مكتب إدارة البيانات
Data Management Office

القواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة العربية السعودية

الإصدار الثاني
فبراير ٢٠٢٥ م

التعريفات

سعيـًا لتطبيق هذه السياسات، تم تحديد معاني الكلمات والمصطلحات الرئيسة الواردة فيها، وتعني أينما وردت المعاني الموضحة أمامها، ما لم يقتض سياق النص خلاف ذلك، وهي:

1. **الجامعة:** جامعة الملك عبدالعزيز.
2. **المكتب:** مكتب إدارة البيانات بجامعة الملك عبدالعزيز.
3. **البيانات:** مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظمة مثل الأرقام أو الحروف أو الصور الثابتة أو التسجيلات المرئية أو التسجيلات الصوتية أو الرموز التعبيرية.
4. **إدارة البيانات:** عملية تطوير وتنفيذ الخطط والسياسات والبرامج والممارسات والإشراف عليها لتمكين حوكمة البيانات وتعزيز قيمتها باعتبارها أحد الأصول الإستراتيجية.
5. **الضوابط:** هي مجموعة من المبادئ والقواعد والتوجيهات التي تُمكن المنظمة من الوصول إلى أهدافها بعيدة المدى.
6. **الوصول إلى البيانات:** القدرة على الوصول المنطقي والمادي إلى البيانات لغرض استخدامها.
7. **البيانات الشخصية:** كل بيان - مهما كان مصدره أو شكله – من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلاً للتعرف عليه بصفةٍ 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 الفرد، وغير ذلك من البيانات ذات الطابع الشخصي.
8. **الامتثال:** تطبيق بنود هذه السياسة وضمان المراقبة الدورية لذلك.
9. **المصدر الموثوق:** مصدر مرجعي للبيانات تم إثبات موثوقيته من خلال التحقق المسبق من صحته.
10. **معالجة البيانات:** عملية تجري على البيانات بأحد الوسائل اليدوية أو الآلية، ومن ذلك عمليات الجمع والتسجيل والحفظ والفهرسة والترتيب والتنسيق والتخزين والتعديل والتحديث والدمج والاسترجاع والاستعمال والإفصاح والنقل والنشر والمشاركة والحجب والمسح والإتلاف.
11. **الضوابط الأمنية:** الأجهزة والإجراءات والسياسات والضمانات المادية المستخدمة لضمان سلامة البيانات وحمايتها ومعالجتها والوصول إليها.
12. **الإفصاح:** تمكين أي شخص - عدا جهة التحكم أو جهة المعالجة بحسب الأحوال - من الحصول على البيانات الشخصية أو استعمالها أو الاطلاع عليها بأي وسيلة ولأي غرض.

13. **الإجراءات:** يقصد بها تصميم خطوات العمل في الجهة وتوثيقها بحيث تتم بتسلسل واضح حسب الأنظمة واللوائح والمسؤوليات الموجودة في الهيكل التنظيمي لضمان الكفاءة المناسبة التي تخدم توجه الجهة في تحسين العمليات وتقديم الخدمات.

14. **السياسة:** وثيقة تنظيمية تقوم بتحديد السياق أو طريقة العمل لإرشاد وتحديد الخطوات الحالية والمستقبلية، كما تحدد المطلوب من الجهات داخل الجامعة أو خارجها من خلال المبادئ التي تضمنتها السياسات.

15. **التشفير:** تحويل البيانات من تنسيق قابل للقراءة إلى تنسيق مشفر. لا يمكن قـراءة البيانـات المشـفرة أو معالجتها إلا بعد فك تشفيرها.

الهدف

تهدف هذه الوثيقة إلى وضع القواعد بجامعة الملك عبدالعزيز من أجل حماية البيانات الشخصية عند نقلها خارج الحدود الجغرافية للمملكة العربية السعودية وفق أفضل الممارسات المحلية والدولية، كما تهدف – أيضًا - إلى الالتزام بالمتطلبات التشريعية الصادرة عن مكتب إدارة البيانات الوطنية وهي لائحة نقل البيانات الشخصية إلى خارج المملكة وجميع السياسات الأخرى ذات العلاقة.

النطاق

تنطبق أحكام هذه القواعد والسياسات على جميع البيانات الشخصية والمشمولة بنطاق تطبيق سياسة حماية البيانات الشخصية عند نقل البيانات الشخصية إلى جهات خارج الحدود الجغرافية للمملكة العربية السعودية بغرض معالجتها.

ملكية سياسات مشاكة البيانات

تعود ملكية هذه السياسة لمكتب إدارة البيانات في جامعة الملك عبدالعزيز، وإصدار النسخ المحدثة منها.

الامتثال لهذه القواعد العامة

يجب على جميع منسوبي الجامعة والمتعاقدين معها الالتزام بهذه السياسات، وعلى جهات الجامعة ضمان تطبيق هذه السياسات داخل إداراتها، علمًا بأن الالتزام ببنود هذه السياسة يخضع لمراجعة دورية من مكتب إدارة البيانات بالجامعة، وأي عدم التزام أو انتهاك لها سيؤدي إلى المساءلة القانونية واتخاذ الإجراءات اللازمة حسب ما يوصي به مكتب إدارة البيانات بالجامعة.

حقوق أصحاب البيانات

يُمنح صاحب البيانات ومن في حكمه جميع الحقوق المنصوص عليها في سياسة البيانات الشخصية الصادرة من مكتب إدارة البيانات بالجامعة، مع التأكيد على الحقوق التالية:

- **الحق في العلم:**

يشمل ذلك إشعاره بالأساس النظامي أو الاحتياج الفعلي لنقل بياناته الشخصية خارج الحدود الجغرافية للمملكة العربية السعودية ومكان تخزينها أو استضافتها، والجهات التي سيتم الإفصاح لها عن بياناته الشخصية عند نقلها، والغرض من هذا النقل، وأخذ موافقته على ذلك.

- **الحق في الرجوع عن موافقته:**

يحق لصاحب البيانات الرجوع عن موافقته على معالجة بياناته الشخصية خارج الحدود –في أي وقت– مالم يكن الغرض من نقل البيانات تحقيقـًا للمصلحة العامة، أو حمايةً للمصالح الحيوية للأفراد، أو تنفيذًا لمتطلبات نظامية.

- **الحق في الوصول إلى بياناته الشخصية:**

يحق لصاحب البيانات الوصول لبياناته الشخصية لدى الجامعة أو جهة المعالجة الخارجية، وذلك للاطلاع عليها، وطلب تصحيحها، أو إتمامها، أو تحديثها، وطلب إتلاف ما انتهت الحاجة إليه منها، والحصول على نسخة منها.

الأصل في معالجة البيانات أن تكون داخل الحدود الجغرافية للمملكة العربية السعودية ولا يجوز نقلها او معالجتها خارج المملكة إلا بعد التحقق من الحالات الموضحة أدناه حسب التسلسل التالي:

1. أن تكون جهة معالجة البيانات الشخصية خارج المملكة في دولة مشمولة بالقائمة المعتمدة لدى مكتب إدارة البيانات الوطنية.
2. إذا كانت الجهة الخارجية التي نُقلت إليها البيانات الشخصية غير مشمولة بقائمة الاعتماد، يتطلب منها مستوى كاف من الحماية لا يقل عن المستوى المعتمد في سياسة حماية البيانات الشخصية.
3. إذا لم يكن هناك مستوى كاف من الحماية، فتقوم الجامعة ممثلة في مكتب إدارة البيانات بوضع ضمانات مناسبة لحماية حقوق أصحاب البيانات، بما يتناسب مع متطلبات مكتب إدارة البيانات الوطنية وهيئة الأمن السيبراني.
4. إذا لم يتم توفير الضمانات الأمنية الكافية لحماية البيانات الشخصية فيمكن لجهة المعالجة الحصول على الاستثناء اللازم وفق التنظيمات ذات العلاقة الصادرة من مكتب إدارة البيانات الوطنية وهيئة الأمن السيبراني.

أولاً: تقييم مستوى الحماية

يقوم مكتب إدارة البيانات بالجامعة بإجراء تقييم الآثار والمخاطر المحتملة – كل حالة على حدة – لتحديد ما إذا كان سيتم توفير مستوى كاف من الحماية لحقوق أصحاب البيانات وعرض نتائج التقييم على مدير مكتب إدارة البيانات لتحديد مستوى قبول المخاطر وإقرارها. وللقيام بذلك يجب أن يقدم ما يثبت الالتزام بمعايير التقييم التالية:

أ- معايير التقييم العامة

1. نوع البيانات وقيمتها وحجمها المراد نقلها لتحديد مستوي الحماية المطلوبة.
2. الغرض من معالجة البيانات، وفئة أصحاب البيانات، ونطاق المعالجة، والجهات التي سيتم مشاركتها.
3. الفترة التي يتم خلالها معالجة البيانات.
4. مستوى الحماية في الدولة التي سيتم نقل البيانات لها.
5. مستوى الحماية في المراحل التي يتم بها نقل البيانات الشخصية – والتي قد تمر بأكثر من دولة أحيانا – وتقييم مستوى الحماية في الدولة التي تعد هي الوجهة النهائية.
6. الإجراءات الإدارية والتدابير التقنية والضوابط المادية المعتمدة في سياسات الجهة الخارجية لأمن المعلومات، كالتشفير والضوابط الأمنية والمعايير الدولية.
7. إذا لم يكن هناك مستوى كاف من الحماية، تقوم الجهة بوضع ضمانات مناسبة لحماية حقوق أصحاب البيانات، بما يتناسب مع متطلبات مكتب إدارة البيانات الوطنية وهيئة الأمن السيبراني.
8. إذا لم تتمكن الجهة من توفير الضمانات الأمنية الكافية لحماية البيانات الشخصية، يمكن الحصول على الاستثناء اللازم وفق التنظيمات ذات العلاقة الصادرة من مكتب إدارة البيانات الوطنية وهيئة الأمن السيبراني.

ب- معايير التقييم القانونية

1. وجود أنظمة وتشريعات في الدولة التي يُراد نقل البيانات إليها التي تحمي حقوق أصحاب البيانات.
2. وجود اتفاقيات دولية أو تبني مبادئ ومعايير دولية لحماية البيانات الشخصية في الدولة التي يُراد نقل البيانات إليها.
3. اعتماد قواعد سلوكية أو ممارسات عامة خاصة لحماية البيانات الشخصية في الدولة التي يُراد نقل البيانات إليها.

ثانيًا: الضمانات المناسبة

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

1. تضمين بنود نموذجية أو قياسية – في العقود والاتفاقيات يتم الموافقة عليها من قبل مكتب إدارة البيانات بالجامعة وذلك لضمان المحافظة على خصوصية البيانات وأصحابها وحماية حقوقهم.
2. إعداد قواعد مشتركة ملزمة قانونيًا تنطبق على عمليات نقل البيانات الشخصية خارج الحدود بما في ذلك معالجة انتهاكات الخصوصية والإشعار عنها - على أن تتم الموافقة عليها من قبل مكتب إدارة البيانات بالجامعة - يتم تضمين هذه القواعد المشتركة كملحقًا لاتفاقيات مستوى الخدمة أو العقود المبرمة بين الجهتين مع أخذ موافقة الأطراف عند وجود أي التزام قانوني تخضع له أي من هذه الأطراف.
3. استخدام قواعد السلوك المعتمدة من قبل مكتب إدارة البيانات الوطنية وهيئة الأمن السيبراني بصفتها أداة فعالة تحدد الالتزامات وذلك لضمان المحافظة على خصوصية أصحاب البيانات وحماية حقوقهم.
4. الاستعانة بأطراف خارجية مستقلة تتولى إصدار شهادات اعتماد تؤكد وجود الضمانات المناسبة للمحافظة على خصوصية أصحاب البيانات وحماية حقوقهم.
5. توقيع اتفاقية ملزمة قانونيا لنقل البيانات الشخصية على أن تتضمن هذه الاتفاقية على بنودًا تعاقدية ملزمة تضمن المحافظة على خصوصية أصحاب البيانات وتحمي حقوقهم.

ثالثًا: الاستثناءات لحالات محددة

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

1. استنادًا على موافقة أصحاب البيانات.
2. تنفيذًا لالتزام تعاقدي للجامعة.
3. تنفيذًا لمتطلبات قضائية.
4. تنفيذًا لأحكام اتفاقية دولية تكون المملكة طرفـًا فيها.
5. المحافظة على المصلحة العامة بما في ذلك حماية الصحة أو السلامة العامة.
6. حماية المصالح الحيوية لأصحاب البيانات.

أحكام عامة

1. يتم أخذ موافقة كتابية من مدير مكتب إدارة البيانات بالجامعة لاعتماد عملية نقل البيانات الشخصية خارج الحدود الجغرافية للمملكة.
2. يحق لمكتب إدارة البيانات بالجامعة وضع قواعد إضافية لنقل أنواع محددة من البيانات الشخصية وفقـًا لطبيعة وحساسية هذه البيانات.
3. يتم مراجعة معايير التقييم – العامة والقانونية – المتعلقة بحماية البيانات الشخصية عند نقلها خارج الحدود الجغرافية للمملكة العربية السعودية واتخاذ الاجراءات المنظمة لها.
4. يتم وضع قائمة محددة للعوامل الرئيسية التي تحدد مستوى الحماية المناسب، ومنها على سبيل المثال، الأنظمة والتشريعات، حماية الحقوق والحريات، الأمن الوطني، قواعد حماية البيانات الشخصية.
5. التحقق بشكل دوري من امتثال جهات المعالجة لهذه القواعد.

الوثائق المرتبطة

1. سياسة حماية البيانات الشخصية
2. إشعار حماية البيانات الشخصية
3. سياسة حماية البيانات الشخصية للأطفال ومن في حكمهم

مكتب إدارة البيانات

Data Management Office

DMO@kau.edu.sa