

مرسوم بقانون اتحادي رقم (45) لسنة 2021

بشأن حماية البيانات الشخصية

رئيس دولة الإمارات العربية المتحدة،

نحن خليفة بن زايد آل نهيان

- بعد الاطلاع على الدستور،
- وعلى القانون الاتحادي رقم (1) لسنة 1972 بشأن اختصاصات الوزارات وصلاحيات الوزراء، وتعديلاته،
- وعلى المرسوم بقانون اتحادي رقم (3) لسنة 2003 في شأن تنظيم قطاع الاتصالات، وتعديلاته،
- وعلى القانون الاتحادي رقم (6) لسنة 2010 بشأن المعلومات الائتمانية، وتعديلاته،
- وعلى القانون الاتحادي رقم (14) لسنة 2016 بشأن المخالفات والجزاءات الإدارية في الحكومة الاتحادية،
- وعلى القانون الاتحادي رقم (2) لسنة 2019 في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية،
- وعلى المرسوم بقانون اتحادي رقم (14) لسنة 2018 في شأن المصرف المركزي وتنظيم المنشآت والأنشطة المالية، وتعديلاته،
- وعلى المرسوم بقانون اتحادي رقم (44) لسنة 2021 في شأن إنشاء مكتب الإمارات للبيانات،
- وبناءً على ما عرضه وزير شؤون مجلس الوزراء، وموافقة مجلس الوزراء،

أصدرنا المرسوم بقانون الآتي:

المادة (1)

التعريف

في تطبيق أحكام هذا المرسوم بقانون، يُقصد بالكلمات والعبارات التالية المعاني المبينة قرين كل منها، ما لم يقض سياق النص بغير ذلك:

الدولة : الإمارات العربية المتحدة.

المكتب : مكتب الإمارات للبيانات المنشأ بموجب المرسوم بقانون اتحادي رقم (44) لسنة 2021 المشار إليه.

البيانات : مجموعة منظمة أو غير منظمة من المعطيات، أو الوقائع أو المفاهيم أو التعليمات أو المشاهدات أو القياسات تكون على شكل أرقام أو حروف أو كلمات أو رموز أو صور أو فيديوهات أو إشارات أو أصوات أو خرائط أو أي شكل آخر، يتم تفسيرها أو تبادلها أو معالجتها، عن طريق الأفراد أو الحواسيب، وتشمل المعلومات أينما وردت في هذا المرسوم بقانون.

- البيانات الشخصية :** أي بيانات تتعلق بشخص طبيعي محدد، أو تتعلق بشخص طبيعي يمكن التعرف عليه بشكل مباشر أو غير مباشر من خلال الربط بين البيانات، من خلال استخدام عناصر التعريف كاسمه، أو صوته، أو صورته، أو رقمه التعريفي، أو المعرف الإلكتروني الخاص به، أو موقعه الجغرافي، أو صفة أو أكثر من صفاته الشكلية أو الفسيولوجية، أو الاقتصادية، أو الثقافية، أو الاجتماعية، وتشمل البيانات الشخصية الحساسة والبيانات الحيوية البيومترية.
- البيانات الشخصية الحساسة :** أي بيانات تكشف بشكل مباشر أو غير مباشر عن عائلة الشخص الطبيعي أو أصله العرقي أو آرائه السياسية أو الفلسفية أو معتقداته الدينية، أو سجل السوابق الجنائية الخاص به، أو بيانات القياسات الحيوية البيومترية الخاصة به، أو أي بيانات تتعلق بصحة هذا الشخص وتشمل حالته الجسدية أو النفسية أو الذهنية أو العقلية أو البدنية أو الجينية أو الجنسية، بما في ذلك المعلومات المتعلقة بتوفير خدمات الرعاية الصحية له التي تكشف عن وضعه الصحي.
- البيانات الحيوية البيومترية :** البيانات الشخصية الناتجة عن المعالجة باستخدام تقنية محددة تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية لصاحب البيانات، والتي تسمح بتحديد أو تؤكد التحديد الفريد لصاحب البيانات، مثل صورة الوجه أو بيانات البصمة.
- صاحب البيانات :** الشخص الطبيعي موضوع البيانات الشخصية.
- المنشأة :** أي شركة أو مؤسسة فردية داخل الدولة أو خارجها، بما فيها الشركات المملوكة بشكل جزئي أو كامل للحكومة الاتحادية أو المحلية أو التي تساهم فيها.
- المتحكم :** المنشأة أو الشخص الطبيعي الذي لديه بيانات شخصية، ويحكم نشاطه يقوم بتحديد طريقة وأسلوب ومعايير معالجة هذه البيانات الشخصية والغاية من معالجتها، سواء بمفرده أو بالاشتراك مع أشخاص أو منشآت أخرى.
- المعالج :** المنشأة أو الشخص الطبيعي الذي يعالج البيانات الشخصية نيابة عن المتحكم، بحيث يقوم بمعالجتها تحت توجيه ووفقاً لتعليماته.
- مسؤول حماية البيانات :** أي شخص طبيعي أو اعتباري يتم تعيينه من قبل المتحكم أو المعالج، يتولى مهام التأكد من مدى امتثال الجهة التي يتبعها بضوابط واشتراطات وإجراءات وقواعد معالجة حماية البيانات الشخصية المنصوص عليها في هذا المرسوم بقانون، والتأكد من سلامة أنظمتها وإجراءاتها من أجل تحقيق الالتزام بأحكامه.

- المعالجة :** أي عملية أو مجموعة عمليات يتم إجراؤها على البيانات الشخصية باستخدام أي وسيلة من الوسائل الإلكترونية بما فيها وسيلة المعالجة وغيرها من الوسائل الأخرى، وتشمل هذه العملية جمع البيانات الشخصية، أو تخزينها، أو تسجيلها أو تنظيمها أو تكييفها أو تعديلها، أو تداولها، أو تحويلها، أو استرجاعها، أو تبادلها، أو مشاركتها، أو استعمالها، أو توصيفها، أو الإفصاح عنها عن طريق بثها أو نقلها أو توزيعها أو إتاحتها أو تنسيقها أو دمجها أو تقييدها أو حجتها أو محوها أو إتلافها أو إنشاء نماذج لها.
- المعالجة :** المعالجة التي تتم باستخدام برنامج أو نظام إلكتروني، يعمل بطريقة آلية وتلقائية إما بشكل
- المؤتمتة** مستقل كلياً دون أي تدخل بشري أو بشكل جزئي بإشراف وتدخل بشري محدود.
- أمن :** مجموعة من التدابير والإجراءات والعمليات التقنية والتنظيمية المحددة وفقاً لأحكام هذا
- البيانات** المرسوم بقانون التي من شأنها الحفاظ على حماية خصوصية وسرية، وسلامة، ووحدة البيانات
- الشخصية** الشخصية، وتكاملها وتوافرها.
- آلية إخفاء :** المعالجة التي يتم إجراؤها على البيانات الشخصية بطريقة تؤدي بعد إتمام المعالجة إلى عدم
- البيانات** إمكانية ربط وتنسيب هذه البيانات بصاحب البيانات دون استخدام معلومات إضافية، شريطة أن تكون تلك المعلومات الإضافية محفوظة بشكل مستقل وآمن، ووفقاً للتدابير والإجراءات التقنية والتنظيمية المحددة بموجب أحكام هذا المرسوم بقانون، لضمان عدم ارتباط البيانات الشخصية إلى شخص طبيعي محدد أو يمكن التعرف عليه من خلالها.
- آلية إخفاء :** المعالجة التي يتم إجراؤها على البيانات الشخصية بطريقة تؤدي إلى إخفاء هوية صاحب
- الهوية** البيانات وعدم ربط وتنسيب هذه البيانات به وعدم إمكانية التعرف عليه بأي طريقة كانت.
- خرق :** عملية خرق لأمن المعلومات وانتهاك البيانات الشخصية من خلال الدخول والوصول إليها بشكل
- وانتهاك** غير مشروع أو غير مرخص به، وتشمل نسخها، أو إرسالها، أو توزيعها أو تبادلها أو نقلها أو تداولها، أو معالجتها بشكل يؤدي إلى الكشف أو الإفصاح إلى الغير عن هذه البيانات، أو إتلافها أو تعديلها أثناء عملية التخزين والنقل والمعالجة.
- التنميط :** شكل من أشكال المعالجة المؤتمتة بحيث تتضمن استخدام البيانات الشخصية لتقييم جوانب شخصية
- معينة** ومرتبطة بصاحب البيانات، ومن بينها تحليل أو توقع الجوانب المتعلقة بأدائه أو وضعه المالي، أو صحته أو تفضيلاته الشخصية أو اهتماماته أو سلوكه أو مكانه أو تحركاته أو موثوقيته.
- المعالجة :** نشر أو استخدام أو عرض أو إرسال أو استقبال أو استرجاع أو استخدام أو مشاركة البيانات
- عبر الحدود** الشخصية أو معالجتها خارج النطاق الجغرافي للدولة.
- الموافقة :** الموافقة التي يصرح فيها صاحب البيانات للغير بمعالجة بياناته الشخصية، على أن تكون هذه
- الموافقة** الموافقة بشكل محدد وواضح لا لبس فيه على قبوله بمعالجة بياناته الشخصية من خلال بيان أو إجراء إيجابي واضح.

المادة (2)

نطاق سريان المرسوم بقانون

1. تسري أحكام هذا المرسوم بقانون على معالجة البيانات الشخصية سواء كلها أو جزء منها عن طريق وسائل الأنظمة الإلكترونية التي تعمل بشكل تلقائي وآلي، أو غيرها من الوسائل الأخرى، وذلك من قبل:
 - أ. كل صاحب بيانات يقيم في الدولة أو له مقر عمل فيها.
 - ب. كل متحكم أو معالج متواجد في الدولة يقوم بمزاولة أنشطة معالجة البيانات الشخصية لأصحاب البيانات في الدولة أو خارجها.
 - ج. كل متحكم أو معالج متواجد خارج الدولة يقوم بمزاولة أنشطة معالجة البيانات الشخصية لأصحاب البيانات في الدولة.
2. لا تسري أحكام هذا المرسوم بقانون على ما يأتي:
 - أ. البيانات الحكومية.
 - ب. الجهات الحكومية المتحكم بالبيانات الشخصية أو تلك التي تقوم بمعالجتها.
 - ج. البيانات الشخصية لدى الجهات الأمنية والقضائية.
 - د. صاحب البيانات الذي يقوم بمعالجة بياناته لأغراض شخصية.
 - هـ. البيانات الشخصية الصحية التي لديها تشريع ينظم حماية ومعالجة تلك البيانات.
 - و. البيانات والمعلومات الشخصية المصرفية والائتمانية التي لديها تشريع ينظم حماية ومعالجة تلك البيانات.
 - ز. الشركات والمؤسسات الواقعة في المناطق الحرة في الدولة ولديها تشريعات خاصة بحماية البيانات الشخصية.

المادة (3)

سلطة المكتب في الإعفاء

مع عدم الإخلال بأي اختصاصات أخرى مقررة للمكتب بموجب أي تشريع آخر، يكون للمكتب إعفاء بعض المنشآت التي لا تقوم بمعالجة حجم كبير من البيانات الشخصية من جزء أو كل متطلبات واشتراطات أحكام حماية البيانات الشخصية المنصوص عليها في هذا المرسوم بقانون، وذلك وفقاً للمعايير والضوابط التي تحددها اللائحة التنفيذية لهذا المرسوم بقانون.

المادة (4)

حالات معالجة البيانات الشخصية بدون موافقة صاحبها

يُحظر معالجة البيانات الشخصية دون موافقة صاحبها، وتُستثنى أي من الحالات التالية من هذا الحظر وتعتبر المعالجة حينها مشروعة:

1. أن تكون المعالجة ضرورية لحماية المصلحة العامة.
2. أن تكون المعالجة مرتبطة بالبيانات الشخصية التي أصبحت متاحة ومعلومة للكافة بفعل من صاحب البيانات.
3. أن تكون المعالجة ضرورية لإقامة أي من إجراءات المطالبة بالحقوق والدعاوى القانونية أو الدفاع عنها أو تتعلق بالإجراءات القضائية أو الأمنية.
4. أن تكون المعالجة ضرورية لأغراض الطب المهني أو الوقائي من أجل تقييم قدرة الموظفين على العمل، أو التشخيص الطبي أو تقديم الرعاية الصحية أو الاجتماعية أو العلاج أو خدمات التأمين الصحي أو إدارة أنظمة وخدمات الرعاية الصحية أو الاجتماعية وفقاً للتشريعات السارية في الدولة.
5. أن تكون المعالجة ضرورية لحماية الصحة العامة، وتشمل الحماية من الأمراض السارية والأوبئة أو لأغراض ضمان سلامة وجودة الرعاية الصحية والأدوية والعقاقير والأجهزة الطبية، وفقاً للتشريعات السارية في الدولة.
6. أن تكون المعالجة ضرورية لأغراض أرشيفية أو دراسات علمية وتاريخية وإحصائية وفقاً للتشريعات السارية في الدولة.
7. أن تكون المعالجة ضرورية لحماية مصالح صاحب البيانات.
8. أن تكون المعالجة ضرورية لأغراض قيام المتحكم أو صاحب البيانات بالتزاماته ومباشرة حقوقه المقررة قانوناً في مجال التوظيف أو الضمان الاجتماعي أو القوانين المعنية بالحماية الاجتماعية وذلك بالقدر الذي يسمح به في تلك القوانين.
9. أن تكون المعالجة ضرورية لتنفيذ عقد يكون صاحب البيانات طرفاً فيه أو لاتخاذ إجراءات بناءً على طلب صاحب البيانات بهدف إبرام عقد أو تعديله أو إنهائه.
10. أن تكون المعالجة ضرورية لتنفيذ التزامات محددة في قوانين أخرى في الدولة على المتحكم.
11. أية حالات أخرى تحددها اللائحة التنفيذية لهذا المرسوم بقانون.

المادة (5)

ضوابط معالجة البيانات الشخصية

يتم معالجة البيانات الشخصية وفقاً للضوابط الآتية:

1. أن تكون المعالجة بطريقة عادلة وشفافة ومشروعة.
2. أن تكون البيانات الشخصية قد جمعت لغرض محدد وواضح، وألا يتم معالجتها في أي وقت لاحق على نحو يتنافى مع ذلك الغرض، ومع ذلك يجوز معالجتها في حال كان الغرض منها مشابه أو متقارب من الغرض الذي جمعت هذه البيانات من أجله.
3. أن تكون البيانات الشخصية كافية ومقتصرة على ما هو ضروري وفقاً للغرض الذي تمت المعالجة من أجله.
4. أن تكون البيانات الشخصية دقيقة وصحيحة، وأن تخضع للتحديث متى اقتضى الأمر ذلك.
5. أن تتوفر تدابير وإجراءات لضمان محو أو تصحيح البيانات الشخصية غير الصحيحة.
6. أن تكون البيانات الشخصية محفوظة بشكل آمن بما فيها حمايتها من أي انتهاك أو اختراق أو معالجة غير مشروعة أو غير مصرح بها من خلال وضع واستخدام تدابير وإجراءات تقنية وتنظيمية ملائمة وفق القوانين والتشريعات السارية في هذا الشأن.
7. عدم الاحتفاظ بالبيانات الشخصية بعد استنفاد الغرض من معالجتها، ويجوز الإبقاء عليها في حال تم إخفاء هوية صاحب البيانات باستخدام خاصية "آلية إخفاء الهوية".
8. أية ضوابط أخرى تحددها اللائحة التنفيذية لهذا المرسوم بقانون.

المادة (6)

شروط الموافقة على معالجة البيانات

1. يشترط للاعتداد بموافقة صاحب البيانات على معالجتها ما يلي:
 - أ. أن يكون المتحكم قادراً على إثبات موافقة صاحب البيانات في حال كانت المعالجة مبنية على موافقة صاحب البيانات لمعالجة بياناته الشخصية.
 - ب. أن تكون الموافقة معدة بطريقة واضحة وبسيطة وغير مهمة وسهلة الوصول إليها سواء كانت كتابية أو إلكترونية.
 - ج. أن تتضمن الموافقة ما يفيد حق صاحب البيانات بالعدول عنها، وأن يكون إجراء العدول بطريقة سهلة.
2. يجوز لصاحب البيانات العدول في أي وقت عن موافقته على معالجة بياناته الشخصية، ولا يؤثر هذا العدول على قانونية ومشروعية المعالجة المبنيّة على الموافقة التي أعطيت قبل العدول عنها.

المادة (7)

الالتزامات العامة للمتحكم

يجب على المتحكم الالتزام بما يأتي:

1. اتخاذ الإجراءات والتدابير التقنية والتنظيمية الملائمة لتطبيق المعايير القياسية اللازمة لحماية وتأمين البيانات الشخصية حفاظاً على سريتها وخصوصيتها، وضمان عدم اختراقها أو إتلافها أو تغييرها أو العبث بها، مع مراعاة طبيعة ونطاق وأغراض المعالجة واحتمالية وجود مخاطر على سرية وخصوصية البيانات الشخصية لصاحب البيانات.
2. تطبيق التدابير الملائمة سواء أثناء تحديد وسائل المعالجة أو أثناء المعالجة نفسها، وذلك بهدف الامتثال لأحكام هذا المرسوم بقانون بما فيها الضوابط المنصوص عليها في المادة (5) منه، وتشمل هذه التدابير آلية إخفاء البيانات.
3. تطبيق التدابير التقنية والتنظيمية الملائمة بالنسبة للإعدادات التلقائية، للتأكد من اقتصار معالجة البيانات الشخصية على الغرض المحدد لها، ويُطبق هذا الالتزام على حجم ونوع البيانات الشخصية التي يتم جمعها، ونوع المعالجة التي سيتم إجراؤها عليها، وفترة تخزين هذه البيانات، ومدى إمكانية الوصول إليها.
4. مسك سجل خاص للبيانات الشخصية، على أن يتضمن هذا السجل بيانات كل من المتحكم ومسؤول حماية البيانات، وبيان وصف فئات البيانات الشخصية لديه، وبيانات الأشخاص المصرح لهم بالوصول إلى البيانات الشخصية، والمدد الزمنية للمعالجة وقيودها ونطاقها، وآلية محو البيانات الشخصية أو تعديلها أو معالجتها لديه، والغرض من المعالجة، وأي بيانات متعلقة بحركة ومعالجة تلك البيانات عبر الحدود، وبيان الإجراءات التقنية والتنظيمية الخاصة بأمن المعلومات وعمليات المعالجة. على أن يقوم المتحكم بتوفير هذا السجل للمكتب متى ما طلب منه ذلك.
5. تعيين المعالج الذي يتوفر لديه ضمانات كافية لتطبيق التدابير التقنية والتنظيمية على نحو يضمن استيفاء المعالجة لمتطلبات وقواعد وضوابط المعالجة المنصوص عليها في هذا المرسوم بقانون ولائحته التنفيذية والقرارات الصادرة تنفيذاً له.
6. تزويد المكتب، وبناءً على قرار من الجهة القضائية المختصة، بأي معلومات يطلبها تنفيذاً لاختصاصاته الواردة في هذا المرسوم بقانون ولائحته التنفيذية.
7. أي التزامات أخرى تحددها اللائحة التنفيذية لهذا المرسوم بقانون.

المادة (8)

الالتزامات العامة للمعالج

يجب على المعالج الالتزام بما يأتي:

1. إجراء المعالجة وتنفيذها وفقاً لتعليمات المتحكم، والعقود والاتفاقات المبرمة بينهما التي تحدد على وجه الخصوص نطاق المعالجة وموضوعها وغرضها وطبيعتها ونوع البيانات الشخصية، وفئات أصحاب البيانات.
2. تطبيق الإجراءات والتدابير التقنية والتنظيمية الملائمة لحماية البيانات الشخصية في مرحلة التصميم، سواء أثناء تحديد وسائل المعالجة أو أثناء المعالجة نفسها، على أن يراعى فيها تكلفة تطبيق هذه الإجراءات والتدابير وطبيعة المعالجة ونطاقها وأغراضها.
3. إجراء المعالجة وفق الغرض والمدة المحددة لها، وفي حال تجاوزت المعالجة المدة المحددة يجب عليه أن يخطر المتحكم بذلك ليأذن له بتمديد هذه المدة أو يصدر إليه التوجيهات المناسبة.
4. محو البيانات بعد انقضاء مدة المعالجة أو تسليمها للمتحكم.
5. عدم القيام بأي عمل من شأنه الإفصاح عن البيانات الشخصية أو نتائج المعالجة إلا في الأحوال المصرح بها قانوناً.
6. حماية وتأمين عملية المعالجة وتأمين الوسائط والأجهزة الإلكترونية المستخدمة في المعالجة وما عليها من بيانات شخصية.
7. مسك سجل خاص للبيانات الشخصية التي تتم معالجتها نيابة عن المتحكم، على أن يتضمن هذا السجل بيانات كل من المتحكم والمعالج ومسؤول حماية البيانات وبيان وصف فئات البيانات الشخصية لديه، وبيانات الأشخاص المصرح لهم بالوصول إلى البيانات الشخصية، والمدة الزمنية للمعالجة وقيودها ونطاقها، وآلية محو البيانات الشخصية أو تعديلها أو معالجتها لديه، والغرض من المعالجة، وأي بيانات متعلقة بحركة ومعالجة تلك البيانات عبر الحدود، وبيان الإجراءات التقنية والتنظيمية الخاصة بأمن المعلومات وعمليات المعالجة. على أن يقوم المعالج بتوفير هذا السجل للمكتب متى ما طلب منه ذلك.
8. توفير كافة الوسائل لإثبات التزامه بتطبيق أحكام هذا المرسوم بقانون عند طلب المتحكم أو المكتب ذلك.
9. إجراء المعالجة وتنفيذها طبقاً للقواعد والاشتراطات والضوابط المحددة بهذا المرسوم بقانون ولائحته التنفيذية أو التي يصدر بموجبها تعليمات من المكتب.
10. في حال اشترك أكثر من معالج في عملية المعالجة، يجب أن تنفذ المعالجة وفقاً لعقد أو اتفاق مكتوب يحدد بموجبه بشكل واضح التزاماتهم ومسؤولياتهم وأدوارهم حول عملية المعالجة، وإلا اعتبروا مسؤولين بالتضامن عن الالتزامات والمسؤوليات الواردة في هذا المرسوم بقانون ولائحته التنفيذية.
11. تحدد اللائحة التنفيذية لهذا المرسوم بقانون الإجراءات والضوابط والشروط والمعايير الفنية والقياسية المتعلقة بهذه الالتزامات.

المادة (9)

الإبلاغ عن انتهاك البيانات الشخصية

1. بالإضافة إلى التزامات المتحكم المنصوص عليها في هذا المرسوم بقانون، يلتزم المتحكم بمجرد علمه بوجود أي اختراق أو انتهاك للبيانات الشخصية لصاحب البيانات الذي من شأنه المساس بخصوصية وسرية وأمن بياناته، بإبلاغ المكتب عن هذا الاختراق أو الانتهاك ونتائج التحقيق خلال المدة ووفقاً للإجراءات والشروط التي تحددها اللائحة التنفيذية لهذا المرسوم بقانون، على أن يكون الإبلاغ مشفوعاً بالبيانات والمستندات الآتية:
 - أ. بيان طبيعة الاختراق أو الانتهاك، وصورته، وأسبابه، والعدد التقريبي له وسجلاته.
 - ب. بيانات مسؤول حماية البيانات المعين لديه.
 - ج. الآثار المحتملة والمتوقعة لحدوث الاختراق أو الانتهاك.
 - د. بيان الإجراءات والتدابير المتخذة من قبله والمقترح تنفيذها لمواجهة هذا الاختراق أو الانتهاك والتقليل من آثاره السلبية.
 - هـ. توثيق الاختراق أو الانتهاك، والإجراءات التصحيحية المتخذة من قبله.
 - و. أية متطلبات أخرى يطلبها المكتب.
2. وفي جميع الأحوال، يجب على المتحكم أن يخطر صاحب البيانات في حال كان الانتهاك أو الاختراق من شأنه المساس بخصوصية وسرية وأمن بياناته الشخصية، خلال المدة ووفقاً للإجراءات والشروط التي تحددها اللائحة التنفيذية لهذا المرسوم بقانون، وموافاته بالإجراءات المتخذة من قبله.
3. في حال علم المعالج بوجود أي اختراق أو انتهاك للبيانات الشخصية لصاحب البيانات، يجب عليه إخطار المتحكم بهذا الاختراق أو الانتهاك فور علمه بذلك، ليقوم المتحكم بدوره بإبلاغ المكتب وفقاً للبند (1) من هذه المادة.
4. يتولى المكتب بعد استلام البلاغ من المتحكم بالتحقق من أسباب الانتهاك والاختراق لضمان سلامة الإجراءات الأمنية المتخذة، وتوقيع الجزاءات الإدارية المشار إليها في المادة (26) من هذا المرسوم بقانون في حال ثبوت مخالفة المتحكم أو المعالج لأحكامه والقرارات الصادرة تنفيذاً له.

المادة (10)

تعيين مسؤول حماية البيانات

1. يجب على المتحكم والمعالج تعيين مسؤول لحماية البيانات تتوفر فيه المهارات والدراسة الكافية بحماية البيانات الشخصية، وذلك في أي من الأحوال الآتية:
 - أ. إذا كانت المعالجة من شأنها إحداث خطر ذو مستوى عالي على سرية وخصوصية البيانات الشخصية لصاحب البيانات نتيجة اعتماد تقنيات جديدة أو مرتبطة بحجم البيانات.
 - ب. إذا كانت المعالجة ستضمن تقييم ممنهج وشامل للبيانات الشخصية الحساسة بما يشمل التمييز والمعالجة المؤتمتة.
 - ج. إذا كانت المعالجة ستتم على حجم كبير من البيانات الشخصية الحساسة.
2. يجوز أن يكون مسؤول حماية البيانات موظفاً لدى المتحكم أو المعالج أو مخول من قبلهما سواء من داخل الدولة أو خارجها.
3. على المتحكم أو المعالج تحديد عنوان الاتصال بمسؤول حماية البيانات وإخطار المكتب بذلك.
4. تحدد اللائحة التنفيذية لهذا المرسوم بقانون أنواع التقنيات ومعايير تحديد حجم البيانات المطلوبة وفقاً لهذه المادة.

المادة (11)

أدوار مسؤول حماية البيانات

1. يتولى مسؤول حماية البيانات التأكد من مدى امتثال المتحكم أو المعالج بتنفيذ أحكام هذا المرسوم بقانون ولائحته التنفيذية والتعليمات الصادرة عن المكتب، ويتولى مسؤول حماية البيانات على وجه الخصوص القيام بالمهام والصلاحيات الآتية:
 - أ. التحقق من جودة وصحة الإجراءات المعمول بها لدى كل من المتحكم والمعالج.
 - ب. تلقي الطلبات والشكاوى المتعلقة بالبيانات الشخصية وفقاً لأحكام هذا المرسوم بقانون ولائحته التنفيذية.
 - ج. تقديم الاستشارات الفنية الخاصة بإجراءات التقييم والفحص الدوري لأنظمة حماية البيانات الشخصية لدى المتحكم والمعالج، وأنظمة منع الاختراق، وتوثيق نتائج هذا التقييم، وتقديم التوصيات المناسبة بشأنها بما فيها إجراءات تقييم المخاطر.
 - د. العمل كحلقة وصل بين المتحكم أو المعالج حسب الأحوال والمكتب بشأن قيامهما بتطبيق أحكام معالجة البيانات الشخصية المنصوص عليها في هذا المرسوم بقانون.
 - هـ. أي مهام أو صلاحيات أخرى يتم تحديدها بموجب اللائحة التنفيذية لهذا المرسوم بقانون.
2. على مسؤول حماية البيانات الالتزام بالحفاظ على سرية المعلومات والبيانات التي يتلقاها تنفيذاً لمهامه وصلاحياته وفقاً لأحكام هذا المرسوم بقانون ولائحته التنفيذية ووفقاً للتشريعات السارية في الدولة.

المادة (12)

واجبات المتحكم والمعالج تجاه مسؤول حماية البيانات

1. على المتحكم والمعالج توفير كافة السبل لضمان أداء مسؤول حماية البيانات الأدوار والمهام الموكلة إليه والمنصوص عليها في المادة (11) من هذا المرسوم بقانون بالشكل المطلوب، وعلى وجه الخصوص ما يأتي:
 - أ. ضمان إشراكه بشكل مناسب وفي الوقت الملائم في كافة المسائل المتعلقة بحماية البيانات الشخصية.
 - ب. ضمان تزويده بكافة الموارد اللازمة وتقديم الدعم اللازم له لتنفيذ المهام الموكلة إليه.
 - ج. عدم إنهاء خدماته أو فرض أي جزاء تأديبي بسبب يتعلق بتأديته لمهامه وفقاً لأحكام هذا المرسوم بقانون.
 - د. ضمان عدم تكليفه بمهام تؤدي إلى تعارض في المصالح بينها وبين المهام المحددة له وفقاً لهذا المرسوم بقانون.
2. لصاحب البيانات التواصل مباشرة مع مسؤول حماية البيانات بكل ما يتعلق ببياناته الشخصية ومعالجتها لتمكينه من ممارسة حقوقه وفقاً لأحكام هذا المرسوم بقانون.

المادة (13)

حق الحصول على المعلومات

1. يحق لصاحب البيانات وبناءً على طلب يقدمه إلى المتحكم ومن دون أي مقابل الحصول على المعلومات الآتية:
 - أ. أنواع البيانات الشخصية التابعة له التي يتم معالجتها.
 - ب. أغراض المعالجة.
 - ج. القرارات المتخذة بناءً على المعالجة المؤتمتة بما فيها الترميز.
 - د. القطاعات أو المنشآت المستهدفة التي سيتم مشاركة بياناته الشخصية معهم من داخل وخارج الدولة.
 - هـ. ضوابط ومعايير مدد تخزين وحفظ بياناته الشخصية.
 - و. إجراءات تصحيح أو محو أو تقييد المعالجة والاعتراض على بياناته الشخصية.
 - ز. تدابير الحماية الخاصة بالمعالجة عبر الحدود التي تتم وفقاً للمادتين (22) و (23) من هذا المرسوم بقانون.
 - ح. الإجراءات التي ستتخذ في حال اختراق أو انتهاك بياناته الشخصية، خاصة إن كان الاختراق أو الانتهاك له خطر مباشر وجسيم على خصوصية وسرية بياناته الشخصية.
 - ط. كيفية تقديم الشكاوى للمكتب.
2. في جميع الأحوال، يجب على المتحكم، وقبل البدء بالمعالجة، تزويد صاحب البيانات بالمعلومات المنصوص عليها في الفقرات (ب) و (د) و (ز) من البند (1) من هذه المادة.

3. يجوز للمتحكم رفض طلب صاحب البيانات في الحصول على المعلومات الواردة في البند (1) من هذه المادة، في حال تبين له ما يأتي:
- أ. أن الطلب لا يتعلق بالمعلومات المشار إليها في البند (1) من هذه المادة أو كان متكرراً بشكل مبالغ به.
 - ب. أن الطلب يتعارض مع الإجراءات القضائية أو التحقيقات التي تجريها الجهات المختصة.
 - ج. أن الطلب قد يؤثر سلباً على جهود المتحكم في حماية أمن المعلومات.
 - د. أن الطلب يمس بخصوصية وسرية البيانات الشخصية للغير.

المادة (14)

حق طلب نقل البيانات الشخصية

1. يحق لصاحب البيانات الحصول على البيانات الشخصية الخاصة به التي تم تزويدها للمتحكم لمعالجتها، وذلك بشكل منظم وقابل للقراءة ألياً متى ما كانت المعالجة مبنية على موافقة صاحب البيانات، أو ضرورة لتنفيذ التزام عقدي، ومنفذة بوسائل مؤتمتة.
2. يحق لصاحب البيانات طلب نقل بياناته الشخصية لمتحكم آخر متى ما كان ذلك ممكناً من الناحية التقنية.

المادة (15)

حق تصحيح أو محو البيانات الشخصية

1. يحق لصاحب البيانات طلب تصحيح بياناته الشخصية غير الدقيقة، أو استكمالها لدى المتحكم دون تأخير غير مبرر.
2. دون الإخلال بالتشريعات السارية في الدولة وما تتطلبه المصلحة العامة، يحق لصاحب البيانات طلب محو بياناته الشخصية الخاصة لدى المتحكم في أي من الحالات الآتية:
 - أ. لم تعد بياناته الشخصية ضرورية للأغراض التي جُمعت أو عُولجت من أجلها.
 - ب. عدول صاحب البيانات عن الموافقة التي بُنيت عليها المعالجة.
 - ج. اعتراض صاحب البيانات على المعالجة، أو غياب الأسباب المشروعة للمتحكم في الاستمرار بالمعالجة.
 - د. أن معالجة بياناته الشخصية تمت بالمخالفة لأحكام هذا المرسوم بقانون والتشريعات السارية، وأن عملية المحو ضرورية للامتثال للتشريعات والمعايير المعتمدة المعمول بها في هذا الشأن.
3. استثناء مما ورد في البند (2) من هذه المادة لا يحق لصاحب البيانات طلب محو بياناته الشخصية لدى المتحكم في الحالات الآتية:
 - أ. في حال كان الطلب يتعلق بمحو بياناته الشخصية المتعلقة بالصحة العامة لدى المنشآت الخاصة.
 - ب. إذا كان الطلب يؤثر على إجراءات التحقيق والمطالبة بالحقوق والدعاوى القانونية أو الدفاع عنها لدى المتحكم.
 - ج. إذا كان الطلب يتعارض مع تشريعات أخرى يخضع لها المتحكم.
 - د. أي حالات أخرى تحددها اللائحة التنفيذية لهذا المرسوم بقانون.

المادة (16)

حق تقييد المعالجة

1. يحق لصاحب البيانات إلزام المتحكم بتقييد وإيقاف المعالجة في أي من الحالات الآتية:
 - أ. اعتراض صاحب البيانات على دقة بياناته الشخصية، وفي هذه الحالة يتم تقييد المعالجة لفترة محددة تسمح للمتحكم التحقق من دقتها.
 - ب. اعتراض صاحب البيانات على معالجة بياناته الشخصية بالمخالفة للأغراض المتفق عليها.
 - ج. أن تكون المعالجة قد تمت بالمخالفة لأحكام هذا المرسوم بقانون والتشريعات السارية.
2. يحق لصاحب البيانات الطلب من المتحكم الاستمرار بالاحتفاظ ببياناته الشخصية لما بعد انتهاء أغراض المعالجة، كون هذه البيانات ضرورية له لاستكمال إجراءات متعلقة بالمطالبة بالحقوق والدعاوى القضائية أو الدفاع عنها.
3. على الرغم مما ورد في البند (1) من هذه المادة، للمتحكم المضي في معالجة البيانات الشخصية لصاحب البيانات دون موافقته في أي من الحالات الآتية:
 - أ. إذا كانت المعالجة مقتصرة على تخزين البيانات الشخصية.
 - ب. إذا كانت المعالجة ضرورية لإقامة أي من إجراءات المطالبة بالحقوق والدعاوى القانونية أو الدفاع عنها أو تتعلق بالإجراءات القضائية.
 - ج. إذا كانت المعالجة ضرورية لحماية حقوق الغير وفقاً للتشريعات السارية.
 - د. إذا كانت المعالجة ضرورية لحماية المصلحة العامة.
4. وفي جميع الأحوال، يجب على المتحكم في حال قام برفع التقييد المنصوص عليه في هذه المادة، أن يخطر صاحب البيانات بذلك.

المادة (17)

الحق في إيقاف المعالجة

- يحق لصاحب البيانات الاعتراض على معالجة بياناته الشخصية وإيقاف المعالجة في أي من الحالات الآتية:
1. إذا كانت المعالجة لأغراض التسويق المباشر بما في ذلك التنميط ذات العلاقة بالتسويق المباشر.
 2. إذا كانت المعالجة لأغراض إجراء المسوح الإحصائية، إلا إذا كانت المعالجة لازمة لتحقيق المصلحة العامة.
 3. إذا كانت المعالجة بالمخالفة لأحكام المادة (5) من هذا المرسوم بقانون.

المادة (18)

حق المعالجة والمعالجة المؤتمتة

1. يحق لصاحب البيانات الاعتراض على القرارات التي تصدر عن المعالجة المؤتمتة وتكون لها تبعات قانونية أو تؤثر بشكل جسيم على صاحب البيانات، بما فيها التنميط.
2. على الرغم مما ورد في البند (1) من هذه المادة، لا يجوز لصاحب البيانات الاعتراض على القرارات التي تصدر عن المعالجة المؤتمتة في الحالات الآتية:
 - أ. إذا كانت المعالجة المؤتمتة ضمن شروط التعاقد بين صاحب البيانات والمتحكم.
 - ب. إذا كانت المعالجة المؤتمتة ضرورية وفق تشريعات أخرى نافذة في الدولة.
 - ج. إذا تمت الموافقة المسبقة من صاحب البيانات على المعالجة المؤتمتة وفق الشروط المحددة في المادة (6) من هذا المرسوم بقانون.
3. يجب على المتحكم تطبيق إجراءات وتدابير مناسبة لحماية خصوصية وسرية البيانات الشخصية لصاحب البيانات في الحالات المشار إليها في البند (2) من هذه المادة، وعدم الإضرار والمساس بحقوقه.
4. يتعين على المتحكم إدخال العنصر البشري في مراجعة قرارات المعالجة المؤتمتة بناءً على طلب صاحب البيانات.

المادة (19)

طرق التواصل مع المتحكم

- على المتحكم توفير طرق وآليات مناسبة وواضحة لتمكين صاحب البيانات من التواصل معه وطلب ممارسة أي من حقوقه المنصوص عليها في هذا المرسوم بقانون.

المادة (20)

أمن معلومات البيانات الشخصية

1. يجب على المتحكم والمعالج وضع واتخاذ إجراءات وتدابير تقنية وتنظيمية ملائمة، لضمان تطبيق مستوى أمن المعلومات الذي يتناسب مع المخاطر المصاحبة للمعالجة وفق أفضل المعايير والممارسات الدولية، ويمكن أن يشمل ذلك التالي:
 - أ. تشفير البيانات الشخصية وتطبيق آلية إخفاء البيانات.
 - ب. تطبيق إجراءات وتدابير تضمن استمرار سرية أنظمة وخدمات المعالجة، وسلامتها وصحتها ومرونتها.
 - ج. تطبيق إجراءات وتدابير تضمن استرجاع البيانات الشخصية والوصول إليها في الوقت المحدد في حال حدوث أي عطل فعلي أو فني.
 - د. تطبيق إجراءات تضمن سلسلة عملية اختبار وتقييم وتأمين فاعلية التدابير التقنية والتنظيمية بما يضمن أمن المعالجة.

2. يراعى عند تقييم مستوى أمن المعلومات المنصوص عليه في البند (1) من هذه المادة، ما يأتي:
- المخاطر المصاحبة للمعالجة، بما فيها تلف البيانات الشخصية أو ضياعها أو التعديل العرضي عليها أو غير القانوني لها أو الإفشاء أو الوصول غير المصرح به لها سواء تم نقلها أو تخزينها أو معالجتها.
 - تكاليف تنفيذ المعالجة وطبيعتها ونطاقها وأغراضها، وكذلك تباين المخاطر المحتملة على خصوصية وسرية البيانات الشخصية لصاحب البيانات.

المادة (21)

تقييم أثر حماية البيانات الشخصية

- مع مراعاة طبيعة المعالجة ونطاقها وأغراضها، يجب على المتحكم قبل القيام بإجراء المعالجة، أن يقوم بتقييم أثر عمليات المعالجة المقترحة على حماية البيانات الشخصية، وذلك عند استخدام أي من التقنيات الحديثة التي من شأنها أن تشكل خطراً عالياً على خصوصية وسرية البيانات الشخصية لصاحب البيانات.
- يكون تقييم الأثر المنصوص عليه في البند (1) من هذه المادة ضرورياً في الأحوال الآتية:
 - إذا كانت المعالجة تتضمن تقييم ممنهج وشامل للجوانب الشخصية بصاحب البيانات التي تعتمد على المعالجة المؤتمتة بما فيها الترميز والتي لها تبعات قانونية أو التي من شأنها أن تؤثر بشكل جسيم على صاحب البيانات.
 - إذا كانت المعالجة ستتم على حجم كبير من البيانات الشخصية الحساسة.
- يجب أن يتضمن التقييم المنصوص عليه في البند (1) من هذه المادة بعد أدنى على ما يأتي:
 - شرح واضح وممنهج لعمليات المعالجة المقترحة على حماية البيانات الشخصية والغرض من معالجتها.
 - تقييم مدى ضرورة وتناسب عمليات المعالجة مع الغرض منها.
 - تقييم المخاطر المحتملة على خصوصية وسرية البيانات الشخصية لصاحب البيانات.
 - الإجراءات والتدابير المقترحة للحد من المخاطر المحتملة على حماية البيانات الشخصية.
- يجوز للمتحكم إجراء تقييم واحد لمجموعة من عمليات المعالجة التي تتماثل في طبيعتها ومخاطرها.
- على المتحكم التنسيق مع مسؤول حماية البيانات عند تقييم أثر حماية البيانات الشخصية.
- على المكتب إعداد قائمة بنوع عمليات المعالجة غير الملزمة بتقييم أثر حماية البيانات الشخصية وإتاحتها للعموم من خلال الموقع الإلكتروني الخاص بها.
- على المتحكم مراجعة مخرجات التقييم بشكل دوري للتأكد من تنفيذ المعالجة وفقاً للتقييم في حال اختلف مستوى المخاطر المصاحبة لعمليات المعالجة.

المادة (22)

نقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة

في حال وجود مستوى حماية ملائم

يجوز نقل البيانات الشخصية إلى خارج الدولة في الأحوال الآتية المعتمدة من المكتب:

1. أن تكون للدولة أو الإقليم الذي سيتم نقل البيانات الشخصية إليها تشريعات خاصة بحماية البيانات الشخصية فيها، تتضمن أهم الأحكام والتدابير والضوابط والاشتراطات والقواعد الخاصة بحماية خصوصية وسرية البيانات الشخصية لصاحب البيانات، وقدرته على ممارسة حقوقه، وأحكام تتعلق بفرض التدابير المناسبة على المتحكم أو المعالج من خلال جهة رقابية أو قضائية.
2. انضمام الدولة إلى الاتفاقيات الثنائية أو متعددة الأطراف المتعلقة بحماية البيانات الشخصية مع الدول التي سيتم نقل البيانات الشخصية إليها.

المادة (23)

نقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة

في حال عدم وجود مستوى حماية ملائم

1. استثناء مما ورد في المادة (22) من هذا المرسوم بقانون، يجوز نقل البيانات الشخصية إلى خارج الدولة في الحالات التالية:
 - أ. في الدول التي لا يتوفر فيها قانون لحماية البيانات، يجوز للمنشآت العاملة في الدولة وفي تلك الدول أن تنقل البيانات بموجب عقد أو اتفاقية يلزم المنشأة في تلك الدول بتطبيق الأحكام والتدابير والضوابط والاشتراطات الواردة في هذا المرسوم بقانون شاملاً أحكاماً تتعلق بفرض التدابير المناسبة على المتحكم أو المعالج من خلال جهة رقابية أو قضائية معنية في تلك الدولة وتحدد في العقد.
 - ب. الموافقة الصريحة من صاحب البيانات على نقل بياناته الشخصية خارج الدولة بما لا يتعارض مع المصلحة العامة والأمنية للدولة.
 - ج. إذا كان النقل ضروري لتنفيذ التزامات وإثبات الحقوق أمام الجهات القضائية أو ممارستها أو الدفاع عنها.
 - د. إذا كان النقل ضروري لإبرام أو تنفيذ عقد مبرم بين المتحكم وصاحب البيانات، أو بين المتحكم والغير لتحقيق مصلحة صاحب البيانات.
 - هـ. إذا كان النقل ضروري لتنفيذ إجراء متعلق بتعاون قضائي دولي.
 - و. إذا كان النقل ضروري لحماية المصلحة العامة.
2. تحدد اللائحة التنفيذية لهذا المرسوم بقانون الضوابط والاشتراطات للحالات المشار إليها في البند (1) من هذه المادة، والتي يجب أن تتوفر في حالات نقل البيانات الشخصية إلى خارج الدولة.

المادة (24)

تقديم الشكوى

1. لصاحب البيانات أن يتقدم إلى المكتب بشكوى، إذا كان لديه ما يحمله على الاعتقاد بوقوع أي مخالفة لأحكام هذا المرسوم بقانون، أو بأن المتحكم أو المعالج يقوم بمعالجة بياناته الشخصية بالمخالفة لأحكامه وفقاً للإجراءات والقواعد التي يحددها المكتب في هذا الشأن.
2. يتولى المكتب استلام الشكاوى المقدمة من صاحب البيانات وفقاً للبند (1) من هذه المادة، والتحقق منها بالتنسيق مع المتحكم والمعالج.
3. للمكتب توقيع الجزاءات الإدارية المشار إليها في المادة (26) من هذا المرسوم بقانون في حال ثبوت مخالفة المتحكم أو المعالج لأحكامه أو مخالفة القرارات الصادرة تنفيذاً له.

المادة (25)

التظلم من قرارات المكتب

- يجوز لكل ذي مصلحة التظلم خطياً لمدير عام المكتب من أي قرار أو جزاء إداري أو إجراء اتخذ بحقه من قبل المكتب، وذلك خلال (30) ثلاثين يوماً من تاريخ إخطاره بذلك القرار أو الجزاء الإداري أو الإجراء، ويتم البت في هذا التظلم خلال (30) ثلاثين يوماً من تاريخ تقديمه.
- ولا يجوز الطعن على أي قرار يصدره المكتب تطبيقاً لأحكام هذا المرسوم بقانون، دون التظلم منه. وتبين اللائحة التنفيذية لهذا المرسوم بقانون إجراءات التظلم والبت فيه.

المادة (26)

الجزاءات والمخالفات الإدارية

- يصدر مجلس الوزراء - بناءً على اقتراح مدير عام المكتب - قراراً بتحديد الأفعال التي تشكل مخالفة لأحكام هذا المرسوم بقانون ولأئحته التنفيذية، والجزاءات الإدارية التي يتم توقيعها.

المادة (27)

التفويض

- لمجلس الوزراء - بناءً على اقتراح مدير عام المكتب - تفويض أي من الجهات الحكومية المحلية المختصة وفي نطاق اختصاصها المحلي، ببعض الاختصاصات المنوطة بالمكتب في هذا المرسوم بقانون.

المادة (28)

اللائحة التنفيذية

- يصدر مجلس الوزراء - بناءً على اقتراح مدير عام المكتب - اللائحة التنفيذية لهذا المرسوم بقانون، وذلك خلال (6) ستة أشهر من تاريخ صدوره.

المادة (29)

توفيق الأوضاع

على المتحكم والمعالج توفيق أوضاعهما بما يتفق وأحكام هذا المرسوم بقانون خلال مدة لا تزيد على (6) ستة أشهر من تاريخ صدور لائحته التنفيذية، ويجوز لمجلس الوزراء تمديد هذه المهلة لمدة أخرى مماثلة.

المادة (30)

الإلغاءات

يُلغى كل حكم يخالف أو يتعارض مع أحكام هذا المرسوم بقانون.

المادة (31)

نشر المرسوم بقانون والعمل به

يُنشر هذا المرسوم بقانون في الجريدة الرسمية، ويُعمل به اعتباراً من 2 يناير 2022م.

خليفة بن زايد آل نهيان

رئيس دولة الإمارات العربية المتحدة

صدر عنا في قصر الرئاسة بأبوظبي:

بتاريخ: 13 / صفر / 1443هـ

الموافق: 20 / سبتمبر / 2021م