هي الجهة المختصة؟

وفقاً لقرار مجلس الوزراء **رقم 98 وتاريخ 1443/2/7** الجهة المختصة هي سدايا لمدة سنتين، وينظر خلالها -في ضوء ما ينتج عن تطبيق أحكام النظام ولوائحه وفي ضوء مستوى النضج في قطاع البيانات- في نقل اختصاص الإشراف على تطبيق أحكام النظام ولوائحه إلى مكتب إدارة البيانات الوطنية.

وتتضمن المهام الرئيسية للجهة المختصة، على سبيل المثال لا الحصر الآتي:

1. مراقبة الالتزام بأحكام النظام والإشراف عليه وتنفيذه.
2. تقديم المشورات حول النظام والوثائق النظامية الأخرى المتعلقة بحماية البيانات الشخصية.
3. إدارة استقبال الشكاوى والتحقيق فيها.

حقوق الأفراد

ينص النظام على أن الأفراد يتمتعون بعدد من الحقوق، ويجب على جهات التحكم التأكد من أنه يمكن للأفراد ممارسة هذه الحقوق.

الرقم	حق الفرد	وصف الحق	مواد النظام
1	الحق في العلم	يحق للأفراد إحاطتهم علماً بالمسوغ النظامي لجمع بياناتهم الشخصية والغرض من ذلك.	الفقرة 1 من المادة 4
2	الحق في الوصول إلى البيانات الشخصية	يحق للأفراد الوصول إلى بياناتهم الشخصية المتوفرة لدى جهة التحكم.	الفقرة 2 من المادة 4
3	الحق في طلب الحصول على البيانات الشخصية	يحق للأفراد طلب تقديم نسخة من بياناتهم الشخصية بصيغة مقروءة وواضحة.	الفقرة 3 من المادة 4
4	الحق في طلب تصحيح البيانات الشخصية	يحق للأفراد طلب تصحيح بياناتهم الشخصية (إذا كانت غير صحيحة)، أو إتمامها (إذا كانت ناقصة)، أو تحديثها (إذا كانت غير محدثة).	الفقرة 4 من المادة 4
5	الحق في طلب إتلاف البيانات الشخصية	يحق للأفراد طلب إتلاف بياناتهم الشخصية وفقاً لمتطلبات النظام واللوائح التنفيذية للنظام.	الفقرة 5 من المادة 4
6	الحق في الرجوع عن الموافقة	يحق للأفراد في أي وقت الرجوع عن موافقتهم التي قدموها من قبل عن معالجة بياناتهم الشخصية.	الفقرة 2 من المادة 5

مبادئ حماية البيانات الشخصية

على الرغم من أن النظام لم ينص صراحة على أي مبادئ تتعلق بحماية البيانات الشخصية، فإنها مذكورة ضمناً في أحكام النظام.

يساعد فهم هذه المبادئ على فهم متطلبات النظام، وثمة سبعة مبادئ أساسية تتعلق بحماية البيانات الشخصية وتشكل أساس النظام، وهي:

الرقم	المبدأ	وصف المبدأ
1	النظامية والأمانة والشفافية	1. يجب التأكد من جمع البيانات الشخصية استناداً إلى مسوغ نظامي. 2. يلزم معالجة البيانات الشخصية في جميع الأوقات بما يتوافق مع الأنظمة واللوائح المعمول بها في المملكة. 3. ينبغي تزويد الأفراد بما يوضح لهم كيفية معالجة بياناتهم الشخصية
2	محدودية الغرض	1. يجب أن يكون لدى الجهة غرض محدد لمعالجة البيانات الشخصية. 2. يجب كذلك تحديد الغرض من جمع البيانات الشخصية وتوثيقه في سجل أنشطة المعالجة.
3	تقليل البيانات	ينبغي الامتناع عن جمع بيانات شخصية بطريقة تزيد على الحاجة من أجل تحقيق الغرض من المعالجة، لذا إذا لم تكن هنالك حاجة إلى البيانات الشخصية، يجب الامتناع عن جمعها.
4	محدودية التخزين	ينبغي الامتناع عن تخزين البيانات الشخصية لفترة أطول من الفترة المناسبة لتحقيق أغراض معالجة البيانات الشخصية أو الفترة المحددة في الأنظمة أو اللوائح المعمول بها.
5	الدقة	1. يجب مراجعة البيانات الشخصية بطريقة مستمرة للتأكد من أنها صحيحة وكاملة ومحدثة. 2. ينبغي أن تمنح للأفراد فرصة لمراجعة بياناتهم الشخصية وتحديثها، إذا كانت هناك حاجة إلى ذلك.
6	النزاهة والسرية	يجب اتخاذ إجراءات تنظيمية وإدارية وتقنية كافية من أجل حماية البيانات الشخصية وضمان سريتها وسلامتها وإمكانية الوصول إليها أثناء نقلها وتخزينها.
7	المسؤولية	يجب اتخاذ إجراءات مناسبة وتوفير السجلات اللازمة لإثبات الالتزام بالأنظمة واللوائح والمبادئ المتعلقة بحماية البيانات الشخصية.

يُرجى العلم أن الالتزام بالمبادئ أعلاه لن يعفي من الالتزام للنظام بشكل كامل، ومن المهم مراجعة كل متطلبات النظام واللوائح لضمان الامتثال لها، وتشكل المبادئ أعلاه الأساس نحو الامتثال الفعال للنظام.

الملحق (1) أمثلة للممارسات المخالفة للنظام عند التعامل مع البيانات الشخصية

يُرجى العلم أن هذه القائمة غير شاملة ووضعت لأغراض التوضيح فحسب، ويلزم عند تجنب الممارسات الواردة في هذه القائمة، الحرص على استيفاء جميع المتطلبات المنصوص عليها في النظام.

مثال (1) | استخدام البيانات الشخصية دون مسوغ نظامي محدد

يجمع متجر إلكتروني من كل عميل، قبل إتمام عملية البيع، اسمه وبريده الإلكتروني ورقم هاتفه، ولا يحصل العملاء على أي توضيحات عن سبب جمع هذه البيانات ولا يُطلب منهم أي موافقة لمعالجة بياناتهم الشخصية.

بعد جمع البيانات الشخصية أعلاه، يعمل المتجر على:

1. وضع البيانات الشخصية المجمعة في نظام التخزين السحابي المستضاف خارج المملكة.
2. إرسال رسائل تسويقية إلى عناوين البريد الإلكتروني المجمعة لديه بشكل مستمر.
3. نقل البيانات الشخصية المجمعة إلى وكالة تحليل البيانات.

لم يحدد المتجر أي مسوغات نظامية لأي من الأغراض أعلاه فيما يتعلق باستخدام البيانات الشخصية، ولا تدرك إدارة المتجر ما هي المسوغات النظامية التي يمكن استخدامها.

تعد هذه من الممارسات المخالفة وينبغي تجنبها، إذ إنه يجب دائماً تحديد المسوغات النظامية لكل غرض من أغراض معالجة البيانات الشخصية وفق المادة الخامسة والمادة السادسة من النظام.

مثال (2) | جمع البيانات الشخصية دون غرض محدد

تجمع الصيدلية أرقام الهواتف الخاصة بكل عملائها، وعند سؤالها عن السبب في ذلك، لم يستطع موظف أو مدير الصيدلية توضيح السبب في حاجة الصيدلية إلى أرقام الهواتف، وما استطاعا تفسيره هو أن "هذا يعتبر إجراءً روتينياً للصيدلية" ولا يوجد في الصيدلية أي وثائق تحدد الغرض من جمع هذه البيانات بصفة رسمية.

تعد هذه من الممارسات المخالفة التي يجب تجنبها، إذ إنه يلزم عدم جمع البيانات الشخصية إلا في حالة تحديد أغراض جمعها وتوثيق هذه الأغراض وإحاطة صاحب البيانات علماً بها.

مثال (3) | تخزين البيانات الشخصية لفترة غير محددة

تخزن إدارة الموارد البشرية في أنظمتها بيانات عن جميع الموظفين العاملين بالجهة، مثل الموظفين الذين تركوا العمل، كما أنها تخزن السير الذاتية لجميع المرشحين الذين تقدموا بطلب للالتحاق بالجهة لمدة غير محددة ولا تحذفها أبداً.

تعد هذه من الممارسات المخالفة التي يجب تجنبها، إذ إنه يلزم إتلاف البيانات الشخصية التي لم تعد الإدارة بحاجة إليها (مع مراعاة الاستثناء الموضح في المادة الثامنة عشرة من النظام).

مثال (4) | معالجة البيانات الشخصية دون تسجيل أنشطة المعالجة

تحلل شركة تسويق كمية كبيرة من البيانات الشخصية الخاصة بعديد من العملاء، ولدى الشركة عدد من الإدارات ذوات مسؤوليات مختلفة.

لا تحرص شركة التسويق على توثيق أي من أنشطة المعالجة التي تجريها، ونتيجة لذلك لا تعلم إدارة الشركة أنواع البيانات الشخصية التي تعالجها ومكان تخزينها وإلى من تُنقل هذه البيانات الشخصية.

تعد هذه من الممارسات المخالفة التي ينبغي تجنبها، إذ إنه يلزم الحفاظ على سجلات الأنشطة المعالجة لفهم العمليات المتعلقة بالبيانات الشخصية في الجهة.

مثال (5) | مشاركة البيانات الشخصية دون أي مسوغ نظامي ودون توجيه أي إشعار خصوصية إلى الأفراد

يحصل العميل على رقم هاتف جديد من إحدى شركات الاتصالات، وفي اليوم ذاته، تبيع الشركة قاعدة البيانات التي تتضمن بيانات العميل الشخصية إلى شركة دعائية، ولم يكن العميل على دراية بنقل بياناته الشخصية لأغراض دعائية، ثم يتفاجأ عندما يبدأ في استلام رسائل دعائية من المتاجر والمطاعم والصيدليات التي لم يتواصل معها أو يزورها من قبل.

تعد هذه من الممارسات المخالفة التي ينبغي تجنبها، إذ إنه يلزم بالامتناع عن مشاركة البيانات الشخصية مع أي جهة ما لم يكن هناك مسوغ نظامي لذلك وما لم يكن هناك امتثال لمتطلبات النظام المتعلقة بالإفصاح عن البيانات الشخصية، ويجب أن يحصل الفرد الذي تشارك بياناته الشخصية مع الآخرين على إشعار خصوصية حتى يدرك كيفية معالجة بياناته الشخصية والسبب في ذلك.

مثال (6) | عدم وجود سياسات وتدريب عن حماية البيانات الشخصية

لم تصدر الصيدلية أي سياسات أو إجراءات تتعلق بحماية البيانات فضلاً عن أن العاملين فيها لم يحصلوا على أي تدريب أو توعية عن ممارسات حماية البيانات الشخصية، ونتيجة لذلك لا يدرك موظفوها كيفية معالجة البيانات الشخصية الخاصة بعملائها بصفة يومية.

تعد هذه من الممارسات المخالفة التي يجب تجنبها، إذ إنه يتعين إصدار سياسات وإجراءات تتعلق بحماية البيانات الشخصية وتنظيم كيفية استخدام البيانات الشخصية في الجهة، وعند إعداد هذه السياسات أو الإجراءات، من المهم تنفيذها داخل المؤسسة وأن يكون الموظفون على دراية بمسؤولياتهم. كما أنه يجب تدريب الموظفين الذين يقومون بمعالجة البيانات بصفة مستمرة حتى يتسنى لهم فعل ذلك وفقاً للنظام وسياسات الجهة الداخلية.

مثال (7) | الإعلان عن بيانات المرضى الشخصية في العيادة

يوجد في إحدى العيادات منطقة انتظار مخصصة للمرضى يجلسون فيها قبل تلقي العلاج، يكون الطبيب بالعيادة جاهزاً لاستقبال المريض، تأتي الممرضة إلى منطقة الانتظار وتنادي بصوت مرتفع على المريض وأسباب الزيارة حيث يمكن لجميع المرضى الآخرين سماع هذه المعلومات، تعد هذه من الممارسات المخالفة التي يجب تجنبها، إذ إن اسم المريض (وسبب الزيارة) من البيانات الشخصية للمريض ويجب التأكد من عدم الإفصاح عن اسم المريض إلا إذا كان ذلك استناداً إلى المسوغات النظامية المحددة في المادة الخامسة والمادة السادسة وشريطة استيفاء المتطلبات الإضافية المنصوص عليها في المادة الخامسة عشرة من النظام.

وللاطلاع على النظام ولوائحه التنفيذية الرجاء زيارة موقع سدايا الإلكتروني

منصة حوكمة البيانات الوطنية