سياسة حماية البيانات الشخصية

وصف السياسة

تهدف سياسة حماية البيانات الشخصية إلى وضع القواعد والضوابط الأساسية لحماية هذه البيانات المتعلقة بمنسوبي الجامعة والمستفيدين من خدماتها وضمان سلامتها.

نطاق السياسة

تنطبق أحكام هذه السياسة على جميع الجهات في الجامعة، والتي تقوم كلياً أو جزئياً 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 جُمعت من أجله أو الإفصاح عنها دون موافقته أو نقلها إلى خارج المملكة في الأحوال التالية:

1. إذا كانت جهة التحكم جهة حكومية وكان جمع البيانات الشخصية أو معالجتها مطلوباً لتحقيق متطلبات نظامية وفقاً للأنظمة واللوائح والسياسات المعمول بها في المملكة أو الاستيفاء متطلبات قضائية أو لتنفيذ التزام بموجب اتفاق تكون المملكة طرفاً فيه.
2. إذا كان جمع البيانات الشخصية أو معالجتها ضرورياً لحماية الصحة أو السلامة العامة أو حماية المصالح الحيوية للأفراد.

المبادئ الرئيسية لحماية البيانات الشخصية

- **المبدأ الأول: المسؤولية**

أن يتم تحديد وتوثيق سياسات وإجراءات الخصوصية واعتمادها من قبل الجامعة ونشرها إلى جميع الأطراف المعنية بتطبيقها.

- **المبدأ الثاني: الشفافية**

أن يتم إعداد إشعار عن سياسات وإجراءات الخصوصية الخاصة بجهة التحكم يحدد فيه الأغراض التي من أجلها تمت معالجة البيانات الشخصية وذلك بصورة محددة وواضحة وصريحة.

- **المبدأ الثالث: 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.

- **المبدأ الرابع: الحد من جمع البيانات**

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

- **المبدأ الخامس: 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 ضرورياً لتحقيق الأغراض المحددة أو لما تقتضيه الأنظمة واللوائح والسياسات المعمول بها في المملكة وإتلافها بطريقة آمنة تمنع التسرب، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو الوصول غير المصرح به نظاماً.

- **المبدأ السادس: الوصول إلى البيانات**

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

- **المبدأ السابع: 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.

- **المبدأ الثامن: أمن البيانات**

أن تتم حماية البيانات الشخصية من التسرب، أو التلف، أو الفقدان، أو الاختلاس، 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**

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

- **المبدأ العاشر: المراقبة والامتثال**

أن تتم مراقبة الامتثال لسياسات وإجراءات الخصوصية الخاصة بجهة التحكم، ومعالجة الاستفسارات والشكاوى والنزاعات المتعلقة بالخصوصية.

حقوق صاحب البيانات

أولاً: 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.

ثانياً: الحق في الرجوع عن موافقته على معالجة بياناته الشخصية - في أي وقت – ما لم تكن هناك أغراض مشروعة تتطلب عكس ذلك.

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

التزامات جهة التحكم

1. يجب على الجامعة إعداد وتطبيق السياسات والإجراءات المتعلقة بحماية البيانات الشخصية، بموافقة واعتماد معالي رئيس الجامعة أو من يقوم بتفويضه عليها.

2. يجب على الجامعة أن تقوم بتقييم المخاطر والآثار المحتملة لأنشطة معالجة البيانات الشخصية وعرض نتائج التقييم على معالي رئيس الجامعة – أو من يفوضه – لتحديد مستوى قبول المخاطر وإقرارها.

3. يجب على الجامعة أن تقوم بمراجعة وتحديث العقود واتفاقيات مستوى الخدمة والتشغيل بما يتوافق مع سياسات وإجراءات الخصوصية المعتمدة من الإدارة العليا.

4. يجب على الجامعة أن تقوم بإعداد وتوثيق الإجراءات اللازمة لإدارة ومعالجة انتهاكات الخصوصية وتحديد المهام والمسؤوليات المتعلقة بفريق العمل المختص، والحالات التي يتم بها إشعار الجهة التنظيمية ومكتب إدارة البيانات الوطنية حسب التسلسل الإداري بناءاً على قياس شدة الأثر.

5. يجب على الجامعة أن تقوم بإعداد برامج توعوية لتعزيز ثقافة الخصوصية ورفع مستوى الوعي وفقاً لسياسات وإجراءات الخصوصية المعتمدة من الإدارة العليا.

6. 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.

7. أن يتم إشعار صاحب البيانات عن المصادر الأخرى التي يتم استخدامها في حال تم جمع بيانات إضافية بطريقة غير مباشرة (من جهات أخرى).

8. 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).

9. أن يتم أخذ موافقة صاحب البيانات على معالجة البيانات الشخصية بعد تحديد نوع الموافقة (صريحة او ضمنية) بناءاً على طبيعة البيانات وطرق جمعها.

10. أن يكون الغرض من جمع البيانات متوافقاً مع الأنظمة واللوائح والسياسات المعمول بها في المملكة وذا علاقة مباشرة بنشاط الجامعة.

11. أن يكون محتوى البيانات مقتصراً على الحد الأدنى من البيانات اللازمة لتحقيق الغرض من جمعها.

12. أن يتم تقييد جمع البيانات على المحتوى المعد سلفاً (الموضح في القاعدة 11) ويكون بطريقة عادلة (مباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التضليل).

13. أن يقتصر استخدام البيانات على الغرض التي جمعت من أجله.

14. يجب على الجامعة أن تقوم بإعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات وفقاً للأغراض المحددة والأنظمة والتشريعات ذات العلاقة.

15. يجب على الجامعة أن تقوم بتخزين البيانات الشخصية ومعالجتها داخل الحدود الجغرافية للمملكة لضمان المحافظة على السيادة الوطنية الرقمية لهذه البيانات، ولا تجوز معالجتها خارج المملكة إلا بعد الحصول على موافقة كتابية من الجهة التنظيمية، بعد تنسيق الجهة التنظيمية مع مكتب إدارة البيانات الوطنية.

16. يجب على الجامعة أن تقوم بإعداد وتوثيق سياسة وإجراءات التخلص من البيانات لإتلاف 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.

17. يجب على الجامعة أن تقوم بتضمين أحكام سياستي الاحتفاظ والتخلص من البيانات في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.

18. يجب على الجامعة أن تقوم بتحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية وذلك لمراجعتها وتحديثها.

19. يجب على الجامعة أن تقوم بالتحقق من هوية الأفراد قبل منحهم الوصول إلى بياناتهم الشخصية وفقاً للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.

20. 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 وتضمينها في العقود والاتفاقيات.

21. أن يشعر أصحاب البيانات وتؤخذ الموافقة منهم في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الأغراض المحددة.

22. يجب على الجامعة أن تقوم بأخذ موافقة مكتب إدارة البيانات الوطنية - بعد التنسيق مع الجهة التنظيمية - قبل مشاركة البيانات الشخصية مع جهات أخرى خارج المملكة.

23. يجب على الجامعة أن تقوم بإعداد وتوثيق وتطبيق الإجراءات اللازمة لضمان دقة البيانات الشخصية واكتمالها وحداثتها وارتباطها بالغرض الذي جمعت من أجله.

24. 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 وفقاً لمهام العاملين ومسؤولياتهم 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 وفقاً للسياسات، والإجراءات، والأنظمة، والتشريعات.
- اختيار العاملين الذين يباشرون عمليات معالجة البيانات ممن يتصفون بالأمانة والمسؤولية ووفقاً 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 وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.

25. يجب على الجامعة أن تكون مسؤولة عن مراقبة الامتثال لسياسات وإجراءات الخصوصية بشكل دوري ويتم عرضها على معالي رئيس الجامعة – أو من يفوضه – كما يتم تحديد وتوثيق الإجراءات التصحيحية التي سيتم اتخاذها في حال عدم الامتثال وإشعار الجهة التنظيمية ومكتب إدارة البيانات الوطنية حسب التسلسل التنظيمي.

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 وفقاً للآليات والإجراءات التي تحددها الجهة التنظيمية.
- **رابعاً:** يجب على الجامعة إبلاغ الجهة التنظيمية فوراً ودون تأخير وبما لا يتجاوز 72 ساعة من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشخصية وفقاً للآليات والإجراءات التي تحددها الجهة التنظيمية.
- **خامساً:** يجب على الجامعة عند تعاقدها مع جهات المعالجة أن تتحقق بشكل دوري من امتثال جهات المعالجة لهذه السياسة وفقاً للآليات والإجراءات التي تحددها الجهة التنظيمية، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها جهات المعالجة.
- **سادساً:** يحق للجهة التنظيمية وضع قواعد إضافية لمعالجة أنواع محددة من البيانات الشخصية وفقاً لطبيعة وحساسية هذه البيانات بعد التنسيق مع مكتب إدارة البيانات الوطنية.
- **سابعاً:** تقوم الجهة التنظيمية – بعد التنسيق مع مكتب إدارة البيانات الوطنية– بإعداد الآليات والإجراءات التي تنظم عملية معالجة الشكاوى وفقاً لإطار زمني محدد وحسب التسلسل التنظيمي.
- **ثامناً:** يقوم مكتب إدارة البيانات الوطنية بوضع المعايير اللازمة التي تساعد جهات التحكم على معرفة ما إذا كان تعيين مسؤول حماية بيانات يعتبر متطلب أساسي أو اختياري.
- **تاسعاً:** تلتزم الجامعة بتطبيق أحكام نظام حماية البيانات الشخصية ولوائحه التنفيذية بما لا يتعارض مع ما لها من اختصاصات ومهمات.

الأدوار المتعلقة بالسياسة

- **مكتب إدارة البيانات ودعم اتخاذ القرار:** الجهة المسؤولة عن التشريعات وتدقيق الامتثال للسياسة.
- **إدارة الأمن السيبراني:** جهة مسؤولة عن التنظيم والتشغيل للسياسة.
- **عمادة تقنية المعلومات:** جهة مسؤولة عن التنظيم والتشغيل للسياسة.

تطبيق السياسة

1. يكون الامتثال لهذه السياسة إلزامي لكافة منسوبي الجامعة بحسب وظائفهم.
2. في حال الإخلال ببنود هذه السياسة يتم اتخاذ الإجراءات المناسبة وفقًا للأنظمة واللوائح الخاصة بالجامعة، أو اتخاذ الإجراءات المناسبة وفقًا لما هو منصوص عليه في الأنظمة واللوائح السارية في المملكة العربية السعودية في حال عدم وجود إجراءات محددة في الجامعة.