تعليمات التدابير الأمنية التقنية والتنظيمية لسنة ٢٠٢٥ صادرة بموجب الفقرة (ب) من المادة (٨) من قانون حماية البيانات الشخصية رقم (٢٤) لسنة ٢٠٢٣

المادة ١- تسمى هذه التعليمات (تعليمات التدابير الأمنية والتقنية والتنظيمية لسنة ٢٠٢٥) ويعمل بها من تاريخ نشرها في الجريدة الرسمية.

المادة ٢- أ-يكون للكلمات والعبارات التالية حيثما وردت في هذه التعليمات المعاني المخصصة لها أدناه ما لم تدل القرينة على غير ذلك:-

القانون : قانون حماية البيانات الشخصية.

الإخفاء : حجب البيانات التي تدل على هوية الشخص المعني بشكل يتعذر معه تحديد هويته.

المحو : إزالة البيانات والنسخ والنسخ الاحتياطية كافة من قواعد البيانات والأنظمة.

التشفير : عملية تحويل البيانات إلى شكل غير قابل للقراءة أو الفهم وذلك باستخدام خوارزميات ومفتاح سري.

الترميز : تحويل البيانات التي تدل على هوية الشخص المعني إلى رموز تجعل من المتعذر تحديدهويته دون استخدام بيانات إضافية.

التدابير الأمنية : مجموعة من الإجراءات يتم اتخاذها لضمان أمن وسلامة قواعد البيانات والأنظمة التي تعالج البيانات.

التدابير التقنية : مجموعة من الإجراءات يتم اتخاذها لتأمين قواعد البيانات والأنظمة التي تعالجها ضد مخاطر استعمالها أو من الوصول غير المشروع أو المصرح به.

التدابير التنظيمية : مجموعة من الإجراءات يتم اتخاذها لتأمين قواعد البيانات والأنظمة التي تعالجها عبر وضع أُطر تنظيمية للمؤسسات والمنظمات وسلوك العاملين فيها.

ب-تعتمد التعاريف الواردة في القانون حيثما ورد النص عليها في هذه التعليمات ما لم تدل القرينة على غير ذلك.

المادة ٣- يلتزم المسؤول بتنفيذ التدابير الأمنية التالية على قواعد البيانات وذلك بحسب طبيعة المعالجة ونطاقها وأهميتها:

أ- تهيئة المكان المناسب من الناحية الأمنية بما في ذلك وضع كاميرات المراقبة وأجهزة الإنذار اللازمة وكل ما يمكنه الحفاظ على البيانات والأجهزة والمعدات والمعلومات بشكل آمن ومحمي من خارج المبنى وجميع مداخله بطريقة محصنة.

ب- مراقبة عمليات الدخول والخروج من المبنى الذي يتم فيه إجراء عملية المعالجة وعلى الأنظمة والشبكات التي تحتوي على البيانات موضوع المعالجة.

ج-ضبط عملية الوصول المصرح به إلى مكان المعالجة ومنع أي شخص ليس له علاقة بعملية المعالجة من الوصول إلى المبنى الذي تتم فيه المعالجة.

د-التخلص من كل ما له علاقة بالبيانات بما يضمن عدم التعرف على هوية الشخص المعني و يكفل الحفاظ على الخصوصية.

هـ-وضع نسخ قواعد البيانات الاحتياطية في مكان آمن.

المادة ٤- يلتزم المسؤول بتنفيذ التدابيرالتقنية التالية على قواعد البيانات وذلك بحسب طبيعة المعالجة ونطاقها وأهميتها وبما يتناسب مع مخاطر معالجتها:

أ- الالتزام بتطبيق تدابير فعالة للحد من مخاطر تسريب البيانات وانتهاك الخصوصية لمواجهة عمليات او محاولات الاختراق كتنظيم قواعد البيانات المحفوظة وضمان الوصول اليها، وحماية كلمات المرور، واستخدام برامج مكافحة الفيروسات وتطبيقات أنظمة جدران الحماية والامتثال لتراخيص البرمجيات، والالتزام بالتشريعات الناظمة لمدد الاحتفاظ بها ومحوها ووضع ضوابط للنسخ الاحتياطية من قواعد البيانات ووضع بروتوكولات تقنية ملائمة تكفل الوصول الى المواقع الفعلية والنظم الافتراضية التي تخزن فيها قواعد البيانات.

ب- إجراء فحوصات دورية ملائمة مرة واحدة سنويا على الأقل لتقييم مواطن الضعف والاختراق في البيئة التقنية المستخدمة لمعالجة البيانات للتحقق من كفاءة التدابير الأمنية والتقنية والتنظيمية المعمول بها وقياس مدى فعاليتها لتصحيح أي ثغرات أمنية والحد منها.

ج-ترميز أو تشفير البيانات وقواعد البيانات أثناء تناقلها أو تخزينها أو في الحالات التي تتطلب ذلك، على أن يتم اختيار تقنية الترميز أو التشفير الذي يتناسب مع طبيعة وأهمية البيانات وقواعد البيانات ودرجة الحماية المطلوبة.

د-القدرة على الوصول الى قواعد البيانات واستعادتها وضمان توافريه عالية للبيانات في الوقت المناسب في حال حدوث خلل أو إخلال بأمن وسلامة البيانات.

هـ-حماية النسخ الاحتياطية من قواعد البيانات من الفقدان العرضي او التدمير او الضرر وضمان إمكانية الرجوع اليها واستعادتها عند الحاجة إليها.

و-ضبط الأنظمة وقواعد البيانات بحيث تكون قادرة على تحديد الصلاحيات والأدوار المحددة للمستخدمين.

ز-اتخاذ التدابير التقنية الملائمة وفقا للتطورات التكنولوجية وضمان مواكبتها للتحديثات وتجديد الإجراءات المتخذة بشكل دوري.

المادة٥- يلتزم المسؤول بتنفيذ التدابير التنظيمية التالية على قواعد البيانات وذلك بحسب طبيعة المعالجة ونطاقها وأهميتها:

أ- وضع السياسات التي تخص حماية وخصوصية البيانات.

ب-الحد من جمع البيانات الشخصية ليقتصر فقط على ما هو متعلق بشكل مباشر وضروري لتحقيق الغرض من المعالجة والاحتفاظ بهذه البيانات فقط للمدة اللازمة لتحقيق الغرض المحدد.

ج-توفير برامج تدريبية دورية تضمن إلمام الموظفين القائمين على معالجة البيانات بما يكفل ضمان أمان البيانات وفقاً لأحكام القانون والأنظمة والتعليمات الصادرة بمقتضاه.

د-تحديد نطاق صلاحية الموظف المعني بمعالجة البيانات بما لا يتجاوز نطاق عمله وفي حدود ضيقة وبما تقتضيه طبيعة عمله بالاطلاع مباشرة على تلك البيانات.

هـ-حفظ مراحل عملية المعالجة كافة وتوثيقها.

و-تطبيق آليات وإجراءات للتحقق من هوية مقدم الطلب قبل الموافقة على طلب الوصول أو المحو أو التحديث أو الاطلاع أو التصحيح أو الإضافة على البيانات.

ز-وضع خطط استجابة لمواجهة الحوادث السيبرانية والاختراقات التي تحصل في عملية معالجة البيانات وبما لا يخالف تعليمات وإجراءات وضوابط المركز الوطني للأمن السيبراني وبشكل يكفل استكمال عملية المعالجة بعد حصول الحادث.

ح-الالتزام بتطبيق تدابير واجراءات تحد من مخاطر انتهاك حق الخصوصية في مواجهة الحوادث السيبرانية والاختراقات وبما ينسجم مع التدابير والإجراءات الصادرة عن المركز الوطني للأمن السيبراني وبشكل يكفل الحفاظ على حقوق الشخص المعني.

المادة٦- أ- لتحديد مستوى خطورة البيانات محل المعالجة وتأثير مستوى الإخلال بأمن البيانات وسلامتها ونوعها واحتماليتها إضافة الى أثرها على حقوق الأشخاص المعنيين، يلتزم المسؤول بإعداد "تقييم أثر حماية البيانات DPIA" أثناء إجراءات المعالجة في أي من الحالتين التاليتين:-

١- معالجة البيانات الشخصية الحساسة أو نقلها إلى خارج المملكة

٢- أي حالة أخرى يقرر المجلس إلزام المسؤول بإعداد "تقييم أثر حماية البيانات" لأجلها.

ب-يجب أن يتضمن "تقييم أثر حماية البيانات" على ما يلي:

١- نوع البيانات التي بحوزته وحجمها وكميتها وتصنيفها أو التي يعالجها والغرض من عملية المعالجة وطبيعتها ومصادرها وأي جهات سيتم الإفصاح لها إذا تتطلب طبيعتها ذلك.

٢- التدابير والإجراءات المتبعة في معالجة البيانات والتي يتم اتخاذها في حال الإخلال بأمن وسلامة البيانات والتدابير التي ستتخذ لمنع حدوث المخاطر والحد منها ومدى ملاءمة الإجراءات المتبعة لتفادي المخاطر المحددة بشكل يراعي حقوق الشخص المعني وغيره من الأشخاص ذوي العلاقة.

٣- مدة الاحتفاظ بالبيانات وتخزينها.

٤- نطاق المعالجة.

٥- استشارات وآراء الشركاء ذوي العلاقة ان وجدت .

٦- احتمالية المخاطر وأثر المخاطر.

٧- أي معلومات أخرى يرى المراقب تضمينها عند إعداد التقييم.

ج- على المسؤول الاحتفاظ بنسخة من تقييم أثر حماية البيانات وتقديمها إلى الوحدة اذا تطلب الأمر ذلك على أن تكون محدثة بصورة دورية مرة واحدة سنويا على الأقل، وعليه اتخاذ قراراته بناء على نتائج تقييم أثر حماية البيانات.

المادة ٧-أ-يلتزم المسؤول بوضع وتصميم وتنفيذ آليات وإجراءات داخلية فعالة تكفل:

١- المحو أو الاخفاء للبيانات عند طلب الشخص المعني أو الوحدة وفقا لأحكام المادة (١٠) من القانون.

٢- محو البيانات عند انتهاء مدة المعالجة ما لم تنص التشريعات النافذة على غير ذلك.

٣- إخفاء البيانات عن غير المخولين بالاطلاع عليها خلال فترة المعالجة.

ب- للمسؤول الاحتفاظ بنتائج المعالجة بعد انتهاء مدة المعالجة إذا تم محو كل ما يؤدي إلى تحديد هوية الشخص المعني.

ج-على المسؤول عند محو البيانات أو إخفائها القيام بما يلي: -

١- اتخاذ الاجراءات اللازمة لإشعار الجهات الأخرى التي أفصح لها عن البيانات الشخصية بموجب أحكام القانون عن عمليتي المحو و الإخفاء.

٢- محو كافة نسخ البيانات المخزنة والنسخ الاحتياطية من قواعد البيانات أو الأنظمة الخاصة به بما في ذلك التأكد من المعالج والمتلقي بضرورة محو قواعد البيانات المخزنة خارج المملكة، وأن تكون موثقة في أحد بنود العقد الموقع بين المسؤول والمعالج أوالمتلقي.

المادة ٨- أ- يلتزم المسؤول عند التعاقد مع المعالج أو المتلقي بتضمين التدابير الأمنية والتقنية والتنظيمية وتقديم الضمانات اللازمة والوسائل والأغراض في بنود العقد على أن يتضمن العقد ما يلي:

١- تحديد غرض المعالجة ومدتها ونطاقها ومدة الاحتفاظ بالبيانات وتحديد الصلاحيات الممنوحة للأشخاص المخولين بمعالجة البيانات والاطلاع عليها ضمن الغرض والمدة التي تقتضيها المعالجة.

٢- تحديد وسائل التواصل بين المسؤول والمتعاقد معه ليتم الإبلاغ عند حدوث أي اختراق للبيانات أو أي أمر يخل بحقوق الشخص المعني وبياناته.

٣- التزام المعالج والمتلقي بإبلاغ المسؤول فور اكتشاف أي إخلال بأمن وسلامة البيانات أو تسريبها أو تعرضها للحوادث السيبرانية وذلك وفقاً لأحكام هذه التعليمات وأي إجراءات مرتبطة بهذا الخصوص.

٤- تحديد الوسائل التي من خلالها سيقوم المعالج بمحو أو إخفاء أو إعادة البيانات للمسؤول بعد انقضاء مدة المعالجة المحددة.

٥- تحديد جهات المعالجة الفرعية المتعاقد معها أو أي طرف آخر سيتم الإفصاح له عن البيانات المعالجة.

ب-عدم إمكانية قيام المعالج أو المتلقي من معالجة البيانات الشخصية إلا بناء على تعليمات المسؤول المتضمنة في العقد المبرم.

ج-مع مراعاة المادة (١٤) من القانون، إذا تعاقد المعالج الرئيسي مع معالج آخر للقيام بنشاط معالجة معين، تطبق الالتزامات ذاتها المنصوص عليها في الفقرة (أ) من هذه المادة على المعالج الآخر، وعلى أن يتم الحصول على الموافقة من المسؤول الخطية و/ أو الإلكترونية وإشعاره قبل القيام بتلك التعاقدات وتمكينه من الاعتراض على جهة المعالجة متى كان ذلك ضرورياً.

المادة٩- يخضع المتلقي والمعالج للمسؤوليات والواجبات المقررة على المسؤول في هذه التعليمات.

مجلس حماية البيانات الشخصية