المملكة العربية السعودية
وزارة التعليم
الجامعة الإسلامية بالمدينة المنورة
مكتب إدارة البيانات

Kingdom of Saudi Arabia
Ministry of Education
Islamic University of Madinah
Data Management Office

سياسة حماية البيانات الشخصية

نسخة 1.0

التاريخ: 2025/4/12
نوع الوثيقة: سياسة
تصنيف الوثيقة: عام
رقم الإصدار: 1.0

جدول المحتويات

المادة الأولى: الغرض والنطاق

تهدف هذه السياسة إلى الحرص على أن تكون الجامعة ملتزمة بالتشريعات والضوابط المتعلقة بحماية البيانات الشخصية الصادرة من الجهات المختصة، وعلى أن يكون التعامل مع البيانات الشخصية داخل الجامعة منضبطا مع تلك التشريعات والضوابط بما يضمن حماية خصوصية الأفراد أصحاب البيانات وتوفير حقوقهم المكفولة لهم. كما تهدف هذه السياسة إلى تنظيم عملية جمع البيانات الشخصية ومعالجتها ومشاركتها والحفاظ عليها.

وتنطبق أحكام هذه السياسة على جميع منسوبي الجامعة، الذين يقومون كليا أو جزئيا بمعالجة البيانات الشخصية. ويلتزم جميع منسوبي الجامعة بهذه السياسة بمن فيهم الأطراف الخارجية التي تتعامل مع البيانات التي تملكها الجامعة، وأي مخالفة لهذه السياسة يترتب عليها تطبيق الأنظمة واللوائح المتعلقة بذلك.

يستثنى من نطاق تطبيق هذه السياسة جمع البيانات الشخصية من غير صاحبها مباشرة دون علمه، أو معالجتها لغير الغرض الذي جمعت من أجله، أو الإفصاح عنها دون موافقته، أو نقلها خارج المملكة في الحالات التالية:

- إذا كان المكتب جهة حكومية وكان جمع البيانات الشخصية أو معالجتها مطلوبًا بموجب الأنظمة واللوائح والسياسات المعمول بها في المملكة، أو للوفاء بمتطلبات قضائية أو لتنفيذ التزام بموجب اتفاقية تكون المملكة طرفًا فيها.

- إذا كان جمع البيانات الشخصية أو معالجتها ضروريًا لحماية الصحة العامة أو السلامة العامة، أو لحماية المصالح الحيوية للأفراد.

المادة الثانية: التعريف بالمصطلحات العامة

- **سياسة حماية البيانات الشخصية:** تنظيم عملية جمع البيانات الشخصية ومعالجتها ومشاركتها والحفاظ على السيادة الوطنية الرقمية عليها.

- **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 الحسابات البنكية والبطاقات الائتمانية، أو صور المستخدم الثابتة أو المتحركة، والأرقام الوظيفية والأرقام الجامعية، وغير ذلك من البيانات ذات الطابع الشخصي.

- **صاحب البيانات الشخصية:** الشخص الطبيعي الذي تتعلق به البيانات الشخصية أو من يمثله أو من له الولاية الشرعية عليه.

- **معالجة البيانات الشخصية:** جميع العمليات التي تجرى على البيانات الشخصية بأي وسيلة كانت يدوية أو آلية، وتشمل هذه العمليات-على سبيل المثال-جمع البيانات ونقلها وحفظها وتخزينها ومشاركتها وإتلافها وتحليلها واستخراج أنماطها والاستنتاج منها وربطها مع بيانات أخرى.

- **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 عن طريق 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 ونيابة عنها.

- **الموافقة الصريحة:** موافقة مكتوبة أو إلكترونية تكون صريحة ومحددة وصادرة بإرادة حرة ومطلقة من صاحب البيانات تدل على قبوله لمعالجة بياناته الشخصية.

- **الموافقة الضمنية:** موافقة لا يتم منحها صراحة من قبل صاحب البيانات، ولكنها تُمنح ضمنياً عن طريق أفعال الشخص ووقائع وظروف الموقف، كتوقيع العقود أو الموافقة على الشروط والأحكام.

- **الإفصاح عن البيانات الشخصية:** تمكين أي شخص-عدا جهة التحكم (الجامعة)-من الحصول على البيانات الشخصية أو استعمالها أو الاطلاع عليها بأي وسيلة ولأي غرض.

- **تسريب البيانات الشخصية**: الإفصاح عن البيانات الشخصية، أو الحصول عليها، أو تمكين الوصول إليها دون تصريح أو سند نظامي، سواء بقصد أو بغير قصد.

- **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.

- **إشعار الخصوصية:** إشعار خارجي موجه للأفراد يوضح محتوى البيانات الشخصية، ووسائل جمعها، والغرض من معالجتها، وكيفية استخدامها، والجهات التي سيتم مشاركة هذه البيانات معها وفترة الاحتفاظ بها وآلية التخلص منها.

المادة الثالثة: المبادئ الرئيسية لحماية البيانات الشخصية

عند التعامل مع البيانات الشخصية يجب مراعاة المبادئ التالية والتي حددتها السياسات المعتمدة من الجهات التنظيمية وعلى مكتب إدارة البيانات التأكد من الالتزام بهذه المبادئ:

1. **المسؤولية:** يقوم مكتب إدارة البيانات بتحديد وتوثيق سياسات وإجراءات الخصوصية الخاصة بالجامعة واعتمادها من قبل رئيس الجامعة أو من يفوضه، ونشرها إلى جميع من تنطبق عليه.

2. **الشفافية:** يقوم مكتب إدارة البيانات بالتنسيق مع الجهات المختصة بإعداد إشعار عن سياسات وإجراءات الخصوصية الخاصة بالجامعة، يحدد فيه الأغراض التي من أجلها تمت معالجة البيانات الشخصية وذلك بصورة محددة وواضحة وصريحة.

3. **الاختيار والموافقة:** يتم تحديد جميع الخيارات المتاحة لصاحب البيانات الشخصية والحصول على موافقته الضمنية أو الصريحة فيما يتعلق بجمع بيانات واستخدامها أو الإفصاح عنها.

4. **الحد من جمع البيانات:** يقتصر جمع البيانات الشخصية على الحد الأدنى من البيانات الذي يمكّن من تحقيق الأغراض المحددة في إشعار الخصوصية.

5. **الحد من استخدام البيانات والاحتفاظ بها والتخلص منها:** تقتصر معالجة البيانات الشخصية على الأغراض المحددة في إشعار الخصوصية والتي من أجلها قدم صاحب البيانات موافقته الضمنية أو الصريحة، ويتم تقييد الاحتفاظ بها طالما كان ذلك ضروريا لتحقيق الأغراض المحددة أولما تقتضيه الأنظمة واللوائح والسياسات المعمول بها في المملكة وإتلافها بطريقة آمنة تمنع التسرب، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو الوصول غير المصرح.

6. **الوصول إلى البيانات:** يتم تحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية لمراجعتها، وتحديثها، وتصحيحها.

7. **الحد من الإفصاح عن البيانات:** يتم تقييد الإفصاح عن البيانات الشخصية للأطراف الخارجية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدم صاحب البيانات موافقته الصريحة أو الضمنية.
8. **أمن البيانات:** تتم حماية البيانات الشخصية من التسرب، أو التلف، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو التعديل، أو الوصول غير المصرح به-وفقا لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.

9. **جودة البيانات:** يتم الاحتفاظ بالبيانات الشخصية بصورة دقيقة، وكاملة، وذات علاقة مباشرة بالأغراض المحددة في إشعار الخصوصية.

10. **المراقبة والامتثال:** يقوم مكتب إدارة البيانات بمراقبة الامتثال لسياسات وإجراءات الخصوصية الخاصة بالجامعة، ومعالجة الاستفسارات والشكاوى والنزاعات المتعلقة بالخصوصية.

المادة الرابعة: حقوق صاحب البيانات

يتمتع صاحب البيانات بحقوق تتعلق ببياناته الشخصية والطريقة التي تتعامل بها الجامعة مع هذه البيانات، ويجب الحرص على الالتزام بتوفير هذه الحقوق لصاحب البيانات:

1. الحق في العلم ويشمل ذلك إشعار صاحب البيانات بالأساس النظامي أو الاحتياج الفعلي لجمع بياناته الشخصية، والغرض من ذلك، وألّا تعالج بياناته لاحقا بصورة تتنافى مع الغرض الذي جمعت من أجله والذي وافق عليه مسبقا سواء كانت الموافقة صريحة أو ضمنية.

2. لصاحب البيانات الحق في الرجوع عن موافقته على معالجة بياناته الشخصية -في أي وقت-مالم تكن هناك أغراض مشروعة تتطلب عكس ذلك.

3. الحق في الوصول إلى بياناته الشخصية. لصاحب البيانات الحق في الوصول إلى بياناته الشخصية لدى الجامعة، وذلك للاطلاع عليها، وطلب تصحيحها، أو إتمامها، أو تحديثها، والحصول على نسخة منها بصيغة واضحة.

4. يحق لصاحب البيانات الشخصية، دون الإخلال بأحكام النظام، التقدم بطلب لإتلاف بياناته الشخصية المحتفظ بها لدى الجامعة الإسلامية وذلك مع الالتزام بالمتطلبات النظامية ذات الصلة.

المادة الخامسة: التزامات الجامعة الإسلامية

1. ان يكون مكتب إدارة البيانات مسؤولاً عن إعداد وتطبيق السياسات والإجراءات الخاصة بحماية البيانات الشخصية، ويكون المسؤول الأول في الجامعة أو من يُفوَّض من قبله مسؤولية اعتمادها والموافقة عليها.
2. ان تقوم الجامعة بإنشاء مكتب إدارة البيانات، تكون مرتبطة بمكتب إدارة البيانات الوطنية بموجب الأمر السامي الكريم رقم 59766 بتاريخ 1439/11/20هـ، وتُناط به مهام تطوير السياسات والإجراءات وتوثيقها ومراقبة تنفيذها، وفقاً لاعتماد الإدارة العليا، إلى جانب وضع معايير ملائمة لتحديد مستويات حساسية البيانات الشخصية.

3. ان يقوم مكتب إدارة البيانات بتقييم المخاطر والآثار المحتملة لأنشطة معالجة البيانات الشخصية، ورفع نتائج هذا التقييم إلى المسؤول الأول في الجامعة أو من يُفوَّضه لاتخاذ قرار بشأن مستوى المخاطر المقبول واعتماده.
4. ان يقوم مكتب إدارة البيانات بمراجعة وتحديث العقود واتفاقيات مستوى الخدمة والتشغيل، لضمان توافقها مع السياسات والإجراءات المعتمدة للخصوصية من قبل الإدارة العليا.
5. يقوم مكتب إدارة البيانات بإعداد وتوثيق إجراءات التعامل مع انتهاكات الخصوصية، بما يشمل تحديد المسؤوليات ومهام فريق العمل المختص، والحالات التي تستوجب إشعار الجهة التنظيمية والمكتب المختص بناءً على تسلسل إداري واضح ووفقاً لقياس شدة الأثر.
6. ان يقوم مكتب إدارة البيانات بإعداد وتنفيذ برامج توعوية تهدف إلى تعزيز ثقافة الخصوصية ورفع مستوى الوعي، بما يتماشى مع السياسات والإجراءات المعتمدة من الإدارة العليا للجامعة.
7. ان يتم إشعار صاحب البيانات بطريقة مناسبة في وقت جمعها، موضحاً الغرض من الجمع، والأساس النظامي أو الحاجة الفعلية لذلك، والوسائل والأساليب المتبعة في جمع البيانات الشخصية ومعالجتها ومشاركتها، إضافة إلى التدابير الأمنية المطبقة لحماية الخصوصية، وذلك بما يتوافق مع الأنظمة واللوائح والسياسات المعمول بها في المملكة.
8. في حال تم جمع بيانات إضافية بطريقة غير مباشرة من مصادر خارجية، يجب إبلاغ صاحب البيانات بهذه المصادر.
9. يجب تزويد صاحب البيانات بالخيارات المتاحة له بشأن معالجة بياناته الشخصية، وتوضيح الآلية المتبعة لممارسة هذه الخيارات، مثل تفضيلات القبول أو الرفض (opt-in)و (opt-out)
10. يلزم الحصول على موافقة صاحب البيانات قبل البدء في معالجة بياناته الشخصية، مع تحديد نوع الموافقة ما إذا كانت صريحة أو ضمنية، وذلك بناءً على طبيعة البيانات وطريقة جمعها.
11. يجب أن يكون الغرض من جمع البيانات متوافقاً مع الأنظمة واللوائح والسياسات المعتمدة في المملكة، وله ارتباط مباشر بنشاط الجامعة.
12. يُشترط أن تقتصر البيانات المجمعة على الحد الأدنى اللازم لتحقيق الغرض المحدد من جمعها.
13. ينبغي أن يقتصر جمع البيانات على المحتوى المُحدد مسبقاً، وأن يتم بأسلوب عادل ومباشر وواضح وآمن، وبعيد عن أي وسائل خادعة أو مضللة.
14. يلتزم مكتب إدارة البيانات باستخدام البيانات فقط للأغراض التي جُمعت من أجلها دون تجاوز ذلك.
15. يقوم مكتب إدارة البيانات بإعداد وتوثيق سياسة وإجراءات خاصة بالاحتفاظ بالبيانات، بما يتماشى مع الأغراض المحددة، والأنظمة والتشريعات ذات العلاقة.
16. يلتزم مكتب إدارة البيانات بمعالجة البيانات الشخصية وتخزينها داخل حدود المملكة، بهدف الحفاظ على السيادة الرقمية الوطنية. ولا يُسمح بنقل أو معالجة البيانات خارج المملكة إلا بعد الحصول على موافقة خطية من الجهة التنظيمية، وذلك بالتنسيق المسبق مع المكتب المختص.
17. يقوم مكتب إدارة البيانات بإعداد وتوثيق سياسة وإجراءات التخلص الآمن من البيانات، بما يضمن منع فقدانها أو إساءة استخدامها أو الوصول غير المصرح به إليها، ويشمل ذلك البيانات التشغيلية، المؤرشفة، والنسخ الاحتياطية، وفقًا لما تصدره الهيئة الوطنية للأمن السيبراني.

18. يقوم مكتب إدارة البيانات بتضمين أحكام سياسات الاحتفاظ والتخلص من البيانات في العقود المبرمة، في حال إسناد هذه المهام إلى جهات معالجة خارجية.
19. يقوم مكتب إدارة البيانات بتحديد وتوفير الوسائل التي تتيح لصاحب البيانات الوصول إلى بياناته الشخصية، بهدف مراجعتها وتحديثها.
20. يقوم مكتب إدارة البيانات بالتحقق من هوية الأفراد قبل منحهم صلاحية الوصول إلى بياناتهم الشخصية، وذلك بما يتوافق مع الضوابط المعتمدة من الهيئة الوطنية للأمن السيبراني والجهات المختصة.
21. يُحظر مشاركة البيانات الشخصية مع جهات أخرى إلا لأغراض محددة، وبعد الحصول على موافقة صريحة من صاحب البيانات، مع ضرورة التقيّد بالأنظمة واللوائح والسياسات المعتمدة، وضمان تزويد الجهات المستلمة للبيانات بسياسات وإجراءات الخصوصية المعتمدة وتضمينها ضمن العقود والاتفاقيات.
22. ان يتم إشعار أصحاب البيانات والحصول على موافقتهم عند مشاركة بياناتهم مع جهات أخرى، في حال استخدامها لأغراض غير تلك التي جُمعت من أجلها.
23. ان يقوم مكتب إدارة البيانات بأخذ موافقة مكتب إدارة البيانات الوطنية - بعد التنسيق مع الجهة التنظيمية - قبل مشاركة البيانات الشخصية مع جهات أخرى خارج المملكة.
24. يلتزم مكتب إدارة البيانات بإعداد وتوثيق وتطبيق إجراءات فعالة لضمان دقة واكتمال وحداثة البيانات الشخصية، ومدى ارتباطها بالغرض الذي جُمعت من أجله.
25. يجب استخدام الضوابط الإدارية والتدابير التقنية المعتمدة ضمن سياسات أمن المعلومات في الجامعة، لضمان حماية البيانات الشخصية، ويشمل ذلك – على سبيل المثال لا الحصر – ما يلي:

- منح صلاحيات الوصول إلى البيانات بما يتناسب مع مهام ومسؤوليات الموظفين، بطريقة تضمن عدم تداخل الاختصاصات وتجنب تشتت المسؤوليات.

- تطبيق الإجراءات الإدارية والتقنية التي توثق مراحل معالجة البيانات، وتوفر إمكانية تتبع المستخدم المسؤول عن كل مرحلة من تلك المراحل (سجلات الاستخدام).

- توقيع الموظفين القائمين على معالجة البيانات على تعهدات بالمحافظة على سرية البيانات وعدم إفشائها، إلا وفقًا للسياسات والإجراءات والأنظمة والتشريعات المعتمدة.

- اختيار الموظفين المعنيين بمعالجة البيانات من ذوي الأمانة والمسؤولية، مع مراعاة طبيعة البيانات وحساسيتها، وسياسة الوصول المعتمدة لدى الجامعة.

- استخدام التدابير الأمنية المناسبة مثل التشفير، وعزل بيئة التطوير والاختبار عن بيئة التشغيل، بما يضمن حماية البيانات الشخصية وفقًا لطبيعتها، حساسيتها، ووسائط نقلها وتخزينها، ووفقًا لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات العلاقة.

26. يتحمل مكتب إدارة البيانات مسؤولية مراقبة الامتثال لسياسات وإجراءات الخصوصية بشكل دوري، ويتم عرض نتائج المراجعة على المسؤول الأول في الجامعة أو من يفوضه. كما يتعيّن تحديد وتوثيق الإجراءات التصحيحية التي ستُتخذ في حال وجود حالات عدم امتثال، مع إشعار الجهة التنظيمية والمكتب وفق التسلسل التنظيمي المعتمد.

المادة السادسة: احكام عامة

1. يتولى مكتب إدارة البيانات مواءمة أحكام هذه السياسة مع الوثائق التنظيمية الخاصة بها وتعميمها على جميع الجهات التابعة لها أو المرتبطة بها بما يحقق التكامل ويضمن تحقيق الهدف المنشود من إعداد هذه السياسة.
2. يقوم مكتب إدارة البيانات بمراقبة الامتثال لهذه السياسة بشكل دوري
3. يلتزم مكتب إدارة البيانات بالامتثال لهذه السياسة وتوثيق الامتثال وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية.
4. يجب على مكتب إدارة البيانات إبلاغ الجهات التنظيمية فوراً ودون تأخير، بما لا يتجاوز 72 ساعة، من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشخصية، وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية.
5. ان يقوم المكتب عند تعاقده مع جهات المعالجة أن يتحقق بشكل دوري من امتثال جهات المعالجة لهذه السياسة وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية، ويشمل ذلك أي تعاقدات لاحقة تقوم بها الجامعة.
6. يحق للجهات التنظيمية وضع قواعد إضافية لمعالجة أنواع محددة من البيانات الشخصية وفقاً لطبيعة وحساسية هذه البيانات بعد التنسيق مع مكتب إدارة البيانات الوطنية.