وزارة العدل والشئون الإسلامية والأوقاف

قرار رقم (٤٣) لسنة ٢٠٢٢
بتحديد الاشتراطات التي يتعين توافرها في التدابير الفنية والتنظيمية الكفيلة بحماية البيانات الشخصية

وزير العدل والشئون الإسلامية والأوقاف:

بعد الاطلاع على قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨، وعلى الأخص المادة (٨) منه،

وعلى المرسوم رقم (٧٨) لسنة ٢٠١٩ بتحديد الجهة الإدارية التي تتولى المهام والصلاحيات المقررة لهيئة حماية البيانات الشخصية،

وعلى القرار رقم (٤٢) لسنة ٢٠٢٢ بشأن نقل البيانات الشخصية إلى خارج مملكة البحرين،

وبناءً على عرض وكيل الوزارة للعدل والشئون الإسلامية،

قرر الآتي:

مادة (١)

التعريفات

في تطبيق أحكام هذا القرار، تكون للكلمات والعبارات الواردة فيه ذات المعانيَ المبيّنةَ في قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨، وتكون للكلمات والعبارات التالية المعانيَ المبيّنةَ قرينَ كُلٍّ منها، ما لم يقتض سياق النص خلاف ذلك:

القانون: قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

تصميم لحماية الخصوصية (Privacy by Design): طريقة نظام مُعالجة البيانات والتي تسعى إلى توفير أقصى درجات الخصوصية بشكل استباقي من خلال ضمان حماية البيانات تلقائياً في النظام التكنولوجي أو المُمارسة التجارية، وتطبيق تدابير الأمان في جميع مراحل المعالجة بشكل يتوقع مشاكل الخصوصية ويمنعها قبل حدوثها.

مادة (٢)

التدابير الفنية والتنظيمية الواجب تطبيقها في المُعالجة

لضمان مستوى كافٍ من الأمان عند معالجة البيانات، على مدير البيانات الالتزام بالتدابير

الفنية والتنظيمية التالية وتطبيقها كلها أو بعضها أثناء إجراء عمليات المعالجة، وذلك بناءً على طبيعة نطاق المعالجة أو سياقها أو أغراضها أو مخاطرها:

١- تطبيق تصميم لحماية الخصوصية (Privacy by Design) عند إعداد وتصميم واختيار واستخدام التطبيقات والخدمات والمنتجات القائمة على معالجة البيانات بأنواعها.

٢- وضع أطر حماية الخصوصية (privacy framework)، وذلك من خلال الهيكلية والممارسة والتعليمات المتعلقة بحماية البيانات في ضوء القانون والقرارات المعمول بها.

٣- الالتزام بتطبيق تدابير فعّالة للحد من مخاطر انتهاك الخصوصية في مواجهة عمليات أو محاولات الاختراق، ومنها على سبيل المثال تنظيم وضمان الوصول للبيانات المحفوظة، وحماية كلمات المرور، واستخدام برامج مكافحة الفيروسات وتطبيقات جدران الحماية (firewalls)، والامتثال لتراخيص البرمجيات، وتنظيم مُدة الاحتفاظ بالبيانات ومحوها، ووضع ضوابط لنسخ البيانات احتياطياً، ووضع بروتوكولات تقنية مُلائمة تكفل الوصول إلى المواقع الفعلية والنظم الافتراضية التي تُخزّن فيها البيانات.

٤- إجراء تقييم لمكامن الضعف والاختراق للبرامج الآلية (Vulnerability Assessment and Penetration Testing) وذلك بصورة دورية للتحقق من كفاءة التدابير الأمنية المعمول بها، وقياس مدى فعاليتها لتصحيح أي ثغرات أمنية والحد منها.

٥- وضع خطة فعّالة لمواجهة الحوادث والاختراقات الفُجائية في أنظمة معالجة البيانات بما يسمح باستمرارية تنفيذ أعمال المعالجة دون انقطاع.

٦- تحديد نطاق الصلاحية الممنوح لكل موظف كلٍ بحسب اختصاصه والمهام المكلف بها، بغرض توفير حماية وخصوصية عالية للبيانات مَحل المُعالجة.

وعلى مدير البيانات إحاطة الموظفين المعنيين بالمعالجة بالتدابير المذكورة في الفقرة السابقة، وذلك على نحو يكفل الامتثال لأحكام القانون والقرارات الصادرة تنفيذاً له.

مادة (٣)

تقييم أثر حماية البيانات (Data Protection Impact Assessment)

أ- يجوز لمدير البيانات إجراء تقييم لأثر حماية البيانات أثناء إجراءات المعالجة، مع مراعاة طبيعة المعالجة ونطاقها وسياقها وأغراضها ومخاطرها العالية على حقوق وحريات الأفراد، ويجوز أن يتناول تقييم واحد مجموعة من عمليات المعالجة المتشابهة التي تمثل مخاطر عالية مماثلة.

ب- يجوز لمدير البيانات أن يطلب مشورة من مراقب حماية البيانات في حال تم تعيينه، أثناء إجراء تقييم أثر حماية البيانات.

ج- على مدير البيانات إجراء تقييم أثر حماية البيانات أثناء إجراءات المعالجة في الحالات الآتية:

١- في حالات المعالجة الآلية للبيانات المشار إليها في البند (١) من المادة (٢٢) من القانون، أو عند إجراء مُعالجة آلية لإجراء تقييم منهجي وشامل للجوانب الشخصية المتعلقة بالأفراد ويشمل ذلك تحديد الصفات (profiling) التي تستند إليها القرارات التي تُنتج آثار قانونية تتعلق بالشخص الطبيعي أو تؤثر بشكل كبير فيه.

٢- المُعالجة على نطاق واسع للبيانات أو البيانات عالية الخطورة أو البيانات المتعلقة برفع الدعاوى الجنائية ومباشرتها وبالأحكام الصادرة فيها المشار إليها في المادة (٧) من القانون.

٣- المراقبة المنهجية لمنطقة متاحة للجمهور على نطاق واسع.

٤-معالجة البيانات بواسطة التسجيل البصري أو المعالجة الآلية لبيانات القياسات الحيوية.

د- يجب أن يحتوي التقييم لأثر حماية البيانات أثناء إجراءات المعالجة بحد أدنى على ما يأتي:

١-وصف منهجي لعمليات المعالجة موضوع التقييم وأغراضها، بما في ذلك - عند الاقتضاء- المصلحة المشروعة التي يسعى إليها مدير البيانات.

٢-تقييم أهمية وتناسب عمليات المعالجة فيما يتعلق بالأغراض.

٣-تقييم المخاطر على حقوق وحريات أصحاب البيانات.

٤-تقييم التدابير المتخذة لمواجهة المخاطر، بما في ذلك الضمانات والتدابير الأمنية والآليات الكفيلة بحماية البيانات من أجل الامتثال للقانون والقرارات الصادرة تنفيذاً له، مع مراعاة الحقوق والمصالح المشروعة لأصحاب البيانات وغيرهم من الأشخاص ذوي العلاقة.

هـ- يجب على مدير البيانات عند الاقتضاء استبيان آراء أصحاب البيانات أو من يمثلهم قانوناً بشأن أثر حماية البيانات أثناء المعالجة المستهدفة بالتقييم، وذلك دون المساس بحماية المصالح التجارية أو العامة أو أمن عمليات المعالجة.

مادة (٤)

الإخطار عن وقوع خرق أو انتهاك للبيانات

أ- يجب على مدير البيانات فتح قنوات اتصال تُتيح التواصل المباشر مع أصحاب البيانات أو من ينوب عنهم قانوناً للإبلاغ عن الخرق أو الانتهاكات.

ب- يلتزم مدير البيانات بتوثيق حالات خرق أو انتهاك البيانات، وبيان أسبابها، والآثار المترتبة على وقوعها، والإجراءات التصحيحية المُتخذة، ويجب عليه وضع إجراءات محددة لإخطار الهيئة بحدوث خرق أو انتهاك للبيانات خلال مدة لا تجاوز اثنان وسبعين ساعة من وقت اكتشافه، ما لم يكن من غير المحتمل أن يؤدي خرق البيانات إلى خطر يُهدد حقوق أصحاب البيانات.

وفي حال لم يلتزم المدير بإخطار الهيئة في المدة المحددة، يجب أن يكون الإخطار مشفوعاً بمبررات التأخير، وإذا لم يُبادر المدير بإخطار أصحابَ البيانات بحادثة الخرق، فللهيئة أن تُلزمه بذلك إذا ما ارتأت أن الحادثة قد تؤدي إلى مخاطر عالية.

ج- لا يُلزم مدير البيانات بإخطار صاحب البيانات بحادثة الخرق أو الانتهاك في الحالات الآتية:

١-إذا كانت البيانات التي تم اختراقها غير مفهومة لأي شخص غير مصرح له بالوصول إليها، كأن تكون مشفرة.

٢-اتخاذ المدير تدابير لاحقة تضمن عدم احتمال ظهور مخاطر عالية على حقوق وحريات أصحاب البيانات.

د- إذا كان إخطار صاحب البيانات يتطلب بذل جهود مُرهقة غير عادية، ففي هذه الحالة يكون إخطار صاحب البيانات بوسيلة علنية.

هـ- يجب أن يتضمن الإخطار بحادثة الخرق أو الانتهاك البيانات الآتية:

١- بالنسبة لأصحاب البيانات:

أ) نوع الخرق أو الانتهاك وطبيعته.

ب) تفاصيل البيانات التي تعرضت للخرق أو الانتهاك.

ج) توصيات للحد أو التخفيف من آثار الخرق أو الانتهاك.

٢- بالنسبة للهيئة:

أ) وصف طبيعة خرق أو انتهاك البيانات، بما في ذلك الفئات والعدد التقريبي لأصحاب البيانات المعنية والفئات والعدد التقريبي لسجلات البيانات المعنية متى كان ذلك ممكناً.

ب) بيانات ومعلومات الاتصال بمراقب البيانات أو أي نقطة اتصال أخرى من أجل الحصول على مزيد من المعلومات.

ج) وصف للآثار المحتملة للخرق أو لانتهاك البيانات.

د) وصف للتدابير المتخذة أو المُقترح اتخاذها من قبل مدير البيانات لمعالجة خرق أو انتهاك البيانات، بما في ذلك -عند الاقتضاء- التدابير المقترحة للتخفيف من الآثار السلبية المحتملة.

هـ) الإجراءات المتخذة لمعالجة السبب الرئيسي المؤدي للخرق، ومنع تكراره.

و- إذا لم يتمكن مدير البيانات من تقديم المعلومات المشار إليها في الفقرة (هـ) من هذه المادة في آن واحد، فيجوز له تقديمها على مراحل بشكل فوري دون أي تأخير.

مادة (٥)

التحقيق الداخلي

على مدير البيانات وضع قواعد واضحة للتحقيق الداخلي تهدف إلى كشف الأسباب التي أدت إلى خرق أو انتهاك البيانات، والوصول إلى الأشخاص المسئولين عن ذلك، ويجب توثيق تلك الإجراءات كتابياً، والاحتفاظ بما يَدُل أو يثبت حصول الخرق أو الانتهاك وتقديمه للهيئة أو الجهات القضائية إن لَزِمَ الأمر.

مادة (٦)

التعاقد مع مُعالج بيانات خارجي أو أي طرف ثالث

يجب على مدير البيانات عند التعاقد مع معالج بيانات خارجي أو أي طرف ثالث لنقل البيانات إليه، أن يراعي تضمين العقد المبرم مع أي منهم الأحكام المنصوص عليها في المادة (٥) من القرار رقم (٤٢) لسنة ٢٠٢٢ بشأن نقل البيانات الشخصية إلى خارج مملكة البحرين.

مادة (٧)

مُعالجة البيانات من قبل أكثر من مدير بيانات

بمراعاة الحصول على التصريح المسبق طبقاً للمادة (١٥) من القانون، في حال تمت مُعالجة البيانات من قبل أكثر من مدير بيانات بصورة مشتركة، يجب على مديري البيانات التقيد بما يأتي:

١- الاتفاق الكتابي فيما بينهم على دور ومسؤوليات كل منهم، لضمان الامتثال للقانون والقرارات الصادرة تنفيذاً له.

٢- الإفصاح لأصحاب البيانات عن معالجة بياناتهم بصورة مشتركة من قبل أكثر من مدير بيانات لضمان وتعزيز الشفافية.

٣- تحديد مدير بيانات واحد من بينهم يكون نقطة الاتصال مع أصحاب البيانات، مع تحديد آلية التواصل.

مادة (٨)

التدريب المستمر

يجب على مدير البيانات توفير برامج تدريبية دورية لضمان إلمام الموظفين القائمين على مُعالجة البيانات بالقانون والقرارات الصادرة تنفيذاً له والتدابير الفنية والتنظيمية والبروتوكولات والإجراءات الخاصة بها.

مادة (٩)

النفاذ

على وكيل الوزارة للعدل والشئون الإسلامية تنفيذ أحكام هذا القرار، ويُعمل به من اليوم التالي لتاريخ نشره في الجريدة الرسمية.

وزير العدل
والشئون الإسلامية والأوقاف
خالد بن علي بن عبدالله آل خليفة

صدر بتاريخ: ١٤ شعبان ١٤٤٣هـ
الموافق: ١٧ مارس ٢٠٢٢م