تعليمات رقم () لسنة 2024 **تعليمات التدابير الأمنية والتقنية والتنظيمية** **الصادرة بموجب الفقرة (ب) من المادة 8 من قانون حماية البيانات الشخصية رقم (24) لسنة 2023**	
المادة (1)	تسمى هذه التعليمات (تعليمات التدابير الأمنية والتقنية والتنظيمية لحماية البيانات الشخصية لسنة 2024)، ويعمل بها من تاريخ إقرارها من مجلس حماية البيانات الشخصية.
المادة (2)	أ. يكون للكلمات والعبارات التالية، أينما وردت في هذه التعليمات، المعاني المخصصة لها أدناه، ما لم تدل القرينة على غير ذلك: **المملكة:** المملكة الأردنية الهاشمية. **المعالجة الآلية:** عملية واحدة أو أكثر يتم اجراؤها على البيانات بواسطة نظام برمجي آلي يعمل الكترونيا على معالجة البيانات دون تدخل بشري مباشر. **قواعد البيانات:** الملفات أو السجلات الإلكترونية أو غير الإلكترونية التي تشتمل على البيانات. ب. تعتمد التعاريف الواردة في القانون حيثما ورد النص عليها في هذه التعليمات ما لم تدل القرينة على غير ذلك.
المادة (3)	تهدف هذه التعليمات إلى توفير أقصى درجات الحماية والخصوصية لحقوق الشخص المعني وبشكل يكفل ضمان حماية البيانات وتطبيق التدابير التي تضمن أمن البيانات في جميع مراحل المعالجة وبشكل يكفل توقع مشاكل المعالجة وحلها أو منعها قبل حدوثها.
المادة (4)	يلتزم المسؤول بتنفيذ التدابير الأمنية التالية وذلك بحسب طبيعة المعالجة ونطاقها وأهميتها: أ- تهيئة المكان المناسب من الناحية الأمنية بما في ذلك وضع كاميرات مراقبة وأجهزة الإنذار اللازمة وكل ما يمكنه الحفاظ على البيانات وأجهزة ومعدات وتقنية المعلومات وخاصة الأجهزة المحمولة بشكل آمن ومحمي ومنع الوصول إليها. ب- مراقبة عمليات الدخول والخروج في المكان الذي يتم فيه إجراء عملية المعالجة وعلى الأنظمة والشبكات التي تحتوي على البيانات موضوع المعالجة. ت- ضبط عملية الوصول المصرح به إلى مكان المعالجة ومنع أي شخص ليس له علاقة بعملية المعالجة من الوصول إلى المكان المخصص. ث- التخلص من كل ما له علاقة بالبيانات بما يضمن عدم التعرف على هوية الشخص المعني وبما يكفل بالحفاظ على الخصوصية. ج- وضع نسخ البيانات الاحتياطية في مكان آمن ومختلف عن مكان قاعدة البيانات الأصلية.
المادة (5)	يلتزم المسؤول بالقيام بالإجراءات التقنية التالية وذلك بحسب طبيعة المعالجة ونطاقها وأهميتها:

	أ. الالتزام بتطبيق تدابير فعالة للحد من مخاطر انتهاك الخصوصية في مواجهة عمليات او محاولات الاختراق على سبيل المثال تنظيم وضمان الوصول للبيانات المحفوظة، وحماية كلمات المرور، واستخدام برامج مكافحة الفيروسات وتطبيقات جدران الحماية (firewalls) والامتثال لتراخيص البرمجيات، وتنظيم مدة الاحتفاظ بالبيانات ومحوها ووضع ضوابط لنسخ البيانات احتياطيا ووضع بروتوكولات تقنية ملائمة تكفل الوصول الى المواقع الفعلية والنظم الافتراضية التي تخزن فيها البيانات. ب. اجراء فحوصات لتقييم مواطن الضعف والاختراق في البيئة التقنية المستخدمة لمعالجة البيانات (vulnerability assessment and penetration testing) وذلك بصورة دورية للتحقق من كفاءة التدابير الأمنية والتقنية والتنظيمية المعمول بها وقياس مدى فعاليتها لتصحيح أي ثغرات امنية والحد منها. ج. ترميز أو تشفير البيانات أثناء تناقلها أو تخزينها أو في الحالات التي تتطلب ذلك. د. القدرة على الوصول الى البيانات واستعادتها وضمان توافرية عالية للبيانات في الوقت المناسب في حالة حدوث خلل أو اخلال بأمن وسلامة البيانات. هـ. حماية النسخ الاحتياطية من 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 والادوار المحددة للمستخدمين. ز. اتخاذ التدابير التقنية وفقا للتطورات التكنولوجية وضمان مواكبتها لأخر التحديثات وتجديد الإجراءات المتخذة بشكل دوري.
المادة (6)	يلتزم المسؤول بتنفيذ التدابير التنظيمية التالية وذلك بحسب طبيعة المعالجة ونطاقها وأهميتها: أ. وضع سياسات لحماية البيانات. ب. توفير برامج تدريبية دورية تضمن إلمام الموظفين القائمين على معالجة البيانات بما يكفل ضمان أمان البيانات وفقاً لأحكام القانون والأنظمة والتعليمات الصادرة بمقتضاه. ج. تحديد نطاق صلاحية الموظف المعني بمعالجة البيانات بما لا يتجاوز نطاق عمله وفي حدود ضيقة وبما تقتضيه طبيعة عمله بالاطلاع مباشرة على تلك البيانات. د. حفظ وتوثيق كافة مراحل عملية المعالجة بوسائل تتيح للشخص المعني الاطلاع والتحقق منها والوصول إليها وتصحيحها وتقييدها وحذفها ونقلها والاعتراض عليها. هـ. تطبيق آليات وإجراءات للتحقق من هوية مقدم الطلب قبل الموافقة على طلب الوصول أو الحذف أو التحديث أو الاطلاع أو التصحيح أو الاضافة على البيانات. و. 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.

	ز. الالتزام بتطبيق تدابير وإجراءات تحد من مخاطر انتهاك حق الخصوصية في مواجهة الحوادث السيبرانية والاختراقات وبما نسجم مع التدابير والإجراءات الصادرة عن المركز الوطني للأمن السيبراني وبشكل يكفل الحفاظ على حقوق الشخص المعني. ح. توفير وسائل تواصل تراعي احتياجات الشخص المعني بما فيها الوسائل المناسبة للأشخاص ذوي الإعاقة والتي تمنح القدرة على ممارسة حقوقهم وفقا للمادة 4 من القانون في أي وقت.
المادة (7)	أ. بهدف تحديد مستوى خطورة البيانات محل المعالجة وتأثير مستوى الاخلال بأمن البيانات وسلامتها ونوعها، يلتزم المسؤول بإعداد "تقييم أثر حماية البيانات" أثناء إجراءات المعالجة في الحالات التالية: 1. إذا كان العمل الرئيسي للمسؤول معالجة البيانات الشخصية. 2. معالجة البيانات الشخصية الحساسة. 3. إذا كانت عملية معالجة البيانات لمن لا يتمتع بالأهلية القانونية. 4. إذا كانت البيانات المعالجة تتعلق بمعلومات مالية. 5. عمليات المعالجة التي تتطلب بطبيعتها مراقبة مستمرة لحقوق الشخص المعني، أو معالجة بيانات شخصية باستخدام التقنيات أو براءات الاختراع، أو اتخاذ قرارات مبنية على المعالجة الآلية للبيانات الشخصية. 6. التشخيص. 7. تقديم منتج أو خدمة معتمدة على معالجة البيانات الشخصية والتي من المحتمل أن تشكل أضراراً جسيمة على خصوصية الأشخاص المعنيين. 8. نقل قواعد البيانات الشخصية خارج المملكة بغرض معالجتها. 9. أي حالة أخرى يقرر المجلس إلزام المسؤول بإعداد "تقييم أثر حماية البيانات" لأجلها. ب. يجب أن يتضمن "تقييم أثر حماية البيانات" على ما يلي: 1. نوع وحجم وكمية وتصنيف البيانات التي بحوزته أو التي يعالجها والغرض من عملية المعالجة وطبيعتها ومصادرها وأية جهات سيتم الإفصاح لها إذا ما تطلبت طبيعتها ذلك. 2. التدابير والإجراءات المتبعة لمعالجة البيانات والتي يتم اتخاذها في حالة الإخلال بأمن وسلامة البيانات والتدابير التي ستتخذ لمنع حدوث المخاطر والحد منها ومدى ملائمة الإجراءات المتبعة لتفادي المخاطر المحددة بشكل يكفل مراعاة حقوق الشخص المعني وغيرهم من الأشخاص ذوي العلاقة. 3. أي معلومات أخرى يراها المراقب مناسبة. ج. يجب على المسؤول الاحتفاظ بنسخة من "تقييم أثر حماية البيانات" وتقديمها إلى الوحدة متى تطلب الأمر ذلك وتحديثه بشكل دوري واتخاذ قراراته بناء على نتائج "تقييم أثر حماية البيانات".
المادة (8)	أ. يلتزم المسؤول بوضع وتصميم وتنفيذ آليات وإجراءات داخلية فعالة تكفل: 1. محو أو اخفاء البيانات عند طلب الشخص المعني أو الوحدة وفقا لأحكام المادة 10 من القانون.

	2. محو البيانات عند انتهاء مدة المعالجة مالم تنص التشريعات على غير ذلك. 3. إخفاء البيانات لغير المخولين بالاطلاع عليها خلال فترة المعالجة. ب. يجوز للمسؤول الاحتفاظ بنتائج المعالجة بعد انتهاء مدة المعالجة إذا تم محو كل ما يؤدي إلى تحديد هوية الشخص المعني بشكل مباشر أو غير مباشر. ج. على المسؤول عند محو البيانات أو إخفاؤها القيام بما يلي: 1. اتخاذ الاجراءات اللازمة لإشعار الجهات الاخرى التي أفصح لها عن البيانات الشخصية بموجب أحكام القانون عن عمليتي المحو أو الاخفاء. 2. محو كافة نسخ البيانات المخزنة والنسخ الاحتياطية في قواعد البيانات أو الأنظمة الخاصة به وتشمل عملية المحو قواعد البيانات المخزنة خارج المملكة.
المادة (9)	أ. يلتزم المسؤول عند التعاقد مع معالج أو متلقي بتضمين التدابير الأمنية والتقنية والتنظيمية وتقديم الضمانات الكافية وعلى أن يتضمن العقد ما يلي: 1. تحديد غرض المعالجة ومدتها ونطاقها وتحديد الصلاحيات الممنوحة للأشخاص المخولين بمعالجة البيانات والاطلاع عليها ضمن الغرض والمدة التي تقتضيها المعالجة. 2. تحديد وسائل التواصل بين المسؤول والمتعاقد معه للتواصل عند حدوث أي أمر يخص بحقوق الشخص المعني وبياناته. 3. التزام المعالج والمتلقي بإبلاغ المسؤول فور اكتشاف أي اخلال بأمن وسلامة البيانات أو تسريبها أو تعرضها للحوادث السيبرانية وذلك وفقاً لأحكام هذه التعليمات واية إجراءات مرتبطة بهذا الخصوص. 4. تحديد الوسائل التي من خلالها سيقوم المعالج بمحو أو إخفاء أو إعادة البيانات للمسؤول بعد انقضاء مدة المعالجة المحددة. 5. تحديد جهات المعالجة الفرعية المتعاقدة أو أي طرف آخر سيتم الإفصاح له عن البيانات المعالجة. ب. لا يمكن للمعالج معالجة البيانات الشخصية إلا بناء على تعليمات المسؤول المكتوبة بموجب أحكام العقد المبرم. ج. مع مراعاة المادة 14 من القانون، إذا تعاقد المعالج الرئيسي مع معالج آخر للقيام بنشاط معالجة معين، تطبق ذات الالتزامات المذكورة في الفقرة (أ) من هذه المادة، وعلى أن يتم الحصول على الموافقة من المسؤول وإشعاره قبل القيام بتلك التعاقدات وتمكينه الاعتراض على جهة المعالجة متى كان ذلك ضرورياً.
المادة (10)	يخضع المتلقي والمعالج للمسؤوليات والواجبات القانونية المقررة ذاتها على المسؤول في هذه التعليمات.