



جامعة الأمير سّطام بن عبدالعزيز
PRINCE SATTAM BIN ABDULAZIZ UNIVERSITY

سياسة حماية البيانات الشخصية

مكتب إدارة البيانات والذكاء الاصطناعي

الإصدار: ٧١,٤

تاريخ الإصدار: ١٧ / ٧ / ٢٠٢٥

التصنيف: عام

المحتويات

١.	المراجع	٣
٢.	المصطلحات والتعريفات	٣
٣.	الغرض	٤
٤.	النطاق	٤
٥.	بيان السياسة	٥
٥-١	المبادئ الرئيسية	٥
٥-٢	التزامات الجامعة	٥
٦.	الاستثناءات	٧
٧.	ملكية السياسة	٧

١. المراجع

رقم المرجع	عنوان المرجع	المصدر	التاريخ
١	سياسات حوكمة البيانات الوطنية مكتب إدارة البيانات الوطنية. (الإصدار الثاني)	مكتب إدارة البيانات الوطنية	٢٠٢١
٢	ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية (الإصدار ١,٥)	مكتب إدارة البيانات الوطنية	٢٠٢١
٣	DAMA Data Management Body of Knowledge (DMBOK). (٢nd ed.) International	DAMA International	٢٠١٧
٤	نظام حماية البيانات الشخصية	مكتب إدارة البيانات الوطنية	٢٠٢٣
٥	اللائحة التنفيذية لنظام حماية البيانات الشخصية	مكتب إدارة البيانات الوطنية	٢٠٢٣
٦	الضوابط الأساسية للأمن السيبراني	الهيئة الوطنية للأمن السيبراني	٢٠٢٤

٢. المصطلحات والتعريفات

المصطلح	التعريف
الجامعة	جامعة الأمير سكام بن عبد العزيز
المكتب	مكتب إدارة البيانات والذكاء الاصطناعي.
الوحدة التنظيمية	الكلية، أو الإدارة، أو القسم المعتمد في هيكل الجامعة التنظيمي.
الموظف	الشخص الطبيعي الذي يعمل لمصلحة الجامعة وتحت إدارتها أو إشرافها مقابل أجر.
مثل بيانات الأعمال	الموظف المعين من قبل الوحدة التنظيمية - بحسب الحال - الذي لا يقل مساهمته الوظيفي عن مدير إدارة، ليكون المسؤول عن الإشراف على تطبيق سياسات وضوابط ومعايير وإجراءات إدارة البيانات فيما يمثل والتي تشمل البيانات التي تم جمعها والاحتفاظ بها من قبل الوحدة التنظيمية التي يرجع إليها، والتحقق من امتثالها للضوابط والسياسات المتعلقة بالبيانات، كذلك متابعة مؤشرات الأداء الرئيسية ومستوى نضج الممارسات المرتبطة بإدارة وحوكمة البيانات داخل الوحدة التنظيمية. أو هو الشخص المسؤول عن البيانات التي يتم جمعها والاحتفاظ بها من قبل الوحدة التنظيمية التي يعمل بها، وغالباً ما يكون في مستوى إداري عالٍ، ويمكن أن يوجد في الجامعة أكثر من ممثل بيانات أعمال.
مختص بيانات الأعمال	الموظف الذي يتم تعيينه من قبل الوحدة التنظيمية في الجامعة لتنفيذ الأعمال الخاصة بتطبيق سياسات وضوابط ومعايير البيانات داخل الوحدة التنظيمية وتحديد وإدارة المشاكل والمخاطر المتعلقة بإدارة البيانات ورفعها إلى ممثل بيانات الأعمال.
تقني وفني بيانات	الموظف المسؤول عن إنشاء وإدارة قواعد البيانات الخاصة بمنصة البيانات/ذكاء الأعمال ونحوه، وبأنظمة الجامعة الرقمية، وتخزين البيانات وضمان توفرها، وتطبيق ضوابط ومعايير هذه السياسة على البيانات المخزنة في قواعد بيانات الجامعة. وكذلك يقدم المساعدة والدعم فيما يخص عمليات وأنشطة إدارة البيانات ذات العلاقة بتقنية المعلومات أو التحول الرقمي.

المصطلح	التعريف
مستخدم البيانات	أي شخص يمنح صلاحية الوصول إلى البيانات بغرض الاطلاع عليها أو استخدامها أو تحديثها وفقاً للمهام المصرح بها من قبل ممثل بيانات الأعمال.
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.
حوكمة البيانات	مجموعة من الممارسات والإجراءات التي تساعد على ضمان إدارة أصول البيانات في الجامعة، بدء من وضع الخطة المعنية بالبيانات وتطوير الضوابط والسياسات وحتى التنفيذ والامتثال. يتم تحقيق ذلك من خلال إطار حوكمي يوضح الأدوار والمسؤوليات بين ذوي العلاقة.
البيانات الشخصية	البيانات الشخصية: كل بيان - مهما كان مصدره أو شكله - من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكناً بصفة مباشرة أو غير مباشرة، ومن ذلك؛ الاسم، ورقم الهوية الشخصية، والعناوين، وأرقام التواصل، وأرقام الرخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي.
صاحب البيانات الشخصية	الفرد الذي تتعلق به البيانات الشخصية.
البيانات الشخصية الحساسة	كل بيان شخصي يتعلق بأصل الفرد العرقي، أو أصله الإثني، أو معتقده الديني، أو الفكري، أو السياسي. وكذلك البيانات الأمنية والجنائية، أو بيانات السمات الحيوية التي تحدد الهوية، أو البيانات الوراثية، أو البيانات الصحية، والبيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهما
تسرب البيانات الشخصية	أي حادثة تؤدي إلى الإفصاح عن البيانات الشخصية أو تلفها أو الوصول غير المشروع إليها، سواء كان ذلك بقصد أو بغير قصد، وبأي وسيلة كانت سواء آلية أو يدوية.
معالجة البيانات الشخصية	جميع العمليات التي تجري 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.
جهات المعالجة	أي جهة حكومية أو جهة اعتبارية عامة مستقلة في المملكة، أو شخصية ذات صفة طبيعية أو اعتبارية خاصة، تعالج البيانات مصلحة الجامعة ونيابة عنها.
الوصول إلى البيانات	القدرة على الوصول المنطقي والمادي إلى البيانات والموارد التقنية الخاصة بالجامعة وذلك لغرض استخدامها في أداء المهام وغيرها.
إتلاف البيانات الشخصية/الإتلاف	يشير إلى أي إجراء يؤدي إلى فقدان، تدمير، أو تغيير البيانات الشخصية بطرق تجعلها غير قابلة للاستعادة أو غير قابلة للاستخدام.

٣. الغرض

تهدف هذه السياسة إلى تحديد المبادئ الرئيسية والضوابط والمسؤوليات ذات العلاقة بأعمال حماية البيانات الشخصية من قبل موظفي الجامعة. وذلك من خلال وضع القواعد العامة التي تنظم جمع ومعالجة ومشاركة البيانات الشخصية بما يضمن المحافظة على خصوصية أصحابها وحماية حقوقهم.

٤. النطاق

تنطبق أحكام هذه السياسة على جميع موظفي الجامعة، وعلى جميع البيانات التي تنتجها أو تتلقاها أو تعالجها الجامعة وذلك وفقاً لأحكام نظام حماية البيانات الشخصية ولوائحه.

٥. بيان السياسة

يجب الالتزام بأحكام ومواد نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم (م/١٩) وتاريخ ٩/٢/١٤٤٣ هـ المعدل بالمرسوم الملكي رقم (م/١٤٨) وتاريخ ٥/٩/١٤٤٤ هـ وكذلك لوائحه فيما يخص جميع الأعمال والالتزامات الخاصة بحماية البيانات الشخصية في الجامعة.

١-٥ المبادئ الرئيسية

- **المسؤولية:** يجب تحديد وتوثيق سياسات وإجراءات حماية البيانات الشخصية الخاصة بالجامعة واعتمادها من قبل صاحب الصلاحية، ونشرها إلى جميع الأطراف المعنية بتطبيقها.
- **الشفافية:** يجب إعداد إشعار خاص بالجامعة يُحدد فيه الأغراض التي من أجلها تم معالجة البيانات الشخصية وذلك بصورة محددة وواضحة وصريحة ويتم نشره على مواقع وبوابات الجامعة.
- **الاختيار والموافقة:** يجب تحديد جميع الخيارات الممكنة لصاحب البيانات الشخصية والحصول على موافقته فيما يتعلق بجمع بياناته واستخدامها أو الإفصاح عنها.
- **الحد من جمع البيانات:** يجب 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:** يجب تقييد معالجة البيانات الشخصية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدّم صاحب البيانات موافقته، والاحتفاظ بها طالما كان ذلك ضرورياً 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 غير المصرّح به نظاماً.
- **الحد من الإفصاح عن البيانات:** يجب تقييد الإفصاح عن البيانات الشخصية للأطراف الخارجية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدّم صاحب البيانات.
- **أمن البيانات:** يجب حماية البيانات الشخصية من التسرب، أو التلف، أو فقدان، أو الاختلاس، أو إساءة الاستخدام؛ أو التعديل أو الوصول غير المصرّح به - وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.
- **جودة البيانات:** يجب الاحتفاظ بالبيانات الشخصية بصورة دقيقة، وكاملة، وذات علاقة مباشرة بالأغراض المحددة في إشعار الخصوصية.
- **المراقبة والامتثال:** أن يتم مراقبة الامتثال لسياسات وإجراءات حماية البيانات الشخصية الخاصة بالجامعة، ومعالجة الاستفسارات والشكاوى والنزاعات المتعلقة بالخصوصية.

٢-٥ التزامات الجامعة

- حق الاطلاع والحصول على أي معلومة غير محمية لدى أي جهة عامة.
- تقوم الجامعة بإعداد وتطبيق السياسات والإجراءات والأدلة الاسترشادية والنماذج المتعلقة بحماية البيانات الشخصية، وتعتمدها.
- يجب أن تقوم الإدارات بتقييم المخاطر والآثار المحتملة لأنشطة معالجة البيانات الشخصية وعرض نتائج التقييم على إدارة وحدة المراجعة الداخلية لتحديد مستوى قبول المخاطر وإقرارها.
- يجب أن يقوم المكتب بمراجعة وتحديث العقود واتفاقيات مستوى الخدمة التنفيذ بما يتوافق مع سياسات وإجراءات حماية البيانات الشخصية.
- يتولى المكتب إعداد إشعار الخصوصية بما يتواءم مع نظام حماية البيانات الشخصية ولوائحه والدليل الاسترشادي لإعداد وتطوير سياسة الخصوصية ومتطلبات الجامعة ونشره في مواقع وبوابات الجامعة التي يتم جمع البيانات الشخصية من خلالها.

- يجب أن تقوم الإدارات التي تعالج البيانات الشخصية بتحديد وتوفير الوسائل التي من خلالها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية وذلك لمراجعتها وتحديثها.
- يجب على المكتب أن يتحقق من هوية الأفراد قبل منحهم الوصول إلى بياناتهم الشخصية وفقاً للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.
- يجب أن تقوم الإدارات المعالجة للبيانات الشخصية بأخذ موافقة صاحب البيانات على معالجة البيانات الشخصية بعد تحديد نوع الموافقة بناءً على طبيعة البيانات وطرق جمعها.
- كما يجب توثيق هذه الموافقة حسب النظام واللوائح.
- يجب أن يكون محتوى البيانات مقتصراً على الحد الأدنى من البيانات اللازمة لتحقيق الغرض من جمعها.
- يجب أن يكون جمع البيانات بطريقة مباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التضليل.
- يجب أن يقتصر استخدام ومعالجة البيانات على الغرض التي جُمعت من أجله.
- تقوم الجامعة بإعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات وفقاً للأغراض المحددة والأنظمة والتشريعات ذات العلاقة.
- تقوم الجامعة بإعداد وتوثيق سياسة وإجراءات التخلص من البيانات ضمن سياسة إدارة الوثائق والمحفوظات لإتلاف البيانات بطريقة آمنة تمنع تسريبها أو إساءة استخدامها أو الوصول غير المصرح به إليها - وتشمل البيانات التشغيلية، المؤرخة، النسخ الاحتياطي - وذلك وفقاً لما يصدر من سياسات إدارة الوثائق والمحفوظات والمركز الوطني للوثائق والمحفوظات.
- تقوم الجامعة بتضمين أحكام نظام حماية البيانات الشخصية ولوائحه الخاصة بالإتلاف في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.
- يجب على جهات المعالجة أن تلتزم بأحكام نظام حماية البيانات الشخصية ولوائحه فيما يتعلق بالإتلاف.
- يحظر مشاركة البيانات الشخصية مع جهات أخرى إلا في الحالات المذكورة في نظام حماية البيانات الشخصية ولوائحه.
- يجب أن يتم إشعار أصحاب البيانات وأخذ الموافقة منهم في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الأغراض المحددة وذلك وفقاً لأحكام نظام حماية البيانات الشخصية ولوائحه.
- أن يتم التنسيق مع المكتب لأخذ موافقة والتأكد من الالتزام بنظام حماية البيانات الشخصية ولوائحه قبل مشاركة البيانات الشخصية مع جهات أخرى خارج المملكة.
- يجب أن يقوم المكتب باستخدام 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 وفقاً لمهام ومسؤوليات العاملين بطريقة تحول دون تدخل الاختصاص وتتلاقى تشبثت المسؤوليات وذلك بحسب سياسات إدارة البيانات ذات العلاقة والمعمول بها في الجامعة.
 - يجب أن يتم تطبيق الإجراءات الإدارية والتدابير التقنية التي توثق مراحل معالجة البيانات وتوفير إمكانية تحديد الموظف المسؤول عن كل مرحلة من هذه المراحل (سجل معالجة البيانات الشخصية).
 - يجب أن يتم توقيع العاملين الذين يباشرون عمليات معالجة البيانات على تعهد للمحافظة على البيانات وعدم الإفصاح عنها إلا وفقاً للسياسات، والإجراءات، والأنظمة، والتشريعات.
 - يجب أن يتم اختيار العاملين الذين يباشرون عمليات معالجة البيانات ممن يتصفون بالأمانة والمسؤولية ووفقاً لطبيعة وحساسية البيانات.
 - يجب أن يتم 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 وفقاً لما يصدر من الهيئة للأمن السيبراني والجهات ذات الاختصاص.

- يجب على المكتب أن يراقب مدى الامتثال لسياسات وإجراءات حماية البيانات الشخصية بشكل دوري وعرضها على صاحب الصلاحية كما يتم تحديد وتوثيق الإجراءات التصحيحية التي سيتم اتخاذها في حال عدم الامتثال وإشعار مكتب إدارة البيانات الوطنية.
- يجب إبلاغ مكتب إدارة البيانات الوطنية فوراً ودون تأخير وبما لا يتجاوز ٧٢ ساعة من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشخصية وفقاً للآليات والإجراءات التي يحددها مكتب إدارة البيانات الوطنية.
- يجب إبلاغ صاحب البيانات الشخصية في حال الحاجة وذلك وفقاً لإجراء تسريب البيانات المعتمد في الجامعة.
- يجب على المكتب عند تعاقد الجامعة مع جهات معالجة أو جهات تحكم أن يتم التحقق بشكل دوري من امتثالها لنظام حماية البيانات الشخصية ولوائحها وفقاً للآليات والإجراءات التي تحددها الجامعة على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها هذه الجهات.

٦. الاستثناءات

أي استثناء لأي ضابط ذكر في هذه السياسة يجب أن يتم الموافقة عليه من قبل مكتب إدارة البيانات والذكاء الاصطناعي.

٧. ملكية السياسة

تعود ملكية هذه السياسة لمكتب إدارة البيانات والذكاء الاصطناعي في جامعة الأمير سكام بن عبد العزيز ويتولى إصدار النسخ المحدث منها، ويجب الحصول على موافقة مكتب إدارة البيانات والذكاء الاصطناعي على أي تغييرات أو تحديثات على هذه الوثيقة.

في حال عدم الامتثال لضوابط السياسة، يخضع منسوبي الجامعة المعنيين للمساءلة حيث يقوم المكتب بتحديد الضرر الناجم عن عدم الامتثال لاتخاذ الإجراء النظامي المناسب.