جامعـــة الأمـيـــر سطام بن عبدالعزيز
PRINCE SATTAM BIN ABDULAZIZ UNIVERSITY

سياسة حماية البيانات الشخصية

تصنيف الوثيقة : عام

الإصدار : 1.4

يناير 2025

المحتويات

التعريفات 3
الأهداف 5
أولاً| النطاق 5
ثانياً | المبادئ الرئيسية لحماية البيانات الشخصية 6
ثالثاً | حقوق صاحب البيانات 6
رابعاً | التزامات مكتب البيانات والذكاء الاصطناعي 7
خامساً | أحكام عامة 10
سادساً | الأدوار والمسؤوليات 11
سابعاً | الالتزام بالسياسة 11

التعريفات

المصطلح	التعريف
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	مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظمة مثل الأرقام أو الحروف أو الصور الثابتة أو الفيديو أو التسجيلات الصوتية أو الرموز التعبيرية.
الوصول إلى البيانات	القدرة على الوصول المنطقي والمادي إلى البيانات والموارد التقنية للجامعة لغرض استخدامها.
التحقق	التأكد من هوية أي مستخدم أو عملية أو جهاز بصفته متطلباً أساسياً للسماح بالوصول إلى الموارد التقنية.
سرية البيانات	الحفاظ على القيود المصرح بها للوصول إلى البيانات أو الإفصاح عنها.
البيانات المحمية	البيانات المصنفة على أنها (سري للغاية، سري، مقيد).
المعلومات العامة	البيانات بعد المعالجة - غير المحمية - التي تتلقاها أو تنتجها أو تتعامل معها الجامعة مهما كان مصدرها، أو شكلها أو طبيعتها.
البيانات الحساسة	البيانات التي يؤدي فقدانها أو إساءة استخدامها أو الوصول غير المصرح به إليها أو تعديلها إلى ضرر جسيم أو تأثير سلبي على المصالح الوطنية أو أنشطة الجهات الحكومية أو خصوصية الأفراد وحماية حقوقهم.
الفرد	الشخص المتقدم بطلب الاطلاع أو الحصول على المعلومات العامة. 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 لا الحصر- 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.
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.

المصطلح	التعريف
تسريب البيانات الشخصية	الإفصاح عن البيانات الشخصية، أو الحصول عليها، أو تمكين الوصول إليها دون تصريح أو سند نظامي، سواء بقصد أو بغير قصد.
الموافقة الضمنية	هي موافقة لا يتم منحها صراحةً من قِبل صاحب البيانات، ولكنها تُمنح ضمنياً عن طريق أفعال الشخص ووقائع وظروف الموقف، كتوقيع العقود أو الموافقة على الشروط والأحكام.
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.
إشعار الخصوصية	هو بيان 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.
الإفصاح عن البيانات	تمكين أي شخص - عدا الجامعة - من الحصول على البيانات الشخصية أو استعمالها أو الاطلاع عليها بأي وسيلة ولأي غرض.
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.
الموافقة الصريحة	موافقة مكتوبة أو الكترونية تكون صريحة ومحددة وصادرة بإرادة حرة ومطلقة من صاحب البيانات تدل على قبوله لمعالجة بياناته الشخصية.
المستخدم	أي شخصية ذات صفة طبيعية أو اعتبارية تقوم بتطبيق أو استخدام أنظمة الذكاء الاصطناعي لتحقيق أهداف محددة.
صاحب البيانات	الفرد الذي تتعلق به البيانات الشخصية أو من يمثله أو من له الولاية الشرعية عليه.

الأهداف

الغرض من هذه السياسة هو توفير متطلبات مكتب إدارة البيانات الوطنية المبني على أفضل الممارسات والمعايير المتعلقة بحماية المستخدمين لخدمات جامعة الأمير سطام بن عبد العزيز لتنظيم عملية نشر وتبادل استخدام/ إعادة استخدام البيانات المحمية والمعلومات العامة وتقليل المخاطر من خلال التركيز على الأهداف الأساسية للحماية وهي:

1. المحافظة على خصوصية البيانات الشخصية وسرية البيانات الحساسة.
2. المحافظة على حقوق الأفراد عند التعامل مع البيانات الشخصية والمعلومات العامة لدى الجامعة.
3. تعزيز الشفافية وإرساء قواعد الحوكمة من خلال توزيع الأدوار والمسؤوليات.
4. رفع مستوى معايير الرقابة المجتمعية على أداء الجامعة
5. دعم جهود تعزيز النزاهة ومكافحة الفساد من خلال الاطلاع على المعلومات العامة كحق إنساني مكفول.

أولاً النطاق

تنطبق أحكام هذه السياسة على جميع فروع الجامعة التي تقوم كليا أو جزئياً بمعالجة البيانات الشخصية، وكذلك الجهات الخارجية التي تقوم بمعالجة البيانات الشخصية المتعلقة بالأفراد المقيمين في المملكة والتي تتم عبر شبكة الإنترنت أو أي وسيلة أخرى -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 الأحوال التالية:

1. إذا كانت جهة التحكم جهة حكومية وكان جمع البيانات الشخصية أو معالجتها مطلوبة لتحقيق متطلبات نظامية وفقا الأنظمة واللوائح والسياسات المعمول بها في المملكة أو لاستيفاء متطلبات قضائية أو لتنفيذ التزام بموجب اتفاق تكون المملكة طرفا فيه.
2. إذا كان جمع البيانات الشخصية أو معالجتها ضروريًا لحماية الصحة أو السلامة العامة أو حماية المصالح الحيوية للأفراد.

ثانياً | المبادئ الرئيسية لحماية البيانات الشخصية

المبدأ	الوصف
المسؤولية	أن يتم تحديد وتوثيق سياسات وإجراءات الخصوصية الخاصة بالجامعة واعتمادها من قبل المسؤول الأول بالجامعة (أو من يفوضه)، ونشرها إلى جميع الأطراف المعنية بتطبيقها.
الشفافية	أن يتم إعداد إشعار عن سياسات وإجراءات الخصوصية الخاصة بالجامعة يحدد فيها الأغراض التي من أجلها تم معالجة البيانات الشخصية وذلك بصورة محددة وواضحة وصريحة.
الاختيار والموافقة	أن يتم تحديد جميع الخيارات الممكنة لصاحب البيانات الشخصية والحصول على موافقته (الضمنية أو الصريحة) فيما يتعلق بجمع بياناته واستخدامها أو الإفصاح عنها.
الحد من جمع البيانات	أن يقتصر جمع البيانات الشخصية على الحد الأدنى من البيانات الذي يمكن من تحقيق الأغراض المحددة في إشعار الخصوصية.
الحد من استخدام البيانات والاحتفاظ بها والتخلص منها	أن يتم 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 تفتضيه الأنظمة واللوائح والسياسات المعمول بها في المملكة وإتلافها بطريقة آمنة تمنع التسرب، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو الوصول غير المصرح به نظاما.
الوصول إلى البيانات	أن يتم تحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية لمراجعتها وتحديثها وتصحيحها.
الحد من الإفصاح عن البيانات	أن يتم تقييد الإفصاح عن البيانات الشخصية للأطراف الخارجية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدم صاحب البيانات موافقته الضمنية أو الصريحة.
أمن البيانات	أن يتم 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.
جودة البيانات	أن يتم الاحتفاظ بالبيانات الشخصية بصورة دقيقة وكاملة وذات علاقة مباشرة بالأغراض المحددة في إشعار الخصوصية.
المراقبة والامتثال	أن تتم مراقبة الامتثال لسياسات وإجراءات الخصوصية الخاصة بالجامعة، ومعالجة الاستفسارات والشكاوى والنزاعات المتعلقة بالخصوصية.

ثالثاً | حقوق صاحب البيانات

أولاً: الحق في العلم ويشمل ذلك إشعاره بالأساس النظامي أو الاحتياج الفعلي لجمع بياناته الشخصية، والغرض من ذلك، وألا تعالج بياناته لاحقا بصورة تتنافى مع الغرض من جمعها والذي من أجله قدم موافقته الضمنية أو الصريحة.

ثانياً: الحق في الرجوع عن موافقته على معالجة بياناته الشخصية - في أي وقت - مالم يكن هناك أغراض مشروعة تتطلب عكس ذلك.

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

رابعاً | التزامات مكتب البيانات والذكاء الاصطناعي

1. أن تقوم الجامعة بإنشاء وحدة لحوكمة البيانات ضمن مكتب إدارة البيانات والذكاء الاصطناعي تكون مرتبطة بمكاتب إدارة البيانات في الجهات الحكومية التي تم تأسيسها بموجب الأمر السامي الكريم رقم 59766 وتاريخ 1439/11/20هـ ويسند لها مسؤولية تطوير وتوثيق ومراقبة تنفيذ السياسات والإجراءات المعتمدة من الإدارة العليا بالجامعة، على أن تتضمن مهام ومسؤوليات الوحدة وضع المعايير المناسبة لتحديد مستويات حساسية البيانات الشخصية.
2. أن يكون مكتب إدارة البيانات والذكاء الاصطناعي مسؤول عن إعداد وتطبيق السياسات والإجراءات المتعلقة بحماية البيانات الشخصية، ويكون المسؤول الأول بالجامعة أو من يفوضه - مسؤول عن الموافقة عليها واعتمادها .
3. أن يقوم مكتب إدارة البيانات والذكاء الاصطناعي بتقييم المخاطر والآثار المحتملة لأنشطة معالجة البيانات الشخصية وعرض نتائج التقييم على معالي رئيس الجامعة -أو من يفوضه - لتحديد مستوى قبول المخاطر وإقرارها .
4. أن يقوم مكتب إدارة البيانات والذكاء الاصطناعي بمراجعة وتحديث العقود واتفاقيات مستوى الخدمة والتشغيل بما يتوافق مع سياسات وإجراءات الخصوصية المعتمدة من الإدارة العليا للجامعة.
5. أن يقوم مكتب إدارة البيانات والذكاء الاصطناعي بإعداد وتوثيق الإجراءات اللازمة لإدارة ومعالجة انتهاكات الخصوصية وتحديد المهام والمسؤوليات المتعلقة بفريق العمل المختص، والحالات التي يتم بها إشعار الجهة التنظيمية والمكتب حسب التسلسل الإداري - بناءً على قياس شدة الأثر .
6. أن يقوم مكتب إدارة البيانات والذكاء الاصطناعي بإعداد برامج توعوية لتعزيز ثقافة الخصوصية ورفع مستوى الوعي وفقا لسياسات وإجراءات الخصوصية المعتمدة من الإدارة العليا للجامعة.
7. أن يتم إشعار صاحب البيانات - بطريقة ملائمة وقت جمع البيانات - بالغرض والأساس النظامي/الاحتياج الفعلي والوسائل والطرق المستخدمة لجمع ومعالجة ومشاركة البيانات الشخصية وكذلك التدابير الأمنية لضمان حماية الخصوصية حسب الأنظمة واللوائح والسياسات المعمول بها في المملكة.
8. أن يتم إشعار صاحب البيانات عن المصادر الأخرى التي يتم استخدامها في حال تم جمع بيانات إضافية بطريقة غير مباشرة مثل تحليل استطلاعات الرأي أو دراسة الحالات السابقة (من جهات أخرى).
9. أن يتم تزويد صاحب البيانات بالخيارات المتاحة فيما يتعلق بمعالجة البيانات الشخصية والآلية المستخدمة لممارسة هذه الخيارات، ومنها على سبيل المثال:
(Opt-in and Opt-out, Preferences)

10. أن يتم أخذ موافقة صاحب البيانات على معالجة البيانات الشخصية بعد تحديد نوع الموافقة (صريحة أو ضمنية) بناء على طبيعة البيانات وطرق جمعها.
11. أن يكون الغرض من جمع البيانات متوافقًا مع الأنظمة واللوائح والسياسات المعمول بها في المملكة وذو علاقة مباشرة بنشاط الجامعة.
12. أن يكون محتوى البيانات مقتصرة على الحد الأدنى من البيانات اللازمة لتحقيق الغرض من جمعها.
13. أن يتم تقييد جمع البيانات على المحتوى المعد سلفًا (الموضح في القاعدة 12) ويكون بطريقة عادلة (مباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التضليل).
14. أن يقتصر استخدام البيانات على الغرض التي جمعت من أجله.
15. أن تقوم الجامعة بإعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات وفقا للأغراض المحددة والأنظمة واللوائح والسياسات ذات العلاقة.
16. أن تقوم الجامعة بتخزين البيانات الشخصية ومعالجتها داخل الحدود الجغرافية للمملكة لضمان المحافظة على السيادة الوطنية الرقمية لهذه البيانات، ولا يجوز معالجتها خارج المملكة إلا بعد حصول الجامعة على موافقة كتابية من الجهة التنظيمية، بعد تنسيق الجهة التنظيمية مع المكتب.
17. أن تقوم الجامعة بإعداد وتوثيق سياسة وإجراءات التخلص من البيانات لإتلاف البيانات بطريقة آمنة تمنع فقدانها أو إساءة استخدامها أو الوصول غير المصرح به - وتشمل البيانات التشغيلية، المؤرشفة، والنسخ الاحتياطية - وذلك وفقا لما يصدر من الهيئة الوطنية للأمن السيبراني.
18. أن يقوم مكتب البيانات والذكاء الاصطناعي بتضمين أحكام سياستي الاحتفاظ والتخلص من البيانات في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى .
19. أن تقوم الجامعة بتحديد وتوفير الوسائل التي من خلالها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية وذلك لمراجعتها وتحديثها.
20. تقوم الجامعة بالتحقق من هوية الأفراد قبل منحهم الوصول إلى بياناتهم الشخصية وفقا للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص .
21. يحظر مشاركة البيانات الشخصية مع جهات أخرى إلا وفقًا للأغراض المحددة بعد موافقة صاحب البيانات ووفقًا للأنظمة واللوائح والسياسات على أن يتم تزويد الجهات الأخرى بسياسات وإجراءات الخصوصية المتبعة وتضمينها في العقود والاتفاقيات.
22. أن يتم إشعار أصحاب البيانات وأخذ الموافقة منهم في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الأغراض المحددة.
23. أن تقوم الجامعة بأخذ موافقة المكتب - بعد التنسيق مع الجهة التنظيمية - قبل مشاركة البيانات الشخصية مع جهات أخرى خارج المملكة .

24. أن تقوم الجامعة بإعداد وتوثيق وتطبيق الإجراءات اللازمة لضمان دقة البيانات الشخصية واكتمالها وحداثتها وارتباطها بالغرض الذي جمعت من أجله.
25. أن يتم استخدام الضوابط الإدارية والتدابير التقنية المعتمدة في سياسات الجامعة لأمن المعلومات لضمان حماية البيانات الشخصية ومنها على سبيل المثال لا الحصر:

- منح صلاحيات الوصول إلى البيانات وفقا لمهام ومسؤوليات العاملين بطريقة تحول دون تداخل الاختصاص وتتلافى تشتيت المسؤوليات.
- تطبيق الإجراءات الإدارية والتدابير التقنية التي توثق مراحل معالجة البيانات وتوفر إمكانية تحديد المستخدم المسؤول عن كل مرحلة من هذه المراحل (سجلات الاستخدام).
- توقيع العاملين الذين يباشرون عمليات معالجة البيانات على تعهد للمحافظة على البيانات وعدم الإفصاح عنها إلا وفقا للسياسات، والإجراءات، والأنظمة، والتشريعات.
- اختيار العاملين الذين يباشرون عمليات معالجة البيانات ممن يتصفون بالأمانة والمسؤولية ووفقا لطبيعة وحساسية البيانات وسياسة الوصول المعتمدة من قبل الجامعة.
- استخدام التدابير الأمنية المناسبة - كالتشفير، وعزل بيئة التطوير والاختبار عن بيئة التشغيل - لأمن البيانات الشخصية وحمايتها بما يتناسب مع طبيعتها وحساسيتها والوسائط المستخدمة لنقلها وتخزينها وفقا لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.

26. أن يكون مكتب البيانات والذكاء الاصطناعي مسؤول عن مراقبة الامتثال لسياسات وإجراءات الخصوصية بشكل دوري ويتم عرضها على المسؤول الأول للجامعة - أو من يفوضه - كما يتم تحديد وتوثيق الإجراءات التصحيحية التي سيتم اتخاذها في حال عدم الامتثال وإشعار الجهة التنظيمية والمكتب حسب التسلسل التنظيمي.

خامساً | أحكام عامة

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

ثانياً: تقوم الجهات التنظيمية بمراقبة الامتثال لهذه السياسة بشكل دوري.

ثالثاً: يجب على الجامعة الامتثال لهذه السياسة وتوثيق الامتثال وفقا لآليات والإجراءات التي تحددها الجهات التنظيمية .

رابعاً: يجب على الجامعة إبلاغ الجهات التنظيمية فورا ودون تأخير وبما لا يتجاوز 72 ساعة من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشخصية وفقا للآليات والإجراءات التي تحددها الجهات التنظيمية.

خامساً: يجب على الجامعة عند تعاقدها مع جهات المعالجة أن تتحقق بشكل دوري من امتثال جهات المعالجة لهذه السياسة وفقا للآليات والإجراءات التي تحددها الجهات التنظيمية، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها جهات المعالجة.

سادساً: يمارس المكتب أدوار ومهام الجهات التنظيمية على مكتب الجهات غير الخاضع لجهات تنظيمية

سابعاً: يحق للجهات التنظيمية وضع قواعد إضافية لمعالجة أنواع محددة من البيانات الشخصية وفقا لطبيعة وحساسية هذه البيانات بعد التنسيق مع المكتب.

ثامناً: تقوم الجهات التنظيمية بعد التنسيق مع المكتب - بإعداد الآليات والإجراءات التي تنظم عملية معالجة الشكاوى وفقا لإطار زمني محدد وحسب التسلسل التنظيمي للجامعة .

تاسعاً: يقوم المكتب بوضع المعايير اللازمة التي تساعد الجامعة على معرفة ما إذا كان تعيين مسؤول حماية بيانات يعتبر متطلب أساسي أو اختياري.

سادساً | الأدوار والمسؤوليات

1. راعي ومالك وثيقة السياسة: مدير مكتب البيانات والذكاء الاصطناعي.
2. مراجعة السياسة وتحديثها: مكتب البيانات والذكاء الاصطناعي
3. تنفيذ السياسة وتطبيقها: مكتب البيانات والذكاء الاصطناعي وجميع الجهات في الجامعة.

سابعاً | الالتزام بالسياسة

4. يجب على مدير مكتب إدارة البيانات والذكاء الاصطناعي ضمان التزام جامعة الأمير سطام بن عبد العزيز بهذه السياسة دوريا .ً
5. يجب على كافة العاملين في جامعة الأمير سطام بن عبد العزيز الالتزام بهذه السياسة .
6. قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الأمير سطام بن عبد العزيز.