SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

قرار إداري رقم (١٥١٦) وتاريخ ١٩ /٢/١٤٤٥هـ

إن رئيس الهيئة السعودية للبيانات والذكاء الاصطناعي

بناءً على الصلاحيات الممنوحة له، وعلى ما تقتضيه مصلحة العمل.

وبناءً على المادة (الثانية والأربعين) من نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم (م/١٩) وتاريخ ١٤٤٣/٢/٩هـ، والمعدل بموجب المرسوم الملكي رقم (م/١٤٨) وتاريخ ١٤٤٤/٩/٥هـ.

وبناءً على ما عرضه علينا معالي رئيس مكتب إدارة البيانات الوطنية بشأن مشروع اللوائح التنفيذية لنظام حماية البيانات الشخصية.

يقرر ما يلي:

أولاً: الموافقة على اللائحة التنفيذية لنظام حماية البيانات الشخصية بالصيغة المرافقة لهذا القرار.

ثانياً: يبلغ هذا القرار للجهات المعنية لتنفيذه والعمل بموجبه.

والله الموفق،،،

رئيس الهيئة السعودية
للبيانات والذكاء الاصطناعي

د. عبدالله بن شرف الغامدي

المدينة الرقمية، مبنى رقم RD04
حي النخيل، الرياض، المملكة العربية السعودية
Digital City, Building RD04
Al Nakheel, Riyadh, Kingdom of Saudi Arabia
SDAIA.GOV.SA

اللائحة التنفيذية لنظام حماية البيانات الشخصية

المادة الأولى: التعريفات

تكون للكلمات والعبارات الواردة في هذه اللائحة المعاني الموضحة أمام كل منها في المادة (الأولى) من نظام حماية البيانات الشخصية، الصادر بالمرسوم الملكي رقم (م/١٩) وتاريخ ١٤٤٣/٢/٩هـ والمعدل بموجب المرسوم الملكي رقم (م/١٤٨) وتاريخ ١٤٤٤/٩/٥هـ، ويقصد بالألفاظ والعبارات الآتية -أينما وردت في هذه اللائحة- المعاني الموضحة أمام كل منها، ما لم يقتضِ السياق غير ذلك:

١- **اللائحة:** اللائحة التنفيذية للنظام.

٢- **التسويق المباشر:** التواصل مع صاحب البيانات الشخصية بأي وسيلة مادية أو إلكترونية مباشرة بهدف توجيه مادة تسويقية، ويشمل ذلك على سبيل المثال لا الحصر الإعلانات أو العروض الترويجية.

٣- **تسرب البيانات الشخصية:** أي حادثة تؤدي إلى الإفصاح عن البيانات الشخصية أو تلفها أو الوصول غير المشروع إليها، سواء كان ذلك بقصد أو بغير قصد، وبأي وسيلة كانت سواء آلية أو يدوية.

٤- **المصلحة الحيوية:** أي من المصالح الضرورية للحفاظ على حياة صاحب البيانات الشخصية.

٥- **المصلحة المتحققة:** أي مصلحة معنوية أو مادية لصاحب البيانات الشخصية ترتبط بشكل مباشر بالغرض من معالجة البيانات الشخصية، وتكون المعالجة ضرورية لتحقيق تلك المصلحة.

٦- **المصلحة المشروعة:** أي حاجة ضرورية لدى جهة التحكم يتطلب تحقيقها معالجة بيانات شخصية لغرض محدد، على ألا تؤثر على حقوق ومصالح صاحب البيانات الشخصية.

٧- **الترميز:** 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 الشخصية بشكل محدد.

٨- **إخفاء الهوية:** إزالة المعرفات المباشرة وغير المباشرة التي تدل على هوية صاحب البيانات الشخصية بشكل نهائي يتعذر معه تحديد هوية صاحب البيانات الشخصية.

٩- **الموافقة الصريحة:** موافقة تمنح بشكل مباشر وصريح من صاحب البيانات الشخصية بأي شكل من الأشكال وتدل على قبوله بمعالجة بياناته الشخصية بحيث لا يمكن تفسيرها بخلاف ذلك، وتكون قابلة للإثبات.

المادة الثانية: الاستخدام الشخصي أو العائلي

١- لا تسري أحكام النظام ولوائحه على قيام الفرد بمعالجة البيانات الشخصية لأغراض لا تتجاوز الاستخدام الشخصي أو العائلي.

٢- يقصد بالاستخدام الشخصي أو العائلي المنصوص عليه في المادة الثانية من النظام قيام الفرد بمعالجة البيانات الشخصية داخل نطاق أسرته أو دائرته الاجتماعية المحدودة ضمن أي نشاط اجتماعي أو عائلي.

٣- لا يعد من قبيل الاستخدام الشخصي أو العائلي ما يلي:

أ- قيام الفرد بنشر البيانات الشخصية للجمهور أو الإفصاح عنها لأي شخص خارج النطاق المحدد في الفقرة (٢) من هذه المادة.

ب- استخدام البيانات الشخصية لأغراض ذوات طابع مهني أو تجاري أو غير ربحي.

المادة الثالثة: الأحكام العامة لحقوق أصحاب البيانات الشخصية

١- على جهة التحكم عند تلقيها طلباً من صاحب البيانات الشخصية يتعلق بحقوقه المنصوص عليها في النظام القيام بما يلي:

أ- تنفيذ طلبات ممارسة الحقوق المنصوص عليها في النظام خلال مدة لا تتجاوز (ثلاثين) يوماً دون تأخير، ولها تمديد ذلك في حال تطلب التنفيذ جهداً إضافياً غير متوقع أو غير معتاد أو في حال تلقيها طلبات متعددة من صاحب البيانات الشخصية، وذلك بما لا يزيد على (ثلاثين) يوماً إضافية، بشرط أن تُشعِر صاحب البيانات الشخصية مسبقا بالتمديد ومبرراته.

ب- تبني الوسائل التقنية والإدارية والتنظيمية اللازمة لضمان سرعة الاستجابة لطلبات ممارسة الحقوق.

ج- اتخاذ الإجراءات والتدابير المناسبة للتحقق من هوية مُقدم الطلب قبل تنفيذه بما يتوافق مع الأحكام النظامية ذوات العلاقة.

د- اتخاذ الوسائل اللازمة لتوثيق وحفظ كافة الطلبات المقدمة لها، بما في ذلك الطلبات الشفهية.

٢- في حال كان الطلب متكرراً بشكل غير مبرر أو يتطلب تنفيذه جهداً غير عادي؛ يكون لجهة التحكم عدم معالجة الطلب، على أن يكون ذلك مسبباً ويُشعَر صاحب البيانات الشخصية به.

٣- في الحالات التي يكون صاحب البيانات الشخصية ناقصاً أو عديم الأهلية، يكون لوليه الشرعي ممارسة حقوقه نيابة عنه.

المادة الرابعة: الحق في العلم

١- في حال تم جمع البيانات الشخصية من صاحبها مباشرةً، يجب على جهة التحكم قبل أو عند جمع البيانات اتخاذ التدابير اللازمة لإبلاغ صاحب البيانات الشخصية بالآتي:

أ- الاسم النظامي لجهة التحكم، وبيانات التواصل الخاصة بها، وأي تفاصيل أخرى تخص القنوات المُنشأة من قبل جهة التحكم لغرض التواصل المرتبط بحماية البيانات الشخصية.

ب- بيانات الاتصال بمسؤول حماية البيانات الشخصية -إن وجد- المعيّن من قبل جهة التحكم.

ج- المسوغ النظامي والغرض من جمع ومعالجة البيانات الشخصية بصورة محددة وواضحة وصريحة.

د- مدة الاحتفاظ بالبيانات الشخصية أو معايير حساب المدة في حال تعذر تحديدها مسبقاً.

هـ- توضيح حقوق صاحب البيانات الشخصية، المنصوص عليها في المادة (الرابعة) من النظام وآلية ممارسة أي من تلك الحقوق.

و- توضيح كيفية العدول عن الموافقة الممنوحة لمعالجة أي من البيانات الشخصية.

ز- بيان ما إذا كان جمع أي من البيانات الشخصية أو معالجتها إلزامياً أو اختيارياً.

٢- لا يطبق ما ورد في الفقرة (١) من هذه المادة في حال كانت المعلومات الموضحة في الفقرات الفرعية (أ) إلى (ز) متوفرة مسبقاً لصاحب البيانات الشخصية، أو إذا كان تقديم تلك المعلومات يتعارض مع أي من الأنظمة السارية في المملكة.

٣- في حال تم جمع البيانات الشخصية من غير صاحبها مباشرة، على جهة التحكم عند تلقيها للبيانات الشخصية القيام -دون تأخر غير مبرر- وخلال مدة لا تتجاوز (٣٠) يوماً اتخاذ الخطوات اللازمة لإبلاغ صاحب البيانات الشخصية بما نصت عليه الفقرة (١) من هذه المادة إضافة إلى فئات البيانات الشخصية التي تتم معالجتها، والمصدر الذي تم من خلاله حصول جهة التحكم على البيانات الشخصية.

٤- لا يطبق مع ما ورد في الفقرة (٣) من هذه المادة في أي من الأحوال الآتية:

أ- إذا كانت المعلومات متوفرة مسبقاً لصاحب البيانات الشخصية.

ب- إذا كان تنفيذ ذلك غير ممكناً أو يتطلب جهداً غير معقول.

ج- إذا كان حصول جهة التحكم على البيانات قد تم تنفيذاً لنظام.

د- إذا كانت جهة التحكم جهة عامة وكان جمع البيانات الشخصية لأغراض أمنية أو لاستيفاء متطلبات قضائية، أو لتحقيق مصلحة عامة.

هـ- إذا كانت البيانات الشخصية تخضع لأحكام السرية المهنية المقررة نظاماً.

٥- على جهات التحكم التي تتضمن أنشطتها -على نطاق واسع أو بصورة متكررة- معالجة بيانات شخصية لناقصي أو عديمي الأهلية، أو عمليات المعالجة التي تتطلب بطبيعتها مراقبة مستمرة

لأصحاب البيانات الشخصية، أو معالجة بيانات شخصية باستخدام تقنيات ناشئة، أو اتخاذ قرارات مبنية على المعالجة الآلية للبيانات الشخصية؛ اتخاذ التدابير اللازمة لإبلاغ صاحب البيانات الشخصية بما نصت عليه الفقرة (١) من هذه المادة، إضافة إلى ما يلي:

أ- وسائل وطرق الجمع والمعالجة للبيانات الحساسة إن تضمنت المعالجة ذلك.

ب- الوسائل والإجراءات المتخذة لحماية البيانات الشخصية.

ج- توضيح ما إذا كان سيتم اتخاذ قرارات مبنية بشكل كامل على المعالجة الآلية للبيانات الشخصية.

٦- عند قيام جهة التحكم بمعالجة إضافية للبيانات الشخصية لغرض آخر غير الذي جمعت من أجله، فيجب عليها قبل إجراء المعالجة الإضافية أن تقدم لصاحب البيانات الشخصية المعلومات اللازمة وفقاً لأحكام هذه المادة.

٧- يجب على جهة التحكم أن توفر المعلومات المطلوبة وفقاً لما ورد في هذه المادة بلغة مناسبة إذا علمت أن صاحب البيانات الشخصية ناقص الأهلية.

المادة الخامسة: الحق في الوصول إلى البيانات الشخصية

١- دون الإخلال بأحكام المادة (التاسعة) والمادة (السادسة عشرة) من النظام، يكون لصاحب البيانات الشخصية حق الوصول إلى بياناته الشخصية المتوافرة لدى جهة التحكم مع مراعاة ما يلي:

أ- ألا تؤثر ممارسة الحق في الوصول إلى البيانات الشخصية سلباً على حقوق الغير، مثل: حقوق الملكية الفكرية أو الأسرار التجارية.

ب- إتاحة الوصول إلى البيانات الشخصية بناءً على طلب يقدمه صاحب البيانات الشخصية، أو وسيلة توفرها جهة التحكم لتمكين صاحب البيانات من الوصول إلى بياناته الشخصية بشكل تلقائي دون الحاجة إلى تقديم طلب.

٢- على جهة التحكم عند تمكين صاحب البيانات من الوصول إلى بياناته الشخصية التأكد من أن ذلك لا يتضمن الإفصاح عن بيانات شخصية تحدد هوية فرد آخر.

المادة السادسة: الحق في طلب الحصول على البيانات الشخصية

مع مراعاة أحكام المادة (السادسة عشرة) من النظام يكون لصاحب البيانات الشخصية الحق في طلب الحصول على نسخة من بياناته الشخصية بصيغة مقروءة وواضحة، مع مراعاة ما يلي:

١- ألا تؤثر ممارسة الحق في الحصول على البيانات الشخصية سلباً على حقوق الغير، مثل: حقوق الملكية الفكرية أو الأسرار التجارية.

٢- تُقدَّم البيانات الشخصية إلى صاحب البيانات الشخصية بصيغة إلكترونية شائعة الاستخدام، ولصاحب البيانات الشخصية طلب نسخة مطبوعة منها متى ما كان تنفيذ ذلك ممكناً.

٣- على جهة التحكم عند تمكين صاحب البيانات من الحصول على بياناته الشخصية التأكد من أن ذلك لا يتضمن الإفصاح عن بيانات شخصية تحدد هوية فرد آخر.

المادة السابعة: الحق في طلب تصحيح البيانات الشخصية

١- يجوز لصاحب البيانات الشخصية في حال عدم صحة بياناته الشخصية المتوافرة لدى جهة التحكم أن يطلب تقييد معالجة بياناته لمدة يمكن لجهة التحكم خلالها التحقق من صحة البيانات

الشخصية، مع مراعاة عدم سريان حق صاحب البيانات الشخصية في الحصول على التقييد المذكور إذا كان تقديم تلك البيانات يتعارض مع أحكام النظام وهذه اللائحة.

٢- يكون لجهة التحكم طلب المستندات أو الوثائق الداعمة لطلب تصحيح البيانات الشخصية متى ما كان ذلك ضرورياً لتحديث أو تصحيح أو إتمام البيانات الشخصية، على أن يتم إتلاف تلك المستندات أو الوثائق بعد الانتهاء من عملية التحقق.

٣- على جهة التحكم بعد تصحيح البيانات الشخصية إشعار الجهات التي أُفصح لها سابقاً عن البيانات الشخصية دون تأخير.

المادة الثامنة: الحق في طلب إتلاف البيانات الشخصية

١- على جهة التحكم إتلاف البيانات الشخصية في أي من الأحوال الآتية:

أ- تنفيذاً لطلب صاحب البيانات الشخصية.

ب- إذا لم تعد البيانات الشخصية ضرورية لتحقيق الغرض الذي جمعت من أجله.

ج- إذا عدل صاحب البيانات الشخصية عن موافقته على جمع بياناته الشخصية، وكانت الموافقة هي المسوغ النظامي الوحيد للمعالجة.

د- إذا علمت أن البيانات الشخصية تجرى معالجتها بطريقة مخالفة للنظام.

٢- على جهة التحكم عند إتلافها للبيانات الشخصية القيام بالآتي:

أ- اتخاذ الإجراءات الملائمة لإشعار الجهات الأخرى التي أفصحت لها جهة التحكم عن البيانات الشخصية ذوات الصلة، وطلب إتلافها.

ب- اتخاذ الإجراءات الملائمة لإشعار الأشخاص الذين تم الإفصاح لهم عن البيانات الشخصية بأي وسيلة كانت، وطلب إتلافها.

ج- إتلاف كافة النسخ المتعلقة بالبيانات الشخصية المخزنة في أنظمة جهة التحكم، بما في ذلك النسخ الاحتياطية، على أن تراعى المتطلبات النظامية ذوات العلاقة بهذا الشأن.

٣- لا يخل ما ورد في هذه المادة ما نصت عليه المادة (الثامنة عشرة) من النظام والمتطلبات النظامية التي تقرها الجهات المختصة ذوات العلاقة.

المادة التاسعة: إخفاء الهوية

١- على جهة التحكم عند إخفائها لهوية صاحب البيانات الشخصية القيام بالآتي:

أ- التأكد من عدم إمكانية إعادة التعرف على هوية صاحب البيانات الشخصية بعد إخفاء هويته.

ب- تقويم الأثر بما في ذلك إمكانية إعادة تحديد هوية صاحب البيانات الشخصية، وذلك في الأحوال المنصوص عليها في الفقرة (١) من المادة (الخامسة والعشرين) من هذه اللائحة.

ج- اتخاذ التدابير التنظيمية والإدارية والتقنية اللازمة لتجنب المخاطر، مع مراعاة التطورات التقنية وأساليب إخفاء الهوية وتحديثها ومواءمتها مع تلك التطورات.

د- تقويم فاعلية تقنيات إخفاء هوية صاحب البيانات الشخصية المُطبقة، وإجراء التعديلات اللازمة لضمان عدم إمكانية إعادة التعرف على هوية صاحب البيانات الشخصية.

٢- لا تعد البيانات التي جرى إخفاء هوية أصحابها بيانات شخصية.

المادة العاشرة: وسائل التواصل

على جهة التحكم توفير الوسائل الملائمة للاستجابة لطلبات صاحب البيانات الشخصية المتعلقة بحقوقه المنصوص عليها في النظام، ويكون لصاحب البيانات الشخصية استخدام واحدة أو أكثر من الوسائل الآتية حسب اختياره وتوافرها لدى جهة التحكم:

١- البريد الإلكتروني.

٢- الرسائل النصية.

٣- العنوان الوطني.

٤- التواصل عبر التطبيقات الإلكترونية.

٥- أي وسيلة تواصل نظامية أخرى معدة لهذا الغرض من قبل جهة التحكم.

المادة الحادية عشرة: الموافقة

١- لجهة التحكم الحصول على موافقة صاحب البيانات الشخصية على معالجة بياناته بأي شكل أو وسيلة ملائمة، بما في ذلك الموافقات الكتابية أو الشفوية أو باستخدام الطرق الإلكترونية، على أن يشترط في الموافقة ما يأتي:

أ- أن تصدر الموافقة بإرادة حرة، وألّا تُستخدم أي طرقٍ مُضللة في سبيل الحصول عليها، وأن يكون الحصول على الموافقة بمراعاة أحكام المادة (السابعة) من النظام.

ب- أن تكون أغراض المعالجة واضحةً ومحددةً، وأن توضح وتبيّن تلك الأغراض إلى صاحب البيانات الشخصية عند أو قبل طلب الموافقة.

ج- أن تصدر من كامل الأهلية.

د- أن توثّق الموافقة بوسائل تتيح التحقق منها مستقبلاً، ومن ذلك الاحتفاظ بسجلات تتضمن موافقة أصحاب البيانات الشخصية على عمليات المعالجة مع بيان وقت ووسيلة الموافقة.

هـ- أن تكون هناك موافقة مستقلة لكل غرض من أغراض المعالجة.

٢- يشترط أن تكون موافقة صاحب البيانات الشخصية صريحة في الأحوال الآتية:

أ- في حال تضمنت المعالجة بيانات حساسة.

ب- في حال تضمنت المعالجة بيانات ائتمانية.

ج- في حال كان سيتم اتخاذ قرارات مبنية بشكل كامل على المعالجة الآلية للبيانات الشخصية.

المادة الثانية عشرة: العدول عن الموافقة

١- لصاحب البيانات الشخصية العدول عن موافقته على معالجة بياناته الشخصية في أي وقت، وله إبلاغ جهة التحكم بذلك بأي من الوسائل المتاحة وفقاً للمادة (الرابعة) من هذه اللائحة.

٢- قبل طلب الموافقة من صاحب البيانات الشخصية، على جهة التحكم وضع إجراءات تُتيح العدول عن تلك الموافقة، واتخاذ التدابير اللازمة لضمان تنفيذها، على أن تكون إجراءات العدول عن الموافقة مماثلة أو أكثر سهولةً من إجراءات الحصول عليها.

٣- في حال العدول عن الموافقة، فيجب على جهة التحكم إيقاف المعالجة دون تأخير غير مبرر، ولا يؤثر الرجوع عن الموافقة على مشروعية أي عملية معالجة تمت في ظل الموافقة وقبل الرجوع عنها.

٤- على جهة التحكم عند عدول صاحب البيانات الشخصية عن موافقته على معالجة بياناته؛ اتخاذ الإجراءات الملائمة لإشعار من تم الإفصاح لهم عن البيانات الشخصية -بأي وسيلة كانت- وطلب إتلافها.

٥- لا يؤثر العدول عن الموافقة على عمليات معالجة البيانات الشخصية التي تتم بناءً على مسوغات نظامية أخرى.

المادة الثالثة عشرة: الولي الشرعي

١- مع مراعاة المتطلبات النظامية ذوات العلاقة، على الولي الشرعي لصاحب البيانات الشخصية ناقص أو عديم الأهلية أن يتصرف بما يحقق مصلحة صاحب البيانات الشخصية، وله في سبيل ذلك ما يلي:

أ- ممارسة الحقوق المقررة لصاحب البيانات الشخصية بموجب النظام وهذه اللائحة.

ب- الموافقة على معالجة بيانات صاحب البيانات الشخصية وفقاً لأحكام النظام وهذه اللائحة.

٢- إضافة إلى ما نصت عليه الفقرة (١) من المادة (الحادية عشرة) من هذه اللائحة، في حال معالجة البيانات الشخصية لناقص أو عديم الأهلية يشترط في الحصول على موافقة الولي الشرعي اتخاذ الوسائل المناسبة للتحقق من صحة الولاية الشرعية لولي صاحب البيانات الشخصية ناقص أو عديم الأهلية.

٣- على جهة التحكم عند الحصول على موافقة الولي الشرعي لناقص أو عديم الأهلية مراعاة الأحكام الآتية:

أ- ألا ينتج عن موافقة الولي الشرعي على المعالجة أي ضرر على مصالح صاحب البيانات الشخصية.

ب- تمكين صاحب البيانات الشخصية ناقص الأهلية من ممارسة حقوقه المنصوص عليها في النظام وهذه اللائحة عند اكتمال أهليته.

المادة الرابعة عشرة: معالجة البيانات الشخصية لمصلحة متحققة

على جهة التحكم عند معالجة البيانات لتحقيق مصلحة متحققة لصاحب البيانات الاحتفاظ بما يثبت توفر تلك المصلحة وتعذر الاتصال بصاحب البيانات الشخصية أو صعوبته.

المادة الخامسة عشرة: جمع البيانات من غير صاحبها مباشرة

١- فيما عدا ما ورد في الفقرة (٣) من المادة (العاشرة) من النظام، على جهة التحكم عند معالجة البيانات الشخصية من غير صاحبها مباشرة، مراعاة ما يأتي:

أ- أن تكون المعالجة ضرورية ومتناسبة مع الغرض المحدد.

ب- ألا تؤثر على حقوق ومصالح صاحب البيانات الشخصية.

٢- على جهة التحكم عند معالجتها للبيانات الشخصية وفقاً للفقرة (٢) من المادة (العاشرة) من النظام، مراعاة أن يكون جمعها من مصدر متاح للعموم قد تم بشكل نظامي.

٣- على جهة التحكم عند معالجتها للبيانات الشخصية وفقاً للفقرة (٦) من المادة (العاشرة) من النظام، مراعاة ما ورد في المادة (التاسعة) من هذه اللائحة في شأن إخفاء الهوية.

المادة السادسة عشرة: المعالجة لأغراض المصلحة المشروعة

١- فيما عدا الأحوال التي تكون فيها جهة التحكم جهة عامة، لجهة التحكم معالجة البيانات الشخصية لتحقيق مصلحة مشروعة يتوفر فيها ما يلي:

أ- ألا يكون الغرض مخالفاً لأي من الأنظمة في المملكة.

ب- الموازنة بين حقوق ومصالح صاحب البيانات الشخصية والمصلحة المشروعة لجهة التحكم، بحيث لا تؤثر مصالح جهة التحكم على حقوق ومصالح صاحب البيانات الشخصية.

ج- ألا تتضمن المعالجة بيانات حساسة.

د- أن تكون المعالجة ضمن التوقعات المعقولة لصاحب البيانات الشخصية.

٢- يعد من المصالح المشروعة كشف عمليات الاحتيال وحماية أمن الشبكة والمعلومات، وغير ذلك من المصالح المشروعة التي يتحقق فيها ما ورد في الفقرة (١) من هذه المادة.

٣- وفقاً لأحكام الفقرة (٤) من المادة (السادسة) من النظام، على جهة التحكم قبل معالجة البيانات الشخصية لمصلحة مشروعة إجراء وتوثيق تقويم للمعالجة المقترحة وأثرها على حقوق ومصالح أصحاب البيانات الشخصية، على أن يتضمن التقويم على وجه التحديد ما يلي:

أ- تحديد المعالجة المقترحة وأغراضها، ونوع البيانات وفئات أصحاب البيانات الشخصية.

ب- تقويم الغرض من خلال التأكد من مشروعيته وعدم مخالفته لأي من الأنظمة في المملكة.

ج- التحقق من أن معالجة البيانات الشخصية ضرورية لتحقيق الغرض المشروع لدى جهة التحكم.

د- تقويم ما إذا كانت المعالجة المقترحة سترتب أي ضرر على مصالح أصحاب البيانات الشخصية أو قدرتهم على ممارسة حقوقهم المقررة نظاماً.

هـ- تقويم ما إذا كانت هناك أي تدابير يتطلب اتخاذها لتجنب المخاطر أو الأضرار المحتملة، وذلك وفقاً لما نصت عليه الفقرة (٢) من المادة (الخامسة والعشرون) من هذه اللائحة.

٤- إذا أظهر التقويم المبيّن بالفقرة (٣) من هذه المادة أن المعالجة المقترحة ستؤدي بأي شكل من الأشكال إلى مخالفة أي من الأنظمة أو المساس بحقوق ومصالح أصحاب البيانات الشخصية أو ترتيب أي ضرر عليهم أو على أي طرف آخر، فيكون على جهة التحكم تعديل المعالجة المقترحة وإجراء تقويم جديد، أو النظر في الاعتماد على مسوغ نظامي آخر.

المادة السابعة عشرة: اختيار جهة المعالجة

١- على جهة التحكم عند اختيار جهة المعالجة الالتزام باختيار جهة معالجة تقدم ضمانات كافية لحماية البيانات الشخصية، وأن يتضمن الاتفاق مع جهة المعالجة ما يلي:

أ- غرض المعالجة.

ب- فئات البيانات الشخصية المعالجة.

ج- المدة الزمنية للمعالجة.

د- التزام جهة المعالجة بإشعار جهة التحكم في حال تسرب البيانات الشخصية، وذلك وفقاً لأحكام النظام وهذه اللائحة ودون تأخر غير مبرر.

هـ- توضيح ما إذا كانت جهة المعالجة تخضع لأنظمة في دول أخرى، وأثر ذلك على التزامها بأحكام النظام ولوائحه.

و- عدم اشتراط حصول جهة المعالجة على موافقة مسبقة من جهة التحكم على الإفصاح الوجوبي عن البيانات الشخصية بموجب الأنظمة المعمول بها في المملكة، على أن تقوم جهة المعالجة بإشعار جهة التحكم بذلك الإفصاح.

ز- تحديد جهات المعالجة الفرعية المتعاقدة مع جهة المعالجة، أو أي طرف آخر سيجري الإفصاح له عن البيانات الشخصية.

٢- على جهة التحكم إصدار التعليمات لجهة المعالجة بشكل واضح، وفي حال مخالفة تعليمات جهة التحكم لأي من الأنظمة المعمول بها في المملكة، فيكون على جهة المعالجة إشعار جهة التحكم بذلك كتابةً ودون تأخير.

٣- تكون جهة التحكم مسؤولة عن التحقق من التزام جهة المعالجة -بشكل دوري- بإجراء عمليات المعالجة وفقاً لأحكام النظام ولوائحه، وضمان استيفائها لكافة المتطلبات النظامية في هذا

الشأن، سواء تمت المعالجة من قبلها أو من قبل جهة أخرى نيابةً عنها، ويكون لجهة التحكم تعيين طرف آخر مستقل للمراجعة والتحقق من الالتزام نيابةً عنها.

٤- عند مخالفة جهة المعالجة للتعليمات الصادرة من جهة التحكم أو الاتفاق المبرم معها بشأن معالجة البيانات الشخصية، فتعد جهة المعالجة في حكم جهة التحكم وتكون مسؤولة عن مخالفة أحكام النظام.

٥- يجب على جهة المعالجة قبل قيامها بأي تعاقدات لاحقة مع جهات معالجة فرعية الالتزام بالآتي:

أ- اتخاذ الضمانات الكافية للتأكد من أن تلك التعاقدات لن تؤثر على المستوى المكفول لحماية البيانات الشخصية محل المعالجة.

ب- اختيار الجهة التي توفر الضمانات اللازمة لتنفيذ أحكام النظام ولوائحه.

ج- الحصول على الموافقة المسبقة من جهة التحكم، على أن يتم إشعار جهة التحكم قبل القيام بتلك التعاقدات وتمكين جهة التحكم من الاعتراض عليها خلال مدة يتفق عليها بين جهة التحكم وجهة المعالجة.

المادة الثامنة عشرة: معالجة البيانات لغرض آخر غير الذي جمعت من أجله

١- على جهة التحكم عند معالجتها البيانات الشخصية لغرض آخر غير الذي جمعت من أجله في الأحوال المنصوص عليها في المادة (العاشرة) من النظام، القيام بما يأتي:

أ- تحديد أغراض المعالجة بشكل محدد وواضح.

ب- توثيق إجراءات تحديد محتوى البيانات وفقاً للأغراض المحددة، ومنها على سبيل المثال استخدام مخططات البيانات التي تبيّن الحاجة إلى كل بيان وربطه بكل هدف من أهداف المعالجة.

ج- اتخاذ التدابير اللازمة لضمان جمع البيانات الشخصية وفق الحد الأدنى الضروري لتحقيق الأغراض المحددة في الفقرة (ب) أعلاه.

٢- فيما عدا الأحوال المنصوص عليها في الفقرة (٣) من المادة (العاشرة) من النظام، على جهة التحكم عند معالجتها البيانات الشخصية لغرض آخر غير الذي جمعت من أجله في الأحوال المنصوص عليها في الفقرات (١) و(٢) و(٤) و(٥) و(٦) من المادة (العاشرة) من النظام، الالتزام بما يأتي:

أ- تحديد الغرض من المعالجة بوضوح ودقة، وتضمينه في سجلات أنشطة معالجة البيانات الشخصية.

ب- أن يقتصر الجمع والمعالجة على الحد الأدنى من البيانات الشخصية المطلوبة لتحقيق الغرض.

ج- أن يتم تحديد نوع البيانات الشخصية المراد معالجتها، والتدابير اللازمة لضمان معالجة تلك البيانات بالشكل المطلوب.

المادة التاسعة عشرة: جمع الحد الأدنى من البيانات الشخصية

١- على جهة التحكم جمع الحد الأدنى اللازم من البيانات الشخصية لتحقيق الغرض من المعالجة، وضمان ما يلي:

أ- جمع البيانات الشخصية الضرورية والمرتبطة ارتباطاً وثيقاً ومباشراً بالغرض من معالجة البيانات، ويتم تحديد ذلك من خلال استخدام الوسائل الملائمة، بما في ذلك مخططات البيانات التي تبيّن الحاجة إلى كل بيان وربطه بكل هدف من أهداف المعالجة أو غيرها من الوسائل.

ب- بذل العناية اللازمة بما يساهم في تحقيق الغرض من المعالجة دون جمع بيانات شخصية غير ضرورية.

٢- على جهة التحكم الاحتفاظ بالحد الأدنى من البيانات الشخصية اللازمة لتحقيق الغرض من المعالجة.

المادة العشرون: الإفصاح عن البيانات الشخصية

١- يشترط في الإفصاح عن البيانات التي تم جمعها من مصادر متاحة للعموم بناءً على الفقرة (٢) من المادة (الخامسة عشرة) من النظام ألا تكون إتاحتها للعموم قد تمت بشكل مخالف لأحكام النظام ولوائحه.

٢- فيما عدا الأحوال المنصوص عليها في الفقرتين (٣) و(٤) من المادة (الخامسة عشرة) من النظام، على جهة التحكم عند الإفصاح عن البيانات الشخصية مراعاة ما يلي:

أ- أن يرتبط طلب الإفصاح ارتباطاً وثيقاً بغرض أو موضوع محدد وواضح.

ب- بذل العناية اللازمة للمحافظة على خصوصية صاحب البيانات الشخصية أو أي فرد آخر.

ج- أن يقتصر الإفصاح على الحد الأدنى من البيانات الشخصية اللازمة لتحقيق الغرض منه.

٣- على جهة التحكم عند الإفصاح عن البيانات الشخصية بناءً على طلب جهة عامة لأغراض أمنية أو لتنفيذ نظام آخر أو لاستيفاء متطلبات قضائية، أو إذا كان الإفصاح ضرورياً لحماية الصحة العامة أو السلامة العامة أو حماية حياة فرد أو أفراد معينين أو حماية صحتهم، القيام بالآتي:

أ- توثيق طلب الإفصاح.

ب- تحديد نوع البيانات الشخصية المطلوب الإفصاح عنها بشكل دقيق.

٤- فيما عدا ما نصت عليه الفقرة (٣) و(٤) من المادة (الخامسة عشرة) من النظام، على جهة التحكم عند الإفصاح عن بيانات شخصية مرتبطة ببيانات شخص آخر غير صاحبها الالتزام ببذل العناية اللازمة وتوفير الضمانات الكافية للمحافظة على خصوصية الفرد الآخر وضمان عدم انتهاكها، ومن ذلك مراعاة الخطوات الآتية:

أ- الموازنة بين حقوق صاحب البيانات الشخصية وحقوق الشخص الآخر في كل حالة على حده.

ب- ترميز البيانات الشخصية التي تدل على هوية الشخص الآخر ما أمكن ذلك.

٥- على جهة التحكم عند إفصاحها عن البيانات الشخصية لتحقيق مصلحة مشروعة لجهة التحكم الالتزام بما نصت عليه المادة (السادسة عشرة) من هذه اللائحة.

٦- على جهة التحكم تضمين عمليات الإفصاح عن البيانات الشخصية في سجلات أنشطة معالجة البيانات الشخصية وتوثيق تواريخها وطرقها والغرض منها.

المادة الحادية والعشرون: ضوابط معالجة البيانات الشخصية لأغراض المصلحة العامة

على الجهة العامة عند جمعها للبيانات الشخصية من غير صاحبها مباشرة أو معالجتها لغرض آخر غير الذي جمعت من أجله أو طلب الإفصاح عنها لتحقيق مصلحة عامة الالتزام بما يلي:

١- التأكد من أن ذلك يعد ضرورياً لتحقيق مصلحة عامة محددة بشكل واضح.

٢- أن تتصل المصلحة العامة بالاختصاصات المقررة لها نظاماً.

٣- اتخاذ الوسائل المناسبة للحد من الأضرار التي قد تنتج عن ذلك، بما في ذلك وضع الضوابط الإدارية والتقنية اللازمة لضمان التزام منسوبيها بأحكام المادة (الحادية والأربعون) من النظام.

٤- تضمين تلك العمليات في سجلات أنشطة معالجة البيانات الشخصية.

٥- جمع ومعالجة الحد الأدنى اللازم من البيانات الشخصية لتحقيق الغرض.

المادة الثانية والعشرون: تصحيح البيانات الشخصية

١- يُقصد بأنواع تصحيح البيانات الشخصية المشار إليها في الفقرة (٢) من المادة (السابعة عشرة) من النظام؛ تصحيح بيانات خاطئة، أو إكمال بيانات ناقصة، أو تحديث بيانات سابقة.

٢- على جهة التحكم عند تصحيح البيانات الشخصية الالتزام بما يلي:

أ- ضمان دقة وسلامة البيانات الشخصية من خلال فحص ومراجعة الوثائق الداعمة إن اقتضت الضرورة ذلك.

ب- إشعار الجهات التي أُفصح لها عن البيانات الشخصية دون تأخير.

ج- إشعار صاحب البيانات الشخصية عند الانتهاء من التصحيح.

د- توثيق كافة التحديثات التي أجريت على البيانات الشخصية.

٣- في حال تبيّن لجهة التحكم أن البيانات الشخصية غير صحيحة أو غير مكتملة وكان من شأن ذلك إحداث أضرار على صاحب البيانات الشخصية؛ القيام بإيقاف المعالجة لحين تحديث أو تصحيح البيانات.

٤- مع مراعاة الفقرة (٢) من هذه المادة، على جهة التحكم عند علمها بعدم صحة أو حداثة البيانات الشخصية العمل على تصحيحها أو إتمامها أو تحديثها وفق الوسائل المتاحة لديها دون تأخر.

٥- على جهة التحكم اتخاذ الإجراءات التنظيمية والإدارية والتقنية المناسبة لتفادي آثار معالجة البيانات الشخصية غير الصحيحة أو غير المكتملة أو غير المحدثة، ومن ذلك ما يأتي:

أ- وضع وتحديث السياسات والإجراءات الداخلية بما يتوافق مع أحكام النظام وهذه اللائحة، بما في ذلك إجراءات تمكن أصحاب البيانات الشخصية من ممارسة حقهم في طلب التصحيح وفق ما نص عليه النظام وهذه اللائحة.

ب- المراجعة الدورية لدقة وحداثة البيانات الشخصية.

المادة الثالثة والعشرون: أمن المعلومات

على جهة التحكم اتخاذ التدابير التنظيمية والإدارية والتقنية اللازمة لضمان أمن البيانات الشخصية وخصوصية أصحابها، والالتزام بالآتي:

١. تطبيق التدابير الأمنية والتقنية الضرورية للحد من المخاطر الأمنية لحدوث تسرب البيانات الشخصية.

٢. الالتزام بالضوابط والمعايير والقواعد ذوات الصلة الصادرة عن الهيئة الوطنية للأمن السيبراني، أو أفضل ممارسات ومعايير الأمن السيبراني المتعارف عليها في حال كانت جهة التحكم غير ملزمة بتطبيق الضوابط والمعايير والقواعد الصادرة عن الهيئة الوطنية للأمن السيبراني.

المادة الرابعة والعشرون: الإشعار عن حوادث تسرب البيانات الشخصية

١- تُشعر جهة التحكم الجهة المختصة في حالة وقوع حادثة تسرّب للبيانات الشخصية خلال مدة لا تتجاوز (٧٢) ساعة من وقت علمها بالحادثة، إذا كان من شأن تلك الحادثة الإضرار بالبيانات الشخصية أو صاحب البيانات الشخصية أو كانت تتعارض مع حقوقه أو مصالحه، على أن يتضمن الإشعار ما يأتي:

أ- وصف لحادثة تسرب البيانات الشخصية، على أن يتضمن وقتها وتاريخها وكيفية وقوعها ووقت علم جهة التحكم بها.

ب- الفئات والأعداد الفعلية أو التقريبية لأصحاب البيانات الشخصية المعنيين، ونوع البيانات الشخصية.

ج- وصف للمخاطر التي قد تنتج عن الحادثة، بما في ذلك مستوى الأثر الفعلي أو المحتمل الذي قد يلحق بالبيانات الشخصية وأصحاب البيانات الشخصية، والإجراءات والتدابير التي تم اتخاذها من قبل جهة التحكم للمنع أو الحد من آثار تلك المخاطر وتخفيفها، والتدابير المستقبلية التي ستتخذها جهة التحكم لمنع تكرار الحادثة.

د- بيان إذا تم أو سيتم إشعار صاحب البيانات الشخصية بتسرب بياناته الشخصية، وفقاً لما نصت عليه الفقرة (٥) من هذه المادة.

هـ- بيانات التواصل لجهة التحكم أو مسؤول حماية البيانات الشخصية لديها -إن وجد- أو أي مسؤول آخر تتوافر لديه معلومات فيما يخص الحادثة محل الإشعار.

٢- إذا لم تتمكن جهة التحكم من تقديم أي من البيانات المطلوبة خلال مدة لا تتجاوز (٧٢) ساعة من وقت علمها بتسرب البيانات الشخصية وفقاً لأحكام الفقرة (١) من هذه المادة، فعليها أن تُقدمها في أقرب وقت ممكن مع إرفاق مبررات التأخير.

٣- على جهة التحكم الاحتفاظ بنسخة من التقارير المقدمة إلى الجهة المختصة وفقاً لأحكام الفقرة (١) من هذه المادة، وتوثيق التدابير التصحيحية المتخذة فيما يتعلق بتسرب البيانات الشخصية، وأي مستندات أو وثائق داعمة ذوات علاقة.

٤- لا تخل أحكام هذه المادة بالتزامات جهة التحكم أو المعالجة بتقديم أي بلاغ أو إشعار عن حوادث تسرب البيانات بموجب ما يصدر عن الهيئة الوطنية للأمن السيبراني أو أي أنظمة ولوائح معمول بها في المملكة.

٥- على جهة التحكم دون تأخير غير مبرر إشعار صاحب البيانات الشخصية بحادثة تسرب بياناته الشخصية، إذا كان من شأنها أن ترتب ضرراً على بياناته أو تتعارض مع حقوقه أو مصالحه، على أن يكون الإشعار بلغة مبسطة وواضحة، وأن يتضمن ما يأتي:

أ- وصف لحادثة تسرب بياناته الشخصية.

ب- وصف المخاطر المحتملة الناشئة عن تسرب بياناته الشخصية، والتدابير المتخذة لمنع تلك المخاطر أو الحد منها وتخفيف آثارها.

ج- اسم وبيانات التواصل لجهة التحكم ومسؤول حماية البيانات لديها -إن وجد- أو أي وسائل تواصل أخرى مناسبة مع جهة التحكم.

د- التوصيات أو النصائح التي قد تساعد صاحب البيانات الشخصية على اتخاذ الإجراءات الملائمة لتجنب المخاطر المحددة أو تخفيف آثارها.

المادة الخامسة والعشرون: تقويم الأثر

١- يجب على جهة التحكم أن تعد تقويماً مكتوباً وموثقاً للآثار والمخاطر التي قد تلحق بصاحب البيانات الشخصية نتيجة معالجة البيانات الشخصية، ويتم إجراء تقويم الأثر في الأحوال التالية:

أ- معالجة البيانات الشخصية الحساسة.

ب- جمع أو مقارنة أو ربط مجموعتين أو أكثر من مجموعات البيانات الشخصية التي تم الحصول عليها من مصادر مختلفة.

ج- أن يتضمن نشاط جهة التحكم -على نطاق واسع أو بصورة متكررة- معالجة بيانات شخصية لناقصي أو عديمي الأهلية، أو عمليات المعالجة التي تتطلب بطبيعتها مراقبة مستمرة لأصحاب البيانات الشخصية، أو معالجة بيانات شخصية باستخدام تقنيات ناشئة، أو اتخاذ قرارات مبنية على المعالجة الآلية للبيانات الشخصية.

د- تقديم منتج أو خدمة تتضمن معالجة البيانات الشخصية التي من المحتمل أن تشكل أضراراً جسيمة على خصوصية أصحاب البيانات الشخصية.

٢- يجب أن يحتوي تقويم الأثر على العناصر الآتية كحد أدنى:

أ- الغرض من المعالجة والمسوغ النظامي لها.

ب- وصف لطبيعة المعالجة التي سيتم تنفيذها، وأنواع ومصادر البيانات الشخصية محل المعالجة وأي جهات سيتم الإفصاح لها عن البيانات الشخصية.

ج- وصف لنطاق المعالجة الذي يحدد نوع البيانات الشخصية والنطاق الجغرافي للمعالجة.

د- وصف لسياق المعالجة الذي يحدد العلاقة بين أصحاب البيانات الشخصية وجهة التحكم وجهات المعالجة وأي ظروف أخرى ذوات صلة.

هـ- ضرورة وتناسب التدابير المتبعة لتمكين جهة التحكم وجهات المعالجة من معالجة الحد الأدنى من البيانات الشخصية المطلوبة لتحقيق أغراض المعالجة.

و- الآثار المترتبة على المعالجة بناءً على شدة تأثيرها مادياً ومعنوياً واحتمال حدوث أي آثار سلبية على أصحاب البيانات الشخصية، ويتضمن ذلك أي آثار نفسية أو اجتماعية أو جسدية أو مالية واحتمال حدوث أي منها.

ز- التدابير التي ستتخذ لمنع المخاطر والحد منها.

ح- مدى ملاءمة التدابير المتبعة لتفادي المخاطر المحددة.

٣- على جهة التحكم تقديم نسخة من تقويم الأثر إلى أي جهة معالجة تتصرف نيابة عنها فيما يتعلق بالمعالجة ذات الصلة.

٤- على جهة التحكم -في حال انتهت نتائج التقويم المشار إليه في هذه المادة إلى أن عملية المعالجة ستؤدي إلى الإضرار بخصوصية أصحاب البيانات الشخصية- القيام بمعالجة الأسباب التي دعت إلى ذلك وإعادة إجراء التقويم.

المادة السادسة والعشرون: معالجة البيانات الصحية

على جهة التحكم اتخاذ الإجراءات والوسائل التنظيمية والتقنية والفنية والإدارية الكفيلة بالمحافظة على البيانات الصحية من أي استعمال غير مشروع، أو من إساءة استخدامها، أو استخدامها لغير الغرض الذي جُمعت من أجله، أو تسربها، وأي إجراءات أو وسائل تضمن المحافظة على خصوصية أصحابها، وعليها بصفة خاصة اتخاذ الضوابط والإجراءات الآتية:

١- تبني وتطبيق الاشتراطات والضوابط الصادرة عن وزارة الصحة والمجلس الصحي السعودي والبنك المركزي السعودي ومجلس الضمان الصحي والجهات الأخرى ذوات العلاقة بتنظيم الخدمات الصحية وخدمات التأمين الصحي، والتي تبين مهام ومسؤوليات منسوبي مقدمي الرعاية الصحية،

وشركات التأمين الصحي، وشركات إدارة مطالبات التأمين الصحي ومن تتعاقد معهم ممن يباشرون عمليات معالجة البيانات الصحية.

٢- تضمين الأحكام الواردة في النظام ولوائحه في السياسات الداخلية لدى جهة التحكم.

٣- توزيع المهام والمسؤوليات بين الموظفين أو العاملين بطريقة تحول دون تداخل الاختصاصات وتشتيت المسؤولية ومراعاة تدرج إمكانية الوصول إلى البيانات بين الموظفين أو العاملين بما يكفل أعلى درجة من المحافظة على خصوصية أصحاب البيانات الشخصية.

٤- توثيق كافة مراحل معالجة البيانات الصحية وتوفير إمكانية تحديد الشخص المسؤول عن كل مرحلة منها.

٥- أن يتضمن اتفاق جهة التحكم مع جهات المعالجة -لتنفيذ أعمال أو مهام تتعلق بمعالجة البيانات الصحية -أحكاماً تلزمها باتباع الإجراءات والوسائل المنصوص عليها في هذه المادة.

٦- قصر عمليات معالجة البيانات على الحد الأدنى اللازم لتقديم خدمات أو منتجات الرعاية الصحية، أو برامج التأمين الصحي.

المادة السابعة والعشرون: معالجة البيانات الائتمانية

مع عدم الإخلال بأحكام نظام المعلومات الائتمانية، على جهة التحكم اتخاذ الإجراءات والوسائل التنظيمية والتقنية والفنية والإدارية التي تضمن المحافظة على البيانات الائتمانية من أي استعمال غير مشروع، أو

إساءة استخدامها، أو الاطلاع عليها من غير المصرح لهم، أو استخدامها لغير الغرض الذي جُمعت من أجله، أو تسربها، وعليها اتخاذ الضوابط والإجراءات الآتية:

١- تبني وتطبيق الاشتراطات والضوابط الصادرة من البنك المركزي السعودي والجهات الأخرى ذوات العلاقة، التي تبين مهام ومسؤوليات منسوبي المنشآت التي تقدم خدمات المعلومات الائتمانية ومن تتعاقد معهم من الذين يباشرون عمليات معالجة البيانات الائتمانية.

٢- تلتزم جهة التحكم بالحصول على موافقة صاحب البيانات الشخصية وإشعاره عند وجود أي طلب للإفصاح عن بياناته الائتمانية، وذلك وفق ما ينص عليه نظام المعلومات الائتمانية، مع مراعاة ما نصت عليه الفقرة الفرعية (د) من الفقرة (١) من المادة (الحادية عشرة) من اللائحة.

المادة الثامنة والعشرون: معالجة البيانات لأغراض دعائية أو توعوية

١- على جهة التحكم قبل إرسال مواد دعائية أو توعوية الحصول على موافقة المتلقي المستهدف، وذلك في حال عدم وجود تعامل مسبق بين جهة التحكم والمتلقي المستهدف.

٢- تكون شروط موافقة المتلقي المستهدف بالمواد الدعائية أو التوعوية وفقاً لما يلي:

أ- أن تصدر الموافقة بإرادة حرة، وألّا تُستخدم أي طرق مُضللة في سبيل الحصول عليها.

ب- تمكين المتلقي من تخصيص الخيارات المتعلقة بالمواد الدعائية أو التوعوية محل الموافقة.

ج- أن توثّق موافقة المتلقي المستهدف بوسائل تتيح التحقق منها مستقبلاً.

٣- دون الإخلال بنظام الاتصالات وتقنية المعلومات والأنظمة الأخرى ذوات الصلة، على جهة التحكم قبل استخدام وسائل الاتصال الشخصية -بما فيها العناوين البريدية والإلكترونية- الخاصة بصاحب البيانات الشخصية لغرض إرسال مواد دعائية أو توعوية، الالتزام بما يأتي:

أ- ذكر اسم الجهة المرسلة بوضوح دون أي إخفاء لهويتها.

ب- توفير آلية تمكن صاحب البيانات الشخصية من إيقاف تلقي تلك المواد الدعائية أو التوعوية متى ما رغب في ذلك، وأن تكون إجراءات إيقاف تلقي المواد الدعائية أو التوعوية سهلة ومبسطة ومماثلة أو أكثر سهولةً من إجراءات الحصول على الموافقة على استقبالها.

ج- التوقف عن إرسال الرسائل الدعائية أو التوعوية فور تلقيها طلب المتلقي المستهدف بذلك.

د- أن يكون إيقاف تلقي المواد الدعائية أو التوعوية دون مقابل مالي.

هـ- الاحتفاظ بما يثبت موافقة المتلقي المستهدف على تلقي المواد الدعائية أو التوعوية.

المادة التاسعة والعشرون: التسويق المباشر

١- دون الإخلال بنظام الاتصالات وتقنية المعلومات والأنظمة الأخرى ذوات الصلة، على جهة التحكم قبل القيام بمعالجة البيانات الشخصية لأغراض التسويق المباشر الالتزام بالآتي:

أ- الحصول على موافقة صاحب البيانات الشخصية وفقاً لأحكام المادة (الحادية عشرة) من هذه اللائحة.

ب- توفير آلية تمكن صاحب البيانات الشخصية من إيقاف تلقي المواد التسويقية متى ما رغب في ذلك، وأن تكون إجراءات إيقاف تلقي المواد التسويقية سهلة ومبسطة ومماثلة أو أكثر سهولةً من إجراءات الحصول على الموافقة على استقبالها.

٢- عند إرسال مواد التسويق المباشر لصاحب البيانات الشخصية، يجب ذكر اسم الجهة المرسلة بوضوح دون أي إخفاء لهويتها.

٣- في حال عدول صاحب البيانات الشخصية عن موافقته على التسويق المباشر، فيكون على جهة التحكم التوقف دون تأخير غير مبرر عن توجيه المواد التسويقية إليه.

المادة الثلاثون: جمع ومعالجة البيانات لأغراض علمية أو بحثية أو إحصائية

على جهة التحكم عند جمع أو معالجة البيانات الشخصية لأغراض علمية أو بحثية أو إحصائية دون موافقة صاحبها الالتزام بالآتي:

١. تحديد الأغراض العلمية أو البحثية أو الإحصائية بشكل واضح ودقيق في سجلات أنشطة معالجة البيانات الشخصية.
٢. اتخاذ التدابير اللازمة لضمان جمع البيانات الشخصية وفق الحد الأدنى اللازم لتحقيق الأغراض المحددة.
٣. ترميز البيانات الشخصية التي تجري معالجتها، في الأحوال التي لا يؤثر ذلك على تحقيق الغرض من المعالجة .
٤. اتخاذ التدابير اللازمة لضمان ألا ترتب المعالجة أي آثار سلبية على حقوق ومصالح صاحب البيانات الشخصية.

المادة الحادية والثلاثون: تصوير أو نسخ الوثائق الرسمية التي تحدد هوية صاحبها

دون الإخلال بالأنظمة ذوات العلاقة، على جهة التحكم الامتناع عن تصوير الوثائق الرسمية -الصادرة من الجهات العامة- التي تحدد هوية صاحب البيانات الشخصية أو نسخها، إلا بناءً على طلب من جهة عامة

مختصة، أو متى ما كان ذلك تنفيذاً لأحكام نظام، وعلى جهة التحكم توفير الحماية اللازمة لتلك الوثائق، وإتلافها فور انتهاء الغرض منها، ما لم يكن هناك متطلب نظامي للاحتفاظ بها.

المادة الثانية والثلاثون: مسؤول حماية البيانات الشخصية

١- تقوم جهة التحكم بتعيين أو تحديد شخص أو أكثر ليكون مسؤولاً عن حماية البيانات الشخصية، وذلك في أي من الحالات الآتية:

أ- أن تكون جهة التحكم جهة عامة تقدم خدمات 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 شخصية حساسة.

٢- مع مراعاة متطلبات الفقرة (١) من هذه المادة يجوز أن يكون مسؤول حماية البيانات الشخصية مسؤولاً أو موظفاً لدى جهة التحكم أو متعاقداً خارجياً.

٣- يتولى مسؤول حماية البيانات الشخصية في جهة التحكم متابعة تنفيذ أحكام النظام ولوائحه، ومراقبة الإجراءات المعمول بها داخل جهة التحكم والإشراف عليها، وتلقي الطلبات المتعلقة بالبيانات الشخصية وفقاً لأحكام النظام ولوائحه، ويتولى على وجه الخصوص الآتي:

أ- العمل كمسؤول اتصال مباشر مع الجهة المختصة وتنفيذ قراراتها وتعليماتها فيما يتصل بتطبيق أحكام النظام ولوائحه.

ب- الإشراف على إجراءات تقويم الأثر وتقارير المراجعة والتدقيق المتعلقة بضوابط حماية البيانات الشخصية، وتوثيق نتائج التقويم وإصدار التوصيات اللازمة لذلك.

ج- تمكين صاحب البيانات الشخصية من ممارسة حقوقه المنصوص عليها في النظام.

د- إشعار الجهة المختصة عن حوادث تسرب البيانات الشخصية.

هـ- الرد على الطلبات المقدمة من صاحب البيانات الشخصية، والرد على الجهة المختصة في الشكاوى المقدمة وفقاً لأحكام النظام واللائحة.

و- متابعة قيد وتحديث سجلات أنشطة معالجة البيانات الشخصية لدى جهة التحكم.

ز- معالجة المخالفات المتعلقة بالبيانات الشخصية داخل جهة التحكم، واتخاذ الإجراءات التصحيحية حيالها.

٤- تصدر الجهة المختصة قواعد تعيين مسؤول حماية البيانات الشخصية، على أن تتضمن القواعد الأحوال التي يجب فيها تعيين مسؤول حماية البيانات الشخصية.

المادة الثالثة والثلاثون: سجلات أنشطة معالجة البيانات الشخصية

١- على جهة التحكم الاحتفاظ بسجل أنشطة معالجة البيانات الشخصية أثناء فترة استمرار عمليات معالجة البيانات الشخصية، إضافة إلى خمس سنوات تبدأ من تاريخ انتهاء نشاط معالجة البيانات الشخصية.

٢- يجب أن تكون سجلات أنشطة معالجة البيانات الشخصية مكتوبةً.

٣- على جهة التحكم ضمان دقة وحداثة سجلات أنشطة معالجة البيانات الشخصية.

٤- على جهة التحكم إتاحة سجلات أنشطة معالجة البيانات الشخصية للجهة المختصة عند طلبها.

٥- يتضمن سجل أنشطة معالجة البيانات الشخصية المحتويات الآتية كحد أدنى:

أ- اسم جهة التحكم وتفاصيل الاتصال المتعلقة بها.

ب- بيانات مسؤول حماية البيانات الشخصية في الأحوال التي تتطلب ذلك وفقاً لما نصت عليه الفقرة (١) من المادة (الثانية والثلاثون) من هذه اللائحة.

ج- أغراض معالجة البيانات الشخصية.

د- وصف لفئات البيانات الشخصية التي تتم معالجتها، وفئات أصحاب البيانات الشخصية.

هـ- مدد الاحتفاظ الخاصة بكل من فئات البيانات الشخصية، ما أمكن ذلك.

و- فئات الجهات التي يتم الإفصاح لها عن البيانات الشخصية.

ز- وصف لعمليات نقل البيانات الشخصية إلى خارج المملكة، بما في ذلك المسوغات النظامية لعمليات النقل والجهات التي يتم نقل البيانات الشخصية إليها.

ح- وصف الإجراءات والوسائل التنظيمية والإدارية والتقنية التي تضمن المحافظة على البيانات الشخصية، ما أمكن ذلك.

٦- تضع الجهة المختصة نماذج استرشادية لسجلات أنشطة معالجة البيانات الشخصية.

المادة الرابعة والثلاثون: السجل الوطني لجهات التحكم

تصدر الجهة المختصة قواعد التسجيل في السجل الوطني لجهات التحكم، على أن تتضمن القواعد تحديد جهات التحكم الملزمة بالتسجيل.

المادة الخامسة والثلاثون: جهات منح شهادات الاعتماد

تصدر الجهة المختصة القواعد المنظمة للترخيص لجهات تتولى إصدار شهادات الاعتماد لجهات التحكم وجهات المعالجة وفق ما نصت عليه الفقرة (٢) من (المادة الثالثة والثلاثون) من النظام، وتُنسّق الجهة المختصة مع هيئة الحكومة الرقمية فيما يتعلق بالترخيص للجهات التي تقدّم الخدمات نيابةً عن الجهات الحكومية.

المادة السادسة والثلاثون: التدقيق والفحص

١- تهدف عمليات التدقيق والفحص إلى التأكد من أن الجهة تقوم بحماية البيانات الشخصية بشكل ملائم، وذلك من خلال تدقيق وفحص أنشطة معالجة البيانات الشخصية المتبعة لدى الجهة، والضوابط والإجراءات ذوات الصلة بها، ورصد أي فجوات لديها فيما يتعلق بتطبيق النظام ولوائحه.

٢- عند القيام بتدقيق وفحص أنشطة معالجة البيانات الشخصية، يتم الالتزام بما يلي:

أ- تقديم هذه الخدمات بشكل مستقل وفق المعايير المهنية المتبعة.

ب- وضع الإجراءات والضوابط الإدارية والتنظيمية اللازمة للتأكد من دقة وسلامة ما يصدر عنها.

٣- تصدر الجهة المختصة القواعد المنظمة للترخيص لجهات تتولى التدقيق أو الفحص لأنشطة معالجة البيانات الشخصية وفق ما نصت عليه الفقرة (٣) من (المادة الثالثة والثلاثين) من النظام،

وتُنسّق الجهة المختصة مع هيئة الحكومة الرقمية فيما يتعلق بالترخيص للجهات التي تقدّم الخدمات نيابةً عن الجهات الحكومية.

المادة السابعة والثلاثون: تقديم ومعالجة الشكاوى

١- لصاحب البيانات الشخصية تقديم شكوى إلى الجهة المختصة خلال مدة لا تتجاوز (٩٠) يوماً من تاريخ الحادثة محل الشكوى أو علم صاحب البيانات الشخصية بها، وللجهة المختصة تقدير قبول

الشكوى من عدمه بعد تجاوز هذه المدة في الحالات التي يتبين لها وجود أسباب واقعية منعت صاحب البيانات الشخصية من تقديم شكواه خلال هذه الفترة.

٢- تتلقى الجهة المختصة الشكاوى الواردة إليها من خلال الوسيلة التي تبيّنها، وذلك وفق إجراءات تكفل السرعة والجودة في التعامل معها.

٣- تقيد الجهة المختصة الشكاوى المقدمة في سجل يعد لهذا الغرض.

٤- يجب أن تتضمن الشكوى البيانات التالية:

أ- مكان وزمان المخالفة.

ب- اسم مقدمها، وهويته، وعنوانه، ورقم هاتفه.

ج- بيانات الجهة المشتكى ضدها.

د- وصف الفعل المخالف بشكل واضح ومحدد، والأدلة والمعلومات المقدمة مع الشكوى.

هـ- أي متطلبات أخرى تحددها الجهة المختصة.

٥- تتولى الجهة المختصة فحص ودراسة الشكاوى ومستنداتها، ولها التواصل مع مقدم الشكوى بحسب الحاجة إلى طلب المستندات والوثائق والمعلومات ذوات الصلة.

٦- تتولى الجهة المختصة اتخاذ الإجراءات اللازمة حيال الشكاوى الواردة إليها وتشعر مقدم الشكوى بالنتيجة التي انتهت إليها.

المادة الثامنة والثلاثون: النشر والنفاذ

تنشر هذه اللائحة في الجريدة الرسمية والموقع الرسمي للجهة المختصة، ويعمل بها من تاريخ نفاذ النظام.