



مكتب إدارة البيانات
Data Management Office

سياسة حماية البيانات الشخصية

الإصدار الثاني
فبراير ٢٠٢٥ م

سعيًا 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 تمكن المنظمة من الوصول إلى أهدافها بعيدة المدى.
6. **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 دمجها 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.
7. **صاحب البيانات الشخصية:** الشخص الطبيعي الذي تتعلق به البيانات الشخصية أو من يمثله أو من له الولاية الشرعية عليه.
8. **الامتثال:** تطبيق بنود هذه السياسة وضمن المراقبة الدورية لذلك.
9. **صاحب البيانات الشخصية:** 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. **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.
12. **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.
13. **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.
14. **التشفير:** تحويل البيانات من تنسيق قابل

تهدف هذه السياسة إلى وضع سياسات حماية البيانات الشخصية بجامعة الملك عبدالعزيز وفق أفضل الممارسات المحلية والدولية، كما تهدف - أيضاً - إلى الالتزام بالمتطلبات التشريعية الصادرة عن مكتب إدارة البيانات الوطنية وهي ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها ونظام حماية البيانات الشخصية وجميع السياسات الأخرى ذات العلاقة.

تنطبق أحكام هذه السياسة على جميع البيانات الشخصية التي تتلقاها أو تنتجها أو تتعامل معها جامعة الملك عبدالعزيز- سواءً أكانت أنتجت أم استخدمت قبل اعتماد هذه السياسة أو بعدها - مهما كان مصدرها، أو شكلها أو طبيعتها، ويشمل ذلك جميع أشكال البيانات الشخصية المتعلقة بالأفراد.

يُستثنى من نطاق تطبيق هذه السياسة في الأحوال التالية:

- إذا كان جمع البيانات الشخصية أو معالجتها مطلوباً لتحقيق متطلبات نظامية وفقاً للأنظمة واللوائح والسياسات المعمول بها في المملكة العربية السعودية أو لاستيفاء متطلبات قضائية أو لتنفيذ التزام بموجب اتفاق تكون المملكة طرفاً فيه.
- إذا كان جمع البيانات الشخصية أو معالجتها ضرورياً لحماية الصحة أو السلامة العامة أو حماية المصالح الحيوية للأفراد.

تعود ملكية سياسات حماية البيانات الشخصية إلى مكتب إدارة البيانات في جامعة الملك عبدالعزيز، وإصدار النسخ المحدث منها.

يجب على جميع منسوبي الجامعة والمتعاقدين معها الالتزام بهذه السياسات، وعلى جهات الجامعة ضمان تطبيق هذه السياسات داخل إداراتها، علماً بأن الالتزام بينود هذه السياسات 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.

من أجل حماية البيانات الشخصية تلتزم الجامعة بالمبادئ الرئيسية التالية:

المبدأ الأول: المسؤولية

ضمان توفير السياسات والإجراءات لحماية البيانات الشخصية يعتبر جزءًا أساسيًا من مسؤولية مكتب إدارة البيانات، وهذا يشمل تطبيق المعايير والإجراءات بفعالية وتعزيز ثقافة الوعي بأهمية حماية البيانات الشخصية، بالإضافة إلى التأكد من توافق الإجراءات مع اللوائح المتعلقة بحماية البيانات الشخصية.

المبدأ الثاني: الشفافية

تتمثل الشفافية في حماية البيانات الشخصية في الوضوح والصراحة في جميع جوانب جمع، معالجة، ومشاركة هذه البيانات. هذا يعني توفير معلومات واضحة ومفهومة لأصحاب البيانات حول كيفية جمع البيانات الخاصة بهم وأسباب جمعها وطرق استخدامها ومعالجتها.

المبدأ الثالث: الاختيار والموافقة

ضمان أن الأفراد لديهم القدرة على اتخاذ القرار بشأن جمع واستخدام بياناتهم الشخصية وذلك بتوفير جميع المعلومات اللازمة بشكل واضح لفهم كيف ستستخدم بياناتهم، والسماح لهم بالموافقة على ذلك أو رفضه.

المبدأ الرابع: الحد من جمع البيانات

اقتصار جمع البيانات الشخصية على الحد الأدنى من البيانات الذي يمكن من تحقيق الأغراض المحددة في إشعار الخصوصية.

المبدأ الخامس: الحد من استخدام البيانات والاحتفاظ بها والتخلص منها

تقييد معالجة البيانات الشخصية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدم صاحب البيانات موافقته الضمنية أو الصريحة، والاحتفاظ بها طالما كان ذلك ضروريًا لتحقيق الأغراض المحددة أو لما تقتضيه الأنظمة واللوائح والسياسات المعمول بها في المملكة وإتلافها بطريقة آمنة تمنع التسرب، أو فقدان، أو الاختلاس، أو إساءة الاستخدام، أو الوصول الغير مصرح به نظامًا.

المبدأ السادس: الوصول إلى البيانات الشخصية

توفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية لمراجعتها، أو تحديثها، أو تصحيحها.

المبدأ السابع: الحد من الإفصاح عن البيانات

تقييد الإفصاح عن البيانات الشخصية للأطراف الخارجية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدم صاحب البيانات موافقته الضمنية أو الصريحة.

المبدأ الثامن: أمن البيانات الشخصية

حماية البيانات من التسرب أو التلف أو فقدان أو إساءة الاستخدام أو التعديل أو الوصول غير المصرح به - وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.

المبدأ التاسع: جودة البيانات الشخصية

الاحتفاظ بالبيانات الشخصية بصورة دقيقة وكاملة وذات علاقة مباشرة بالأغراض المحددة في إشعار الخصوصية.

المبدأ العاشر: المراقبة والامتثال

مراقبة الامتثال لسياسات وإجراءات الخصوصية بالجامعة، ومعالجة الاستفسارات والشكاوى والنزاعات المتعلقة بالخصوصية.

الأدوار والمسؤوليات

1. تلتزم الجامعة باعتماد السياسات والإجراءات المتعلقة بحماية البيانات الشخصية، ويكون مدير مكتب إدارة البيانات بالجامعة - أو من يفوضه - مسؤولاً عن الموافقة عليها.
2. يكون مكتب إدارة البيانات بالجامعة مسؤول عن مراقبة تنفيذ السياسات والإجراءات المعتمدة بالجامعة، وتتضمن مهام ومسؤوليات المكتب وضع المعايير المناسبة لتحديد مستويات حساسية البيانات الشخصية.
3. يقوم مكتب إدارة البيانات بتقييم المخاطر والآثار المحتملة لأنشطة معالجة البيانات الشخصية وعرض نتائج التقييم على مدير مكتب إدارة البيانات بالجامعة - أو من يفوضه - لتحديد مستوى قبول المخاطر وإقرارها.
4. تلتزم كافة جهات الجامعة بتطبيق السياسات والإجراءات المتعلقة بحماية البيانات الشخصية المعتمدة وذلك يشمل تحديث العقود واتفاقيات مستوى الخدمة والتشغيل بما يتوافق مع سياسات وإجراءات الخصوصية.
5. تلتزم الأطراف الخارجية التي يسند إليها خدمات معالجة البيانات من الامتثال لهذه السياسة.
6. يحق لمكتب إدارة البيانات بالجامعة وضع قواعد إضافية لمعالجة أنواع محددة من البيانات الشخصية وفقاً لطبيعة وحساسية هذه البيانات.

ضوابط جمع ومعالجة البيانات الشخصية

1. أن يكون الغرض من جمع البيانات الشخصية متوافقاً مع الأنظمة واللوائح والسياسات المعمول بها في المملكة العربية السعودية وذات علاقة مباشرة بنشاط الجامعة.
2. أن يكون محتوى البيانات مقتصرًا على الحد الأدنى من البيانات اللازمة لتحقيق الغرض من جمعها.
3. أن يتم تقييد جمع البيانات على المحتوى المعد سلفاً (الموضح في الضابط السابق - رقم 2) ويكون بطريقة عادلة (مباشرة وواضحة وأمنة وخالية من أساليب الخداع أو التضليل).
4. أن يقتصر استخدام البيانات على الغرض الذي جمعت من أجله.

1. إشعار صاحب البيانات - بطريقة ملائمة وقت جمع البيانات - بالغرض والأساس النظامي والاحتياج الفعلي والوسائل والطرق المستخدمة لجمع ومعالجة ومشاركة البيانات الشخصية وكذلك التدابير الأمنية لضمان حماية الخصوصية حسب الأنظمة واللوائح والسياسات المعمول بها في المملكة العربية السعودية.
2. إشعار صاحب البيانات عن المصادر الأخرى التي يتم استخدامها في حال تم جمع بيانات إضافية بطريقة غير مباشرة (من جهات أخرى).
3. تزويد صاحب البيانات بالخيارات المتاحة فيما يتعلق بمعالجة البيانات الشخصية والآلية المستخدمة لممارسة هذه الخيارات، ومنها على سبيل المثال (Preferences, Opt-in and Opt-out).
4. تحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية وذلك لمراجعتها وتحديثها.
5. التحقق من هوية الأفراد قبل منحهم الوصول إلى بياناتهم الشخصية وفقاً للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.
6. أخذ موافقة صاحب البيانات على معالجة البيانات الشخصية بعد تحديد نوع الموافقة (صرحية أو ضمنية) بناءً على طبيعة البيانات وطرق جمعها.
7. إعداد وتوثيق وتطبيق الإجراءات اللازمة لضمان دقة البيانات واكتمالها وحدثتها وارتباطها بالغرض الذي جمعت من أجله.

مشاركة البيانات الشخصية

1. يحظر مشاركة البيانات الشخصية مع جهات أخرى إلا وفقاً للأغراض المحددة بعد موافقة صاحب البيانات ووفقاً للأنظمة واللوائح والسياسات على أن تزود الجهات الأخرى بسياسات وإجراءات الخصوصية المتبعة وتضمنها في العقود والاتفاقيات.
2. تؤخذ موافقة أصحاب البيانات في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الأغراض المحددة، ولهم حق الرفض.
3. أخذ موافقة مدير مكتب إدارة البيانات في حال مشاركة البيانات الشخصية مع جهات أخرى خارج المملكة العربية السعودية.

1. يتم تخزين البيانات الشخصية، ومعالجتها داخل الحدود الجغرافية للمملكة، لضمان المحافظة على السيادة الوطنية الرقمية لهذه البيانات، ولا يجوز معالجتها خارج المملكة إلا بعد الحصول على موافقة كتابية من مدير مكتب إدارة البيانات بجامعة الملك عبدالعزيز.
2. عند التخلص من البيانات الشخصية، يتم إتلاف البيانات بطريقة آمنة تمنع فقدانها أو إساءة استخدامها أو الوصول غير المصرح به إليها - وتشمل البيانات التشغيلية، المؤرشفة، والنسخ الاحتياطية - وذلك وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني.
3. تضمن هذه الضوابط في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.

معالجة انتهاكات الخصوصية

- تلتزم جميع جهات الجامعة بإشعار صاحب البيانات الشخصية فوراً ودون تأخير وبما لا يتجاوز 72 ساعة من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشخصية وفقاً للآليات والإجراءات التي حددها المكتب.
- تلتزم جميع جهات الجامعة إبلاغ مكتب إدارة البيانات بالجامعة فوراً ودون تأخير وبما لا يتجاوز 72 ساعة من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشخصية وفقاً للآليات والإجراءات التي حددها المكتب.
- تلتزم جميع جهات الجامعة بالتعاون في الاستجابة والتحقيق في حوادث انتهاك خصوصية البيانات، والرفع بذلك لمكتب إدارة البيانات بالجامعة لاستكمال الاجراءات النظامية.

التدابير الأمنية لحماية البيانات الشخصية

1. منح صلاحيات الوصول إلى البيانات وفقاً لمهام العاملين ومسؤولياتهم بناء على مبدأ "الحد الأدنى من الامتيازات" و"الحاجة إلى المعرفة" والمذكورة في سياسة تصنيف البيانات.
2. تطبيق الإجراءات الإدارية والتدابير التقنية التي توثق مراحل معالجة البيانات وتوفير إمكانية تحديد المستخدم المسؤول عن كل مرحلة من هذه المراحل (سجلات الاستخدام).
3. استخدام التدابير الأمنية المناسبة - كالتشفير- لأمن البيانات الشخصية وحمايتها بما يتناسب مع طبيعتها وحساسيتها والوسائط المستخدمة لنقلها وتخزينها وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.
4. مراقبة الامتثال لسياسات وإجراءات الخصوصية بشكل دوري ويتم عرضها على مدير مكتب إدارة البيانات - أو من يفوضه - كما يتم تحديد وتوثيق الإجراءات التصحيحية التي سيتم اتخاذها في حال عدم الامتثال وإشعار المكتب بذلك.

1. الحق في العلم ويشمل ذلك إشعاره بالأساس النظامي أو الاحتياج الفعلي لجمع بياناته الشخصية، والغرض من ذلك، وألا تعالج بياناته لاحقاً بصورة تتنافى مع الغرض من جمعها والذي من أجله قدم موافقته الضمنية أو الصريحة.
2. الحق في الرجوع عن موافقته على معالجة بياناته الشخصية - في أي وقت - ما لم تكن هناك أغراض مشروعة تتطلب عكس ذلك.
3. الحق في الوصول إلى بياناته الشخصية، وذلك للاطلاع عليها وطلب تصحيحها أو إتمامها أو تحديثها وطلب إتلاف ما انتهت الحاجة إليه منها والحصول على نسخة منها بصيغة واضحة.

الوثائق المرتبطة بسياسة حماية البيانات الشخصية

ترتبط هذه السياسة بالوثائق التالية:

1. إشعار حماية البيانات الشخصية



مكتب إدارة البيانات

Data Management Office

DMO@kau.edu.sa