NDMO
مكتب إدارة البيانات الوطنية
National Data Management Office

القواعد العامة
لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة

النسخة الأولى
2020/11/25 م

جدول المحتويات

مقدمة 5

التعريفات 6

الأهداف 7

النطاق 7

حقوق أصحاب البيانات 7

التزامات الجهات 8

أحكام عامة 10

1. مقدمة

يعتبر التدفق الحر للبيانات عبر الحدود – بما في ذلك البيانات الشخصية – من أهم الأسس التي يقوم عليها الاقتصاد العالمي في هذا العصر مما يتطلب تحقيق التوازن بين التنمية الاقتصادية والمحافظة على خصوصية أصحاب البيانات الشخصية. ومن هذا المنطلق، سعت العديد من الدول في جميع أنحاء العالم إلى الاستفادة من تبادل البيانات باعتبارها مورداً اقتصادياً يساهم في دعم التحولات الاقتصادية ويعزز المقومات التنافسية للدول وذلك من خلال سن الأنظمة والتشريعات التي تنظّم عمليات نقل البيانات الشخصية عبر الحدود الجغرافية للدول. وعلى الصعيد الوطني، تسعى المملكة إلى وضع السياسات والمعايير الخاصة بنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة بما يضمن المحافظة على السيادة الوطنية على هذه البيانات، وكذلك المحافظة على خصوصية أصحاب البيانات الشخصية وحماية حقوقهم من خلال تحديد التزامات جهات التحكم والمعالجة حيال عمليات نقل البيانات الشخصية خارج الحدود الجغرافية، وتوفير الوسائل المناسبة التي تمكّن أصحاب البيانات من ممارسة حقوقهم، وتحديد أدوار ومسؤوليات هذه الجهات بالإضافة إلى الجهات التنظيمية والجهات الإشرافية على تطبيق أحكام هذه السياسات.

2. التعريفات

لأغراض تطبيق هذه القواعد العامة، يُقصد بالكلمات والمصطلحات الواردة أدناه -أينما وردت في هذه الوثيقة - المعاني الموضحة أمام كل منها، ما لم يقتضِ سياق النص خلاف ذلك:

البيانات الشخصية: كل بيان – مهما كان مصدره أو شكله – من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلاً للتعرف عليه بصفة مباشرة أو غير مباشرة عند دمجه مع بيانات أخرى، ويشمل ذلك – على سبيل المثال لا الحصر – الاسم، وأرقام الهويات الشخصية، والعناوين، وأرقام التواصل، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور المستخدم الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي.

البيانات الشخصية الحساسة: كل بيان شخصي يتضمن الإشارة إلى أصل الفرد العرقي أو القبلي، أو معتقده الديني أو الفكري أو السياسي، أو يدل على عضويته في جمعيات أو مؤسسات أهليه. وكذلك البيانات الجنائية والأمنية، وبيانات السمات الحيوية التي تحدد الهوية، والبيانات الوراثية، والبيانات المالية والائتمانية، والبيانات الصحية، وبيانات تحديد المواقع، والبيانات المتعلقة بأسرة الفرد، والبيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهما.

نقل البيانات الشخصية: إرسال البيانات الشخصية إلى جهة خارج الحدود الجغرافية للمملكة – بأي وسيلة كانت – بهدف معالجتها سواء كانت بطريقة مباشرة أو غير مباشرة وفقاً لأغراض محددة مبنية على أسس نظامية – بما في ذلك النقل لأغراض أمنية أو لحماية الصحة أو السلامة العامة أو تنفيذاً لاتفاقية تكون المملكة طرفاً فيها.

النقل المباشر: نقل البيانات الشخصية من الجهة المرسلة إلى الجهة المستقبلة دون مرور البيانات بأي جهة أخرى.

النقل غير المباشر: نقل البيانات الشخصية من الجهة المرسلة إلى الجهة المستقبلة مروراً بجهة أخرى أو أكثر.

النقل العرضي: نقل البيانات الشخصية بشكل غير متكرر أو منتظم – عادةً ما يكون لمرة واحده – لعدد محدود من الأشخاص، ومنها على سبيل المثال، نقل البيانات لغرض الاستفادة من خدمة في دولة أخرى لمصلحة صاحب البيانات.

قائمة الاعتماد: قائمة معتمدة من مكتب إدارة البيانات الوطنية تتضمن أسماء الدول التي تتمتع بمستوى كافٍ من الحماية لحقوق أصحاب البيانات فيما يتعلق بمعالجة بياناتهم الشخصية.

جهة التحكم: أي جهة حكومية أو جهة اعتبارية عامة مستقلة في المملكة، وأي شخصية ذات صفة طبيعية أو اعتبارية خاصة؛ تحدد الغرض من معالجة البيانات الشخصية وكيفية ذلك؛ سواء تمت معالجة البيانات بواسطتها أو من خلال جهة المعالجة.

جهة المعالجة: أي جهة حكومية أو جهة اعتبارية عامة مستقلة في المملكة، وأي شخصية ذات صفة طبيعية أو اعتبارية خاصة؛ تعالج البيانات الشخصية لمصلحة جهة التحكم ونيابةً عنها.

الجهة العامة: أي جهة حكومية أو جهة اعتبارية عامة مستقلة في المملكة، أو أي من الجهات التابعة لها – وتعد في حكم الجهة العامة أي شركة تقوم بإدارة المرافق العامة أو البنى التحتية الوطنية أو تشغيلها أو صيانتها، أو تقوم بمباشرة خدمة عامة فيما يخص إدارة تلك المرافق أو البنى التحتية.

الجهة التنظيمية: أي جهة حكومية أو جهة اعتبارية عامة مستقلة تتولى مهام ومسؤوليات تنظيمية أو رقابية لقطاع معين في المملكة العربية السعودية بناءً على مستند نظامي.

المكتب: مكتب إدارة البيانات الوطنية

3. الأهداف

إشارةً إلى قرار مجلس الوزراء رقم (292) وتاريخ 1441/04/27هـ، القاضي في الفقرة (1) من المادة عاشراً بأن "يتولى المكتب وضع السياسات وآليات الحوكمة والمعايير والضوابط الخاصة بالبيانات والذكاء الاصطناعي ومتابعة الالتزام بها بعد إقرارها"، عليه فقد قام مكتب إدارة البيانات الوطنية بالاستفادة من الممارسات والمعايير العالمية عند إعداد القواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة والتي تهدف إلى:

1. دعم وتعزيز جهود المملكة في تحقيق الرؤية والاستراتيجيات الوطنية.
2. المحافظة على السيادة الوطنية الرقمية على البيانات الشخصية.
3. العمل على توفير أفضل مستويات الحماية عند نقل البيانات الشخصية خارج الحدود الجغرافية للمملكة لضمان المحافظة على خصوصية أصحابها وحماية حقوقهم.
4. ايجاد التوازن بين الآثار والمخاطر المحتملة والحاجة إلى نقل البيانات الشخصية لأغراض محددة مبنية على أسس نظامية.
5. ضمان الامتثال لسياسة حماية البيانات الشخصية عند نقل البيانات خارج الحدود الجغرافية للمملكة.

4. النطاق

تنطبق أحكام هذه الوثيقة على جميع الجهات العامة والخاصة وكذلك الجهات غير الربحية في المملكة – المشمولة بنطاق تطبيق سياسة حماية البيانات الشخصية – والتي تقوم بنقل البيانات الشخصية إلى جهات أخرى خارج الحدود الجغرافية للمملكة بغرض معالجتها، ويستثنى من ذلك نقل البيانات الشخصية من وإلى الأفراد مباشرة.

5. حقوق أصحاب البيانات

إشارةً إلى سياسة حماية البيانات الشخصية، فإن المبادئ الأساسية لحماية تمنح الأفراد حقوقًا محددة فيما يتعلق بمعالجة بياناتهم الشخصية، بينما تحدد التزامات جهات التحكم القواعد العامة التي يجب الالتزام بها عند معالجتها. وفيما يتعلق بنقل البيانات الشخصية عبر الحدود، فإن لصاحب البيانات نفس الحقوق الموضحة في سياسة حماية البيانات الشخصية مع التأكيد على الحقوق التالية:

أولاً: الحق في العلم ويشمل ذلك إشعاره بالأساس النظامي أو الاحتياج الفعلي لنقل بياناته الشخصية خارج الحدود الجغرافية للمملكة ومكان تخزينها أو استضافتها، والجهات التي سيتم الإفصاح لها عن بياناته الشخصية عند نقلها، والغرض من هذا النقل، وأخذ موافقته على ذلك، والتدابير الأمنية المتخذة لحماية بياناته الشخصية أثناء وبعد النقل.

ثانياً: الحق في الرجوع عن موافقته على معالجة بياناته الشخصية خارج الحدود – في أي وقت – مالم يكن الغرض من نقل البيانات تحقيقاً للمصلحة العامة، أو حمايةً للمصالح الحيوية للأفراد، أو تنفيذاً لمتطلبات نظامية.

ثالثاً: الحق في الوصول إلى بياناته الشخصية لدى جهة التحكم/جهة المعالجة الخارجية، وذلك للاطلاع عليها، وطلب تصحيحها، أو إتمامها، أو تحديثها، وطلب إتلاف ما انتهت الحاجة إليه منها، والحصول على نسخة منها بصيغة واضحة.

6. التزامات الجهات

الأصل في المعالجة أن تكون داخل الحدود الجغرافية للمملكة، حيث تقوم الجهة بتخزين البيانات الشخصية ومعالجتها داخل المملكة لضمان المحافظة على السيادة الوطنية على هذه البيانات وحماية خصوصية أصحابها، ولا يجوز نقلها أو معالجتها خارج المملكة إلا بعد التحقق من الحالات الموضحة أدناه حسب التسلسل التالي:

1. إذا كانت جهة المعالجة الخارجية المسند إليها أنشطة معالجة البيانات الشخصية في دولة ضمن قائمة الاعتماد، فتقوم جهة التحكم/جهة المعالجة الداخلية بأخذ موافقة كتابية من الجهة التنظيمية على نقل البيانات، وعلى الجهة التنظيمية التنسيق مع المكتب.
2. إذا كانت جهة المعالجة الخارجية في دولة ليست ضمن قائمة الاعتماد، فإن نقل البيانات الشخصية خارج الحدود الجغرافية للمملكة يتطلب مستوى كافٍ من الحماية – لا يقل عن مستوى الحماية الذي كفلته سياسة حماية البيانات الشخصية الصادرة من المكتب – بعد إجراء تقييم مستوى الحماية التي توفرها جهة المعالجة الخارجية.
3. إذا لم يكن هناك مستوى كافٍ من الحماية، فتقوم الجهة بوضع ضمانات مناسبة لحماية حقوق أصحاب البيانات، ومنها على سبيل المثال، استخدم البنود القياسية، أو القواعد الملزمة.
4. إذا لم تتمكن الجهة من توفير الضمانات الكافية، فيمكن الاعتماد على أحد الاستثناءات النظامية التي تتطلب نقل البيانات والموضحة في البند (ثالثاً) أدناه.

في جميع الحالات الواردة في الفقرات (2) و (3) و(4) أعلاه، يجب على جهة التحكم أو المعالجة الداخلية الحصول على موافقة كتابية من الجهة التنظيمية على نقل البيانات، وعلى الجهة التنظيمية التنسيق مع المكتب.

أولاً: تقييم مستوى الحماية

يجب أن تقوم الجهة التي ترغب بنقل البيانات خارج الحدود الوطنية بإجراء تقييم الآثار والمخاطر المحتملة – لكل حاله على حده – لتحديد ما إذا كانت جهة التحكم/جهة المعالجة الخارجية ستوفر مستوى كافٍ من الحماية لحقوق أصحاب البيانات وعرض نتائج التقييم على (المسؤول الأول للجهة) لتحديد مستوى قبول المخاطر وإقرارها. وللقيام بذلك يجب أن تقوم الجهة بالالتزام بمعايير التقييم سواء المعايير العامة أو القانونية – وذلك لضمان أن يكون مستوى الحماية ملائماً في جميع الظروف:

أ- معايير التقييم العامة

- **طبيعة وحساسية البيانات:** يجب على الجهة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار نوع وقيمة وحجم البيانات المراد نقلها ودرجة حساسيتها، حيث إن نقل البيانات الشخصية الحساسة يتطلب مستوى عالٍ من الحماية.
- **الغرض من معالجة البيانات:** يجب على الجهة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار الغرض من المعالجة والفئة المستهدفة من أصحاب البيانات ونطاق المعالجة والجهات التي سيتم مشاركة البيانات معها، حيث إن معالجة بيانات شخصية حساسة على نطاق واسع يتطلب مستوى عالٍ من الحماية.
- **الفترة التي يتم خلالها معالجة البيانات:** يجب على الجهة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار ما إذا كانت المعالجة ستتم بشكل مقيّد أو عرضي – لمرة واحدة فقط أو لفترة محدودة – أو ستتم بشكل متكرر ومنتظم، حيث إن البيانات الشخصية التي سيتم معالجتها بشكل منتظم وعلى المدى الطويل تتطلب مستوى عالٍ من الحماية.

- **منشأ البيانات:** يجب على الجهة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار الدولة التي جُمعت منها البيانات – ليس بالضرورة الدولة التي سيتم نقل البيانات منها – وذلك لتحديد توقعات أصحاب البيانات فيما يتعلق بمستوى الحماية، حيث إن نقل البيانات الشخصية التي تم جمعها من دول تخضع لمستوى حماية عالٍ جداً يتطلب مستوى لا يقل عن مستوى الحماية في هذه الدول.
- **الوجهة النهائية للبيانات:** يجب على الجهة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار المراحل التي يتم بها نقل البيانات الشخصية – والتي قد تمر بأكثر من دولة أحياناً – وتقييم مستوى الحماية في الدولة التي تعتبر هي الوجهة النهائية – أخر مرحلة من مراحل النقل.
- **الضوابط الأمنية:** يجب على الجهة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار الإجراءات الإدارية والتدابير التقنية والضوابط المادية المعتمدة في سياسات الجهة لأمن المعلومات، كالتشفير والضوابط الأمنية والمعايير الدولية.

إذا أظهرت نتائج تقييم مستوى الحماية – بناءً على المعايير العامة – أنه بالظروف الخاصة للحالة يكون الآثار السلبية على حقوق أصحاب البيانات محدودة والمخاطر المحتملة منخفضة، فقد لا يكون تقييم مستوى الحماية – بناءً على المعايير القانونية – ضروري في هذه الحالة.

ب- معايير التقييم القانونية:

يجب أن تقوم الجهة التي ترغب بنقل البيانات خارج الحدود الوطنية بمراعاة هذه المعايير عندما تكون نتائج تقييم الآثار والمخاطر المحتملة في الفقرة (أ) أعلاه غير كافيه، ومن هذه الحالات على سبيل المثال، أن يتم نقل بيانات شخصية حساسة بشكل دائم ومنتظم وعلى نطاق واسع.

- **الأنظمة والتشريعات النافذة:** يجب على الجهة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار ما إذا كان في الدولة – المراد نقل البيانات لها – أنظمة وتشريعات تحمي حقوق أصحاب البيانات فيما يتعلق بمعالجة بياناتهم الشخصية، وتضمن قدرة الأطراف المشاركة على التعاقد والالتزام بموجب هذه العقود.
- **الالتزامات الدولية:** يجب على الجهة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار ما إذا كانت الدولة – المراد نقل البيانات لها – طرفاً في اتفاقيات دولية أو تتبنى مبادئ ومعايير دولية لحماية البيانات الشخصية.
- **القواعد والممارسات المعتمدة:** يجب على الجهة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار ما إذا كانت الدولة – المراد نقل البيانات لها – تعتمد قواعد سلوكية أو ممارسات عامة أو معايير خاصة لحماية البيانات الشخصية.

ثانياً: الضمانات المناسبة

إذا كانت الجهة في دولة ليست من ضمن قائمة الاعتماد ولم تخضع لتقييم مستوى الحماية أو كان مستوى الحماية غير كافٍ، فيجب عليها توفير الضمانات المناسبة لحماية البيانات الشخصية، ومنها:

- **البنود التعاقدية القياسية:** يجب على الجهة أن تضمّن في العقود والاتفاقيات بنود نموذجية أو قياسية – يتم الموافقة عليها من قبل المكتب – لتقييد نقل البيانات الشخصية خارج الحدود الجغرافية للمملكة بما يضمن المحافظة على خصوصية أصحابها وحماية حقوقهم.
- **القواعد المشتركة الملزمة:** يجب على جهة التحكم وجهة المعالجة – كلٍ على حده – التي تعمل ضمن مجموعة متعددة الجنسيات أن تقوم بإعداد قواعد مشتركة داخلية ملزمة قانونياً تنطبق على عمليات نقل البيانات الشخصية خارج الحدود بما في ذلك معالجة انتهاكات الخصوصية والإشعار عنها – على أن تتم الموافقة عليها من قبل المكتب، ويتم تضمين هذه القواعد المشتركة كملحق لاتفاقيات مستوى الخدمة أو العقود المبرمة بين الجهتين. كما يجب على جهة التحكم أخذ موافقة الجهة التنظيمية عند وجود أي التزام قانوني تخضع له هذه الجهة أو أحد الجهات التابعة لها في دولة أخرى يرجّح أن يكون له أثر سلبي على الضمانات التي توفرها القواعد المشتركة الملزمة.

- **قواعد السلوك المعتمدة:** أن تقوم الجهات باستخدام قواعد السلوك المعتمدة من الجهات التنظيمية أو المكتب كأداة فعّالة تحدّد الالتزامات على جهات التحكم والمعالجة لضمان المحافظة على خصوصية أصحاب البيانات وحماية حقوقهم.
- **الشهادات المعتمدة:** أن تقوم الجهات بالاستعانة بأطراف خارجية مستقلة تتولى إصدار شهادات اعتماد تؤكد وجود الضمانات المناسبة التي توفرها جهات التحكم أو جهات المعالجة الخارجية. كما تقوم هذه الجهات بتقديم التزامات قابلة للتنفيذ لتطبيق هذه الضمانات بما في ذلك الأحكام المتعلقة بحقوق أصحاب البيانات.
- **الاتفاقيات الملزمة بين الجهات العامة:** أن تقوم الجهات العامة – سواءً جهات التحكم أو جهات المعالجة – بتوقيع اتفاقية ملزمة قانونياً لنقل البيانات الشخصية على أن تتضمن هذه الاتفاقية على بنود تعاقدية ملزمة تضمن المحافظة على خصوصية أصحاب البيانات وتحمي حقوقهم.

ثالثاً: الاستثناءات لحالات محددة

يمكن للجهات نقل البيانات الشخصية خارج الحدود الجغرافية دون الالتزام بالشروط والأحكام الموضحة في البند (أولاً) والبند (ثانياً) أعلاه في حالات محددة، ومنها أن يكون نقل البيانات خارج الحدود الجغرافية للمملكة:

1. استنادًا على موافقة أصحاب البيانات.
2. تنفيذاً لالتزام تعاقدي ويكون صاحب البيانات طرفاً فيه.
3. تنفيذاً لمتطلبات قضائية.
4. تنفيذاً لأحكام نظام آخر أو اتفاقية دولية تكون المملكة طرفاً فيها.
5. للمحافظة على المصلحة العامة – بما في ذلك حماية الصحة أو السلامة العامة.
6. لحماية المصالح الحيوية لأصحاب البيانات.

في جميع هذه الحالات الواردة في الفقرات (1)، (2)، (3)، (4)، (5)، يجب على جهة التحكم أو المعالجة الداخلية الحصول على موافقة كتابية من الجهة التنظيمية على نقل البيانات – كل حالة على حدة – وعلى الجهة التنظيمية التنسيق مع المكتب. أما ما يتعلق بالحالة الواردة في الفقرة (6) فيجب على جهة التحكم أو جهة المعالجة إشعار الجهة التنظيمية فقط، وعلى الجهة التنظيمية إشعار المكتب بذلك.

7. أحكام عامة

أولاً: تتولى الجهات التنظيمية موائمة هذه الوثيقة مع وثائقها التنظيمية وتعميمها على جميع الجهات التابعة لها أو المرتبطة بها بما يحقق التكامل ويضمن تحقيق الهدف المنشود من إعداد هذه القواعد.

ثانياً: تقوم الجهات التنظيمية بمراقبة امتثال الجهات التابعة لها أو المرتبطة بها لهذه القواعد بشكل دوري.

ثالثاً: يجب على جهات التحكم وجهات المعالجة الامتثال لهذه القواعد وتوثيق الامتثال وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية.

رابعاً: يجب على جهات التحكم عند تعاقدها مع جهات المعالجة – داخل أو خارج المملكة – أن تتحقق بشكل دوري من امتثال جهات المعالجة لهذه القواعد وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها جهات المعالجة.

خامساً: يمارس المكتب أدوار ومهام الجهات التنظيمية على جهات التحكم غير الخاضعة لجهات تنظيمية.

سادساً: يحق للجهات التنظيمية وضع قواعد إضافية لنقل أنواع محددة من البيانات الشخصية وفقاً لطبيعة وحساسية هذه البيانات بعد التنسيق مع المكتب.

سابعاً: يقوم المكتب بمراجعة معايير التقييم – العامة والقانونية – المتعلقة بحماية البيانات الشخصية عند نقلها خارج الحدود الجغرافية للمملكة واتخاذ القرارات المنظمة لها.

ثامناً: يقوم المكتب بوضع قائمة محددة للعوامل الرئيسية التي تحدد مستوى الحماية المناسب، ومنها على سبيل المثال، الأنظمة والتشريعات، حماية الحقوق والحريات، الأمن الوطني، قواعد حماية البيانات الشخصية، جهة إشرافية لحماية البيانات، الالتزامات الملزمة التي تعهدت بها الدولة.

تاسعاً: يقوم المكتب بإعداد ومراجعة ونشر قائمة الاعتماد وتحديثها بشكل دوري وذلك بناءً على تقييم مستوى الحماية المناسب بحيث لا يقل عن مستوى الحماية الذي كفلته سياسة حماية البيانات الشخصية الصادرة من المكتب.

عاشراً: يقوم المكتب بإعداد ومراجعة البنود القياسية لحماية البيانات الشخصية.