*هذا الدليل خاضع للمراجعة والتحسين المستمر.

دليل سياسة حوكمة البيانات المفتوحة بجامعة شقراء

(الإصدار الأول - 2022)


بسم الله الرحمن الرحيم

الإصدار	الأول/ مايو2022-15
مصادر إعداد الدليل	مكتب إدارة البيانات الوطنية.
الفئة المستهدفة	منسوبو جامعة شقراء.
الجهة المعدة للدليل	وكالة الجامعة للتطوير والجودة.
الجهة المعتمدة للدليل	مكتب التحول المؤسسي (إحْكَام).

المحتويات

مقدمة

في عمل مستمر ودؤوب من جامعة شقراء في سبيل تطوير العملية الإدارية والتعليمية وتحسينها، فقد عملت على إنشاء سلسلة من الأدلة الموجهة لمنسوبي الجامعة من طلبة، وأعضاء هيئة تدريس، وموظفين. ويحوي كل دليل بين دفتيه معلومات ضرورية وهامة يستفيد منها كل من يطلع عليه من داخل وخارج الجامعة، بحيث يساعده على رسم صورة واضحة حول الأنظمة والقوانين المتبعة في جامعة شقراء.

ومما لا شك فيه إن دليل سياسة حوكمة البيانات؛ سيساعد على تكوين صورة واضحة ومبسطة عن أنظمة الجامعة فيما يتعلق بطريقة تعامل الجامعة مع بياناتها الإدارية وبيانات منسوبيها، مما يشعرهم بالثقة حول طريقة التعامل النظامية والمحوكمة مع البيانات في الجامعة. آملين أن يلبي هذا الدليل احتياجات منسوبي الجامعة من المعلومات، وأن يمدهم بالإجابات الكافية لجميع الاستفسارات والتساؤلات التي تتبادر إلى أذهانهم.

الميثاق الأخلاقي للموظف بجامعة شقراء

هو مجموعة القواعد والمعايير الأخلاقية المثالية التي تنظم السلوك المهني الواجب إتباعه من قبل العاملين في الجامعة. وهذا يعكس الالتزام الأدبي والأخلاقي داخل الحرم الجامعي، ومنها:

أخلاقيات التعامل الجامعي:

وترتكز على مجموعة من السمات التي تميز العمل الجامعي أهمها:

- التمتع بحسن الأخلاق والتسامح في المعاملة.
- الاحترام المتبادل بين الموظفين بعضهم بعضًا وباقي منسوبي الجامعة من طلبة وأعضاء هيئة تدريس، ومع المراجعين.
- حسن التصرف والاتزان في ردود الأفعال خلال المواقف المختلفة.
- الإخلاص في العمل واعتبار الوظيفة شرفاً أخلاقياً ورسالة.

- الالتزام بحسن السمت والهيئة والمظهر اللائق.
- الدوام بمظهر لائق ومناسب وبما يتلاءم مع الأنظمة المعمول بها في القطاعات الحكومية بالدولة.
- التحلي بصفة الجدية وروح المسؤولية والتعاون الجماعي لإنجاز الأعمال.
- الحفاظ على مرافق الجامعة وترشيد استخدامها.
- الحرص على حضور جميع الاجتماعات وورش العمل التي تقيمها الكليات وإدارة الجامعة.
- أخلاقيات الحوار العملي:

- الحفاظ على لغة الحوار الهادئ البنّاء فيما يخص جوانب العمل المختلفة .
- إبراز الجوانب الإيجابية من الحوار لإزالة الأمور السلبية.
- الالتزام بالقواعد والأعراف والتقاليد الجامعية.

نبذة عن جامعة شقراء

نشأة جامعة شقراء:

تعد جامعة شقراء من أحدث الجامعات السعودية التي صدر القرار السامي الملكي بإنشائها، حيث صدر المرسوم الملكي الكريم رقم (7305/ م ب وتاريخ 1430/9/3هـ) بإنشاء جامعة شقراء.

يقع المقر الرئيس للجامعة بمدينة شقراء وتضم الجامعة حالياً أكثر من عشرين كلية موزعة في عدة محافظات ومراكز وهي: شقراء، والقويعية، والدوادمي، وساجر، وضرماء، وعفيف، والمزاحمية، وثادق والمحمل، وتضم، هذه الكليات العديد من الأقسام الأكاديمية، التي تمنح مختلف الدرجات العلمية في التعليم العالي للتخصصات النظرية والتطبيقية والهندسية والطبية والتقنية؛ إذ تغطي هذه التخصصات مدينة شقراء والمحافظات التابعة لها، وتبلغ مساحة الحرم الجامعي للمدينة الجامعية (13 مليونًا و707 آلاف و436 مترًا مربعًا). وقد بلغ عدد طلاب الجامعة 28112 طالباً وطالبة، وبلغ عدد أعضاء هيئة التدريس ومن في حكمهم 1337عضواً، وبلغ عدد الموظفين 987 موظفاً وموظفة. كما تشكّلت في الجامعة منظومة إدارية بالإضافة للمنظومة الأكاديمية المتكاملة، ففيها (5) وكالات، و(10)عمادات مساندة، إضافة إلى الإدارات والوحدات مثل إدارة التعاون الدولي ووحدة الوعي الفكري، ووحدة الإرشاد الأكاديمي والنفسي، وجميعها تركز وظائفها الأساسية على دعم العملية التعليمية التي تقدمها الجامعة للطلاب والطالبات بمختلف المستويات الدراسية، وخدمة الجامعة والمجتمع بجميع فئاته وأفراده، لتلبية احتياجات سوق العمل السعودي بالقطاعين العام والخاص.

وفي الجامعة انتهت المرحلة الأولى من البنية التحتية للكليات والعمادات، وكذلك إسكان أعضاء هيئة التدريس، وتم تشغيل عدد من مباني كليات الطالبات في عدد من كليات الجامعة في مختلف

المحافظات مثل: ثادق، وحريملاء، وضرماء، والقويعية، وشقراء، والدوادمي، وعفيف، ولا زال العمل جارياً على تجهيز مباني الكليات للطلاب. ولقد قامت الجامعة ببناء العديد من القاعات الدراسية والمرافق المؤقتة لتلبية احتياجات الأقسام الأكاديمية والكليات والإدارات المختلفة في كليات الطلاب.

رؤية جامعة شقراء ورسالتها وأهدافها

رؤية الجامعة:

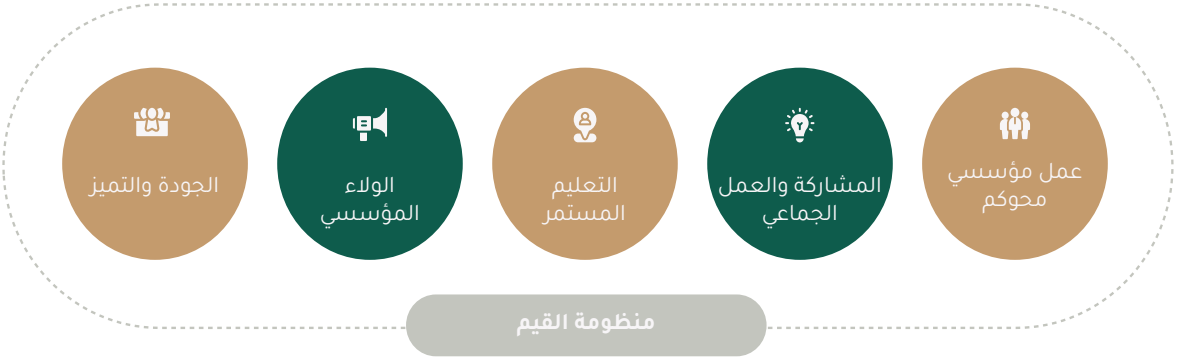
تعليم متميز، بحث علمي مؤثر، مجتمع حيوي.

الرسالة

بناء كفاءات متخصصة ومميزة تواكب متغيرات سوق العمل من خلال برامج تعليمية تنافسية، وكوادر مؤهلة في بيئة أكاديمية وبحثية جاذبة، وأنظمة فاعلة، وشراكات مجتمعية مثمرة.

القيم الحاكمة

- ✓ تلتزم الجامعة بالقيم التالية:



الأهداف الاستراتيجية

1. رفع كفاءة وفاعلية البيئة التنظيمية والإدارية والمالية.
2. الارتقاء بكفاءة وفعالية الموارد البشرية الأكاديمية والإدارية.
3. تحقيق مخرجات تعليمية تنافسية تواكب متغيرات سوق العمل.
4. تقديم بحث علمي وفق الأولويات التنموية والمجتمعية.
5. تعزيز الشراكة مع المجتمع والمساهمة الفعالة في تنميته وخدمته.
6. تحسين البنى التحتية والتقنية والخدمات المساندة.

مصطلحات الدليل

البيانات الشخصية: كل بيان - مهما كان مصدره أو شكله- من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلًا 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 منظّمة، 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 للجهة لغرض استخدامها.

توافر البيانات: ضمان إمكانية الوصول المناسب والموثوق إلى البيانات واستخدامها عند الحاجة.

سرية البيانات: الحفاظ على القيود المصرح بها للوصول إلى البيانات أو الإفصاح عنها.

سلامة البيانات: حماية البيانات من أي تعديل أو إتلاف غير مصرّح به نظاماً.

تمهيد

تعد البيانات الشخصية مجموعة فرعية من المعلومات العامة وفقاً لمستويات التصنيف الموضحة في سياسة تصنيف البيانات الصادرة من مكتب إدارة البيانات الوطنية. (للاطلاع على سياسة تصنيف البيانات (اضغط هنا).

الفصل الأول: سياسة حماية البيانات الشخصية

أولاً: نطاق السياسة

تنطبق أحكام هذه السياسة على جميع الجهات في الجامعة، التي تقوم كلياً أو جزئياً بمعالجة البيانات الشخصية.

يستثنى من نطاق تطبيق هذه السياسة ما ذكر في دليل سياسات حوكمة البيانات الوطنية (للاطلاع اضغط هنا). ولا يجوز 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 إلا 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 لاستيفاء متطلبات قضائية، أو لتنفيذ التزام بموجب اتفاق تكون المملكة طرفاً فيه.
2. إذا كان جمع البيانات الشخصية أو معالجتها ضرورياً لحماية الصحة أو السمعة العامة، أو حماية المصالح الحيوية للأفراد.

ثانياً: المبادئ الرئيسة لحماية البيانات الشخصية

المبدأ الأول: المسؤولية

أن يتم تحديد وتوثيق سياسات وإجراءات الخصوصية الخاصة بجهة التحكم واعتمادها من قبل المسؤول الأول بالجهة (أو من يفوضه)، 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 قدّم 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 المصرّح به نظاماً.

المبدأ السادس: الوصول إلى البيانات

أن يتم تحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات 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 قدّم 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 المصرّح 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.

ثالثاً: حقوق صاحب البيانات

أولًا: 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 قدّم 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.

رابعاً: التزامات جهة التحكم (عمادة تقنية المعلومات)

1.أن تكون جهة التحكم مسؤولة عن إعداد وتطبيق السياسات والإجراءات المتعلقة بحماية البيانات الشخصية، ويكون المسؤول الأول بالجهة - أو من يفوضه - مسؤولًا عن الموافقة عليها واعتمادها.

2.أن تقوم عمادة تقنية المعلومات بإنشاء وحدة لحوكمة البيانات تكون مرتبطة بمكاتب إدارة البيانات في الجهات الحكومية التي تم تأسيسها بموجب الأمر السامي الكريم رقم 59766 وتاريخ 20/ 11/ 1439هـ، وتسند إليها 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.

3.أن تقوم عمادة تقنية المعلومات بتقييم المخاطر والآثار المحتملة لأنشطة معالجة البيانات الشخصية وعرض نتائج التقييم على رئيس الجامعة - أو من يفوضه - لتحديد مستوى قبول المخاطر وإقرارها.

4.أن تقوم عمادة تقنية المعلومات بمراجعة وتحديث العقود واتفاقيات مستوى الخدمة والتشغيل بما يتوافق مع سياسات وإجراءات الخصوصية المعتمدة من الإدارة العليا للجامعة.

5.أن تقوم عمادة تقنية المعلومات 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 تقوم عمادة تقنية المعلومات بإعداد برامج توعوية لتعزيز ثقافة الخصوصية ورفع مستوى الوعي، وفقاً 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 (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: (Preferences, Opt-in and Opt-out)

10. أن يتم أخذ موافقة صاحب البيانات على معالجة البيانات الشخصية بعد تحديد نوع الموافقة (صريحة أو ضمنية) بناءً على طبيعة البيانات وطرق جمعها.

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

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

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

14. أن يقتصر استخدام البيانات على الغرض الذي جُمعت من أجله.

15. أن تقوم عمادة تقنية المعلومات بإعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات وفقاً للأغراض المحددة والأنظمة والتشريعات ذات العلاقة.

16.أن تقوم عمادة تقنية المعلومات بتخزين البيانات الشخصية ومعالجتها داخل الحدود الجغرافية للمملكة لضمان المحافظة على السيادة الوطنية الرقمية لهذه البيانات، ولا تجوز معالجتها خارج المملكة إلا بعد حصول عمادة تقنية المعلومات على موافقة كتابية من الجهة التنظيمية، بعد تنسيق الجهة التنظيمية مع مكتب إدارة البيانات الوطنية.

17.أن تقوم عمادة تقنية المعلومات 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، والمؤرشفة، والنسخ الاحتياطية، وذلك وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني.

18. أن تقوم عمادة تقنية المعلومات بتضمين أحكام سياستي الاحتفاظ والتخلص من البيانات في العقود فيحال إسناد هذه المهام إلى جهات معالجة أخرى.

19. أن تقوم عمادة تقنية المعلومات بتحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية؛ وذلك لمراجعتها وتحديثها.

20. أن تقوم عمادة تقنية المعلومات بالتحقق من هوية الأفراد قبل منحهم الوصول إلى بياناتهم الشخصية، وفقاً للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.

21. تحظر مشاركة البيانات الشخصية مع جهات أخرى إلا وفقاً للأغراض المحددة بعد موافقة صاحب البيانات، ووفقاً للأنظمة واللوائح والسياسات، على أن تُزوّد الجهات الأخرى بسياسات وإجراءات الخصوصية المتبعة ويتم تضمينها في العقود والاتفاقيات.

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

23.أن تقوم عمادة تقنية المعلومات بأخذ موافقة المكتب - بعد التنسيق مع الجهة التنظيمية - قبل مشاركة البيانات الشخصية مع جهات أخرى خارج المملكة.

24. أن تقوم عمادة تقنية المعلومات بإعداد وتوثيق وتطبيق الإجراءات اللازمة لضمان دقة البيانات الشخصية واكتمالها وحداثتها وارتباطها بالغرض الذي جُمعت من أجله.

25. أن يتم استخدام الضوابط الإدارية والتدابير التقنية المعتمدة في سياسات الجهة المسؤولة عن أمن 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 إلا 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.

26. أن تكون عمادة تقنية المعلومات مسؤولة عن مراقبة الامتثال لسياسات وإجراءات الخصوصية بشكل دوري، ويتم عرضها على سعادة رئيس الجامعة - 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

أولًا: يجب على عمادة تقنية المعلومات الامتثال لهذه السياسة وتوثيق الامتثال وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية.

ثانياً: يجب على عمادة تقنية المعلومات إبلاغ الجهات التنظيمية فوراً ودون تأخير وبما لا يتجاوز 72 ساعة من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشخصية، وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية.

ثالثاً: يجب على عمادة تقنية المعلومات عند تعاقدها مع جهات المعالجة أن تتحقق بشكل دوري من امتثال جهات المعالجة لهذه السياسة وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها جهات المعالجة.

رابعاً: يحق لعمادة تقنية المعلومات وضع قواعد إضافية لمعالجة أنواع محددة من البيانات الشخصية وفقاً لطبيعة وحساسية هذه البيانات بعد التنسيق مع المكتب.

خامساً: تقوم عمادة تقنية المعلومات - بعد التنسيق مع المكتب - بإعداد الآليات والإجراءات التي تنظم عملية معالجة الشكاوى وفقاً لإطار زمني محدد وحسب التسلسل التنظيمي للجهات.

الفصل الثاني: سياسة مشاركة البيانات

أولًا: نطاق السياسة

تنطبق أحكام هذه السياسة على جميع جهات الجامعة وذلك لمشاركة البيانات التي تنتجها هذه الجهات - مع جهات أخرى داخل الجامعة أو خارجها سواءً كانت حكومية أو جهات خاصة أو أفراد - مهما كان مصدر هذه البيانات، أو شكلها أو طبيعتها، ويشمل ذلك السجلات الورقية ورسائل البريد الإلكتروني، والبيانات المخزنة على الوسائط الإلكترونية أو أشرطة الصوت أو الفيديو، أو الخرائط أو الصور الفوتوغرافية أو المخطوطات أو الوثائق المكتوبة بخط اليد، أو أي شكل آخر من أشكال البيانات المسجلة.

لا تنطبق أحكام هذه السياسة على مشاركة بيانات القطاع الخاص أو البيانات التي لدى الأفراد، كما لا تنطبق أحكام هذه السياسة في حال كانت الجهة الطالبة للبيانات جهة حكومية وكان الطلب لأغراض أمنية أو لاستيفاء متطلبات قضائية.

ثانياً: المبادئ الرئيسة لمشاركة البيانات

المبدأ الأول: تعزيز ثقافة المشاركة

على جميع جهات الجامعة مشاركة البيانات الرئيسية التي تنتجها، وذلك لتحقيق التكامل بين هذه الجهات وتبني "مبدأ المرّة الواحدة" للحصول على البيانات من مصادرها الصحيحة والحد من ازدواجيتها وتعارضها وتعدد مصادرها. وفي حال تم طلب البيانات من غير مصدرها الأساسي، فعلى الجهة المطلوب منها مشاركة هذه البيانات أخذ موافقة الجهة الرئيسة وهي مصدر البيانات قبل مشاركتها مع الجهة الطالبة.

المبدأ الثاني: مشروعية الغرض

أن تُشارك البيانات لأغراض مشروعة مبنية على أساس نظامي أو احتياج عملي مسوغ يهدف إلى تحقيق مصلحة عامة، دون إلحاق أي ضرر بالمصالح الوطنية،

أو أنشطة الجهات أو خصوصية الأفراد أو سلامة البيئة. ويستثنى من ذلك البيانات والجهات المستثناة بأوامر سامية.

المبدأ الثالث: الوصول المصرّح به

أن يكون لدى جميع الأطراف المُشارِكة في مشاركة البيانات صلاحية الاطلاع على هذه البيانات والحصول عليها واستخدامها (والتي قد تتطلب المسح الأمني حسب طبيعة وحساسية البيانات)، بالإضافة إلى توافر المعرفة، والمهارة، والأشخاص المؤهلين والمدربين بشكل صحيح للتعامل مع البيانات المشتركة.

المبدأ الرابع: الشفافية

يجب على جميع الأطراف المشاركة في عمليات مشاركة البيانات إتاحة جميع المعلومات الضرورية لتبادل البيانات، بما في ذلك: البيانات المطلوبة، والغرض من جمعها، ووسائل نقلها، وطرق حفظها، والضوابط المستخدمة لحمايتها وآلية التخلص منها.

المبدأ الخامس: المسؤولية المشتركة

أن تكون جميع الأطراف المُشارِكة في مشاركة البيانات مسؤولة مسؤولية مشتركة عن قرارات مشاركة البيانات ومعالجتها وفقاً للأغراض المحددة، وضمان تطبيق الضوابط الأمنية المنصوص عليها في اتفاقية مشاركة البيانات، والأنظمة والتشريعات والسياسات ذات العلاقة.

المبدأ السادس: أمن البيانات

أن تقوم جميع الأطراف المُشارِكة في مشاركة البيانات بتطبيق الضوابط الأمنية المناسبة لحماية البيانات ومشاركتها في بيئة آمنة وموثوقة، وفقاً للأنظمة والتشريعات ذات العلاقة، ووفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني.

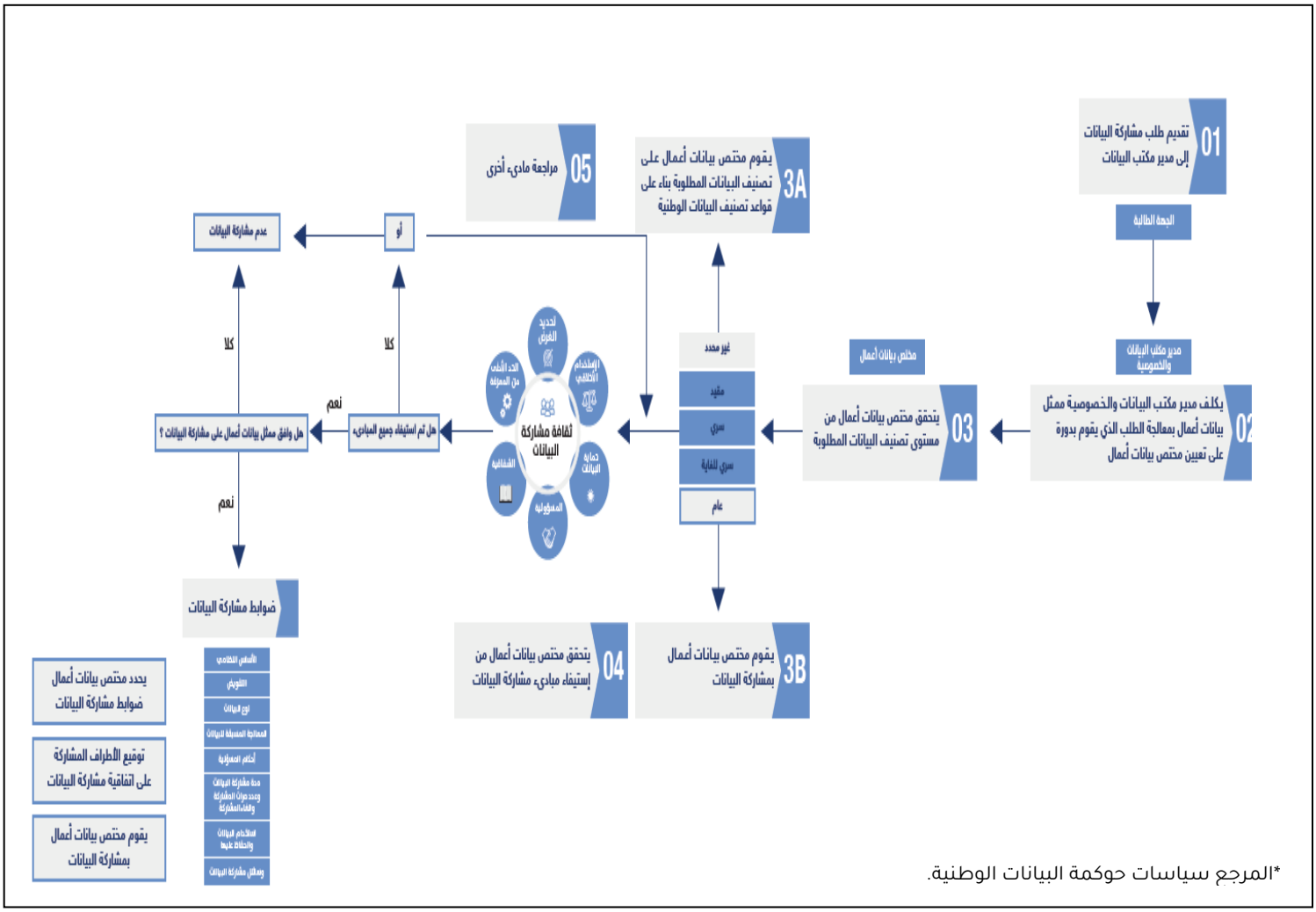
المبدأ السابع: الاستخدام الأخلاقي

أن تقوم جميع الأطراف المُشارِكة في مشاركة البيانات بتطبيق الممارسات الأخلاقية أثناء عملية مشاركة البيانات؛ لضمان استخدامها في إطار من العدالة والنزاهة والأمانة والاحترام، وعدم الاكتفاء بالالتزام بسياسات أمن المعلومات أو الالتزام بالمتطلبات التنظيمية والتشريعية ذات العلاقة.

ثالثاً: الخطوات اللازمة لإجراء عملية مشاركة البيانات

تم تحديد الخطوات الأساسية لعملية مشاركة البيانات لمساعدة الجهات على توحيد ممارسات المشاركة وضمان استيفاء جميع الضوابط والمتطلبات اللازمة، والتي قد لا تتجاوز 3 أشهر.

الشكل (٣) أدناه يوضح الخطوات اللازمة لمشاركة البيانات



*المرجع سياسات حوكمة البيانات الوطنية.

1.يقوم مقدّم الطلب - سواء أكان جهة داخل الجامعة أو جهة حكومية أو خاصة أو فرداً- بإرسال طلب مشاركة بيانات إلى عمادة تقنية المعلومات، على أن يُرسل الطلب عن طريق مكتب الجهة في حال كان مقدم الطلب جهة حكومية.

2.تقوم عمادة تقنية المعلومات بإحالة الطلب إلى ممثل بيانات الأعمال المختص والذي بدوره يقوم بتوجيه هذا الطلب إلى أحد مختصي بيانات الأعمال لتقييم هذا الطلب ومعالجته.

3.يقوم مختص بيانات الأعمال بالتحقق من مستوى تصنيف البيانات المطلوبة:

أ. في حالة عدم تحديد مستوى التصنيف، يجب على مكتب الجهة - المطلوب منها مشاركة البيانات- تصنيف البيانات المطلوبة وفقاً لسياسة تصنيف البيانات.

ب. في حالة تحديد مستوى التصنيف على أنه "عام"، يمكن لمختص بيانات الأعمال مشاركة البيانات المطلوبة دون تقييم الطلب وفقاً للمبادئ الرئيسية لمشاركة البيانات.

ج. في حالة تحديد مستوى التصنيف على أنه "مقيّد" أو "سري" أو "سري للغاية"، يتعين على مختص بيانات الأعمال تقييم الطلب وفقاً للمبادئ الرئيسية لمشاركة البيانات.

4.يجب على مختص بيانات الأعمال في الجامعة استكمال عملية المشاركة إذا تم استيفاء جميع مبادئ مشاركة البيانات بالكامل.

5.لا يجوز لمختص بيانات الأعمال الاستمرار في مشاركة البيانات في حالة عدم استيفاء مبدأ واحد أو أكثر من مبادئ مشاركة البيانات. كما يجب على مختص بيانات الأعمال أن يرد الطلب إلى مقدم الطلب مع الملاحظات وإتاحة الفرصة لتلبية جميع مبادئ مشاركة البيانات غير المتوافقة.

6.عند استيفاء جميع مبادئ مشاركة البيانات، يقوم مختص بيانات الأعمال بالحصول على موافقة ممثل بيانات الأعمال على استكمال عملية مشاركة البيانات.

7.يقوم مختص بيانات الأعمال بتحديد الضوابط المناسبة لضمان الالتزام بمبادئ مشاركة البيانات وتحقيق الأهداف المحددة لكل منها، كما يجب أن يتم الاتفاق بين مختص بيانات الأعمال ومقدم الطلب والأطراف الأخرى المشاركة في عملية المشاركة على تطبيق هذه الضوابط.

8.بعد الاتفاق على ضوابط مشاركة البيانات والالتزام بتطبيقها، ينبغي لمختص بيانات الأعمال توضيحها بالتفصيل في الاتفاقية. ويجب على جميع الأطراف المُشارِكة في عملية المشاركة التوقيع على اتفاقية مشاركة البيانات.

9.يمكن لعمادة تقنية المعلومات مشاركة البيانات المطلوبة مع الجهة الطالبة بعد توقيع اتفاقية مشاركة البيانات.

رابعاً: الإطار الزمني لعملية مشاركة البيانات

تقوم عمادة تقنية المعلومات - المطلوب منها مشاركة البيانات - بتقييم الطلب خلال فترة زمنية لا تتجاوز (30) يوماً من تاريخ استلام الطلب، وإشعار مقدم الطلب بقرار المشاركة على أن يكون القرار مكتوباً ومسبّباً (الخطوات من 2 إلى 4 من عملية مشاركة البيانات الموضحة أعلاه).وفي حال عدم الموافقة على طلب المشاركة، فيحق لمقدم الطلب استكمال المتطلبات لاستيفاء جميع المبادئ وطلب الاستئناف من مختص بيانات الأعمال لإعادة تقييم الطلب وإصدار قرار المشاركة خلال فترة زمنية لا تتجاوز (14) يوماً من تاريخ استلامه (الخطوة 5 من عملية مشاركة البيانات)بعد الحصول على موافقة ممثل بيانات الأعمال على الاستمرار في عملية المشاركة (الخطوة 6 من عملية مشاركة البيانات)، يقوم مختص بيانات الأعمال بتطوير وتطبيق الضوابط المناسبة لمشاركة البيانات وإعداد اتفاقية مشاركة بيانات خلال فترة زمنية لا تتجاوز (60) يوماً من تاريخ موافقة ممثل بيانات الأعمال (الخطوة 7 من عملية مشاركة البيانات).بعد توقيع اتفاقية مشاركة البيانات (الخطوة 8

من عملية مشاركة البيانات)، يقوم مختص بيانات الأعمال بمشاركة البيانات مع مقدم الطلب خلال (7) أيام من تاريخ توقيع الاتفاقية (الخطوة 9 من عملية مشاركة البيانات).

خامساً: ضوابط مشاركة البيانات

يجب على جميع الأطراف المشاركة في عملية مشاركة البيانات الموافقة على الضوابط اللازمة لإدارة البيانات المشتركة وحمايتها (الصادرة من مكتب إدارة البيانات الوطنية) بشكل مناسب.

الأساس النظامي:

(المبادئ ذات العلاقة، هي: المبدأ الأول: تعزيز ثقافة المشاركة، والمبدأ الثاني: مشروعية الغرض، والمبدأ الخامس: المسؤولية المشتركة، والمبدأ السابع: الاستخدام الأخلاقي).

- أن يُوضّح الأساس النظامي أو الاحتياج الفعلي لمشاركة البيانات، ومنها على سبيل المثال: تنظيم الجهة، الأمر الملكي/السامي الذي يسمح للجهة بمشاركة البيانات، أو الاتفاقيات الموقعة.

- أن يُلتزم بمستويات تصنيف البيانات، والمحافظة على حقوق الملكية الفكرية وخصوصية البيانات الشخصية.

التفويض:

(المبادئ ذات العلاقة، هي: المبدأ الثالث: الوصول المصرح به، والمبدأ السادس: أمن البيانات).

- أن تُحدد الجهات والأشخاص المخولون بطلب البيانات وتلقيها (يمكن التحقق من الامتثال لسياسة تصنيف البيانات، وضوابط الاستخدام والوصول إلى البيانات).

نوع البيانات:

(المبادئ ذات العلاقة، هي: المبدأ الأول: تعزيز ثقافة المشاركة، والمبدأ الثاني: مشروعية الغرض، والمبدأ الرابع: الشفافية).

•أن يتم التأكد من أن البيانات المطلوبة ضمن البيانات الرئيسية التي تنتجها الجهة لضمان طلب البيانات من مصدرها الصحيح.

•أن تحدد الحد الأدنى من البيانات المطلوبة لتحقيق الأغراض المحددة.

•أن تحدد البيانات المطلوبة وصيغتها والمتطلبات المتعلقة بتعديلها أو تغييرها، (مثل صيغة البيانات، دقة البيانات، مستوى التفاصيل، هيكلة البيانات، نوع البيانات خام أم بيانات مُعالجة).

المعالجة المسبقة للبيانات:

• (المبادئ ذات العلاقة، هو: المبدأ السادس: أمن البيانات).

•أن تُحدد ما إذا كان هناك حاجة لمعالجة البيانات قبل مشاركتها، وفي حال الحاجة لذلك يتم الاتفاق على أساليب المعالجة المطلوبة - على سبيل المثال: الحجب وإخفاء الهوية والتجميع- (على ألا تتم معالجة البيانات بشكل يغير المحتوى).

•أن تُقيّم جودة البيانات المطلوبة وصحتها، وتحديد سلامتها وتحديد ما إذا كانت تتطلب إجراء تحسين قبل مشاركتها، وفي حال الحاجة لذلك يجب على مكتب الجهة تدقيق البيانات قبل مشاركتها.

وسائل مشاركة البيانات:

(المبادئ ذات العلاقة: المبدأ السادس: أمن البيانات).

•الالتزام بضوابط حماية البيانات التي تصدرها الهيئة الوطنية للأمن السيبراني.

•أن يتم تحديد وسائل مشاركة البيانات المادية والرقمية.

•أن يتم التحقق من أمن وموثوقية وسائل المشاركة للتقليل من المخاطر المحتملة، كما يمكن الاستفادة من وسائل المشاركة الآمنة المعتمدة بين الجهات.

•أن يتم تحديد آلية مشاركة البيانات، وما إذا كان مختص بيانات الأعمال سيقوم بنقل البيانات مباشرةً إلى مقدم الطلب أو سيتم الاستعانة بمقدم خدمة لإتمام عملية المشاركة.

•أن يتم تحديد ما إذا كان سيتم استخدام وسائط المشاركة الموجودة، (على سبيل المثال: قناة التكامل الحكومية، شبكة مركز المعلومات الوطني)، أو سيتم استخدام وسائط مختلفة، مثل: (شبكة الإنترنت اللاسلكية، وإمكانية الوصول عن بعد، والشبكة الافتراضية الخاصة، وواجهة برمجة التطبيقات).

•أن يتم الاتفاق على آلية إتلاف الوسائط المادية المستخدمة في مشاركة البيانات.

استخدام البيانات والحفاظ عليها:

(المبادئ ذات العلاقة، هي: المبدأ الثاني: مشروعية الغرض، والمبدأ الرابع: الشفافية، والمبدأ السادس: أمن البيانات، والمبدأ السابع: الاستخدام الأخلاقي).

•أن تُحدد متطلبات حماية البيانات عند مشاركتها، وتطبيق الضوابط المحددة لحماية البيانات بعد مشاركتها.

•أن تُفرض قيود مناسبة على الاستخدام أو المعالجة المسموح بها للبيانات (إن وُجدت)، مثل قيود خاصة بالمعالجة، أو قيود مكانية أو زمانية، أو حقوق حصرية أو تجارية.

•أن يتم تحديد حقوق جميع الأطراف المشاركة في عملية المشاركة بإجراء عمليات التدقيق والمراجعة.

•أن يتم الاتفاق على إجراءات تسوية النزاعات والتحكيم.

•أن تُحدد ما إذا كان هناك طرف ثالث للاستفادة من البيانات بعد مشاركتها والاتفاق على الآلية المنظمة لذلك.

مدة مشاركة البيانات وعدد مرات المشاركة وإلغاء المشاركة:

(المبادئ ذات العلاقة، وهي: المبدأ الثاني: مشروعية الغرض، والمبدأ السادس: أمن البيانات).

•أن تُحدد مدة مشاركة البيانات والموعد النهائي للوصول إلى البيانات أو تخزينها.

•أن تُحدد عدد مرات مشاركة البيانات، والمتطلبات اللازمة للمراجعة، وإجراء التعديلات والإجراءات التي سيتم اتخاذها عند انتهاء الاتفاقية، (مثل إخفاء هوية أصحاب البيانات، أو إلغاء الوصول إلى البيانات أو إتلافها).

•أن تُحدد الأطراف الذين يحق لهم إنهاء مشاركة البيانات قبل التاريخ المتفق عليه، المستند النظامي، وفترة الإشعار المسموح بها.

أحكام المسؤولية:

(المبادئ ذات العلاقة: المبدأ الخامس: المسؤولية المشتركة).

•أن يُتّفق على تحديد المسؤوليات في حال عدم الالتزام ببنود الاتفاقية، وغيرها من الالتزامات التي بين الأطراف المشاركة، كإنهاء الاتفاقية والإجراءات التصحيحية.

•أن تُحدد القواعد المتعلقة بأحكام المسؤولية عند مشاركة بيانات خاطئة، أو وجود مشاكل فنية أثناء عملية نقل البيانات، أو فقدان البيانات بشكل غير مقصود أو غير نظامي، مما قد يتسبب في أضرار أخرى.

القواعد العامة لمشاركة البيانات

فيما يلي بعض القواعد العامة التي يجب على الجهات اتباعها عند مشاركة البيانات:

1.يجب على جميع الجهات إعطاء الأولوية لوسائط المشاركة المعتمدة والآمنة لتبادل البيانات، ومنها على سبيل المثال قناة التكامل الحكومية، وشبكة مركز المعلومات الوطني.

2.يتولى مختص بيانات الأعمال في الجامعة مسؤولية مشاركة البيانات بعد استيفاء جميع مبادئ مشاركة البيانات، بالإضافة إلى تحديد الضوابط المناسبة للمشاركة.

3.يجب على كل جهة تعيين أو تفويض الشخص المناسب - حسب المؤهلات والتدريب المطلوب- للتعامل مع البيانات بطريقة صحيحة، على أن يكون مصرحًا له طلب البيانات المشتركة وتلقيها والوصول إليها وتخزينها وإتلافها.

4.يجب إخفاء هوية أصحاب البيانات الشخصية، إلا إذا كان ذلك ضرورياً لغرض المشاركة مع تحديد الضوابط اللازمة للمحافظة على خصوصية أصحاب البيانات وفقاً لسياسة خصوصية البيانات الشخصية.

5.يجب إرفاق البيانات الوصفية (metadata) عند مشاركة البيانات في الحالات التي تتطلب ذلك.

6.تكون الجهات المشاركة في مشاركة البيانات مسؤولة عن حماية البيانات واستخدامها وفقاً للأغراض المحددة، ويحق لمكتب الجهة مراجعة مدى الالتزام بشكل دوري أو عشوائي بما يتوافق مع الضوابط المحددة في اتفاقية مشاركة البيانات.

7.يقوم المكتب بإعداد الدليل الإرشادي لمشاركة البيانات والمتضمن نموذج طلب مشاركة البيانات ونموذج اتفاقية قياسية لمشاركة البيانات.

8.تقوم الجهات التنظيمية بالجامعة- بعد التنسيق مع مكتب إدارة البيانات الوطنية - بإعداد الآليات والإجراءات والضوابط المتعلقة بتسوية النزاع وفقاً لإطار زمني محدد.

9.في حال وجود نزاع بين الأطراف المشاركة في عملية مشاركة البيانات، يحق للجهات إشعار عمادة تقنية المعلومات والمطالبة بتسوية النزاع بين الأطراف المشاركة.

10. في حال وجود جانب من جوانب مشاركة البيانات لا تشملها سياسة مشاركة البيانات الصادرة من مكتب إدارة البيانات الوطنية، يحق لعمادة تقنية المعلومات في الجامعة وضع قواعد إضافية لا تتعارض مع مبادئ مشاركة البيانات، مع تقديم مسوغ كافٍ وإشعار المكتب بذلك.

11. على الجهات المشاركة في مشاركة البيانات إيجاد التوازن المناسب بين الحاجة إلى مشاركة البيانات وضمان حماية سرية البيانات والمخاطر المحتملة على الفرد أو المجتمع.

12. يجب على الجهات الاحتفاظ بسجلات خاصة بطلبات مشاركة البيانات والقرارات المتعلقة بها.

13.يجب على الجهات تطوير واعتماد ونشر سياسة مشاركة البيانات الخاصة بها وفقاً لهذه السياسة.

14. يجب على الجهات عند استلامها للبيانات المشتركة عدم مشاركتها مع طرف آخر أو جهة أخرى دون موافقة الجهة المنتجة للبيانات.

15. أن تكون الجهة مسؤولة عن مراقبة وتنفيذ هذه السياسة.

الفصل الثالث: سياسة حرية المعلومات

أولاً: النطاق

تنطبق هذه السياسة على جميع طلبات الأفراد للاطلاع أو الحصول على المعلومات العامة - غير المحمية، التي تنتجها الجهات العامة مهما كان مصدرها، أو شكلها أو طبيعتها، ويشمل ذلك السجلات الورقية ورسائل البريد الإلكتروني والمعلومات المخزنة على الكمبيوتر، أو أشرطة الصوت أو الفيديو أو الخرائط أو الصور الفوتوغرافية أو المخطوطات أو الوثائق المكتوبة بخط اليد، أو أي شكل آخر من أشكال المعلومات المسجلة.

لا تنطبق أحكام هذه السياسة على المعلومات المحمية، وهي:

1. المعلومات التي يؤدي إفشاؤها إلى الإضرار بالأمن الوطني للدولة أو سياساتها أو مصالحها أو حقوقها.

2. المعلومات الأمنية.

3. المعلومات والوثائق التي يتم الحصول عليها بمقتضى اتفاق مع دولة أخرى وتصنف على أنها محمية.

4. التحريات والتحقيقات وأعمال الضبط وعمليات التفتيش والمراقبة المتعلقة بجريمة أو مخالفة أو تهديد.

5. المعلومات التي تتضمن توصيات أو اقتراحات أو استشارات من أجل إصدار تشريع أو قرار حكومي لم يصدر بعد.

6. المعلومات ذات الطبيعة التجارية أو الصناعية أو المالية أو الاقتصادية التي يؤدي الإفصاح عنها إلى تحقيق ربح أو تلافي خسارة بطريقة غير مشروعة.

7. الأبحاث العلمية أو التقنية، أو الحقوق المشتملة على حق من حقوق الملكية الفكرية التي يؤدي الكشف عنها إلى المساس بحق معنوي.

8.المعلومات المتعلقة بالمنافسات والعطاءات والمزايدات التي يؤدي الإفصاح عنها إلى الإخلال بعدالة المنافسة.

9.المعلومات التي تكون سرية أو شخصية بموجب نظام آخر، أو تتطلب إجراءات نظامية معينة للوصول إليها أو الحصول عليها.

ثانياً: المبادئ الرئيسة لحرية المعلومات

المبدأ الأول: الشفافية

للفرد الحق في معرفة المعلومات المتعلقة بأنشطة الجهات العامة تعزيزاً لمنظومة النزاهة والشفافية والمساءلة.

المبدأ الثاني: الضرورة والتناسب

إن أي قيود على طلب الاطلاع أو الحصول على المعلومات المحمية التي تتلقاها أو تنتجها أو تتعامل معها الجهات العامة، يجب أن تكون مسوغة بطريقة واضحة وصريحة.

المبدأ الثالث: الأصل في المعلومات العامة الإفصاح

لكل فرد الحق في الاطلاع على المعلومات العامة - غير المحمية - وليس بالضرورة أن يتمتع مقدم الطلب بحيثية معينة أو باهتمام معين بهذه المعلومات ليتمكن من الحصول عليها، كما لا يتعرض لأي مساءلة قانونية متعلقة بهذا الحق.

المبدأ الرابع: المساواة

يتم التعامل مع جميع طلبات الاطلاع أو الحصول على المعلومات العامة على أساس المساواة وعدم التمييز بين الأفراد.

ثالثاً: حقوق الأفراد بما يتعلق بالاطلاع على المعلومات العامة أو الحصول عليها

أولًا: حق الاطلاع والحصول على أي معلومة غير محمية لدى أي جهة عامة.

ثانياً: الحق في معرفة سبب رفض الاطلاع أو الحصول على المعلومات المطلوبة.

ثالثاً: الحق في التظلم على قرار رفض طلب الاطلاع والحصول على المعلومات المطلوبة.

رابعاً: التزامات مكتب إدارة الأعمال وعمادة تقنية المعلومات بالجامعة

1.أن تكون مسؤولة عن إعداد وتطبيق السياسات والإجراءات المتعلقة بممارسة حق الوصول إلى المعلومات العامة أو الحصول عليها، ويكون سعادة رئيس الجامعة مسؤولًا عن الموافقة عليها واعتمادها.

2.أن تقوم بإنشاء وحدة إدارية تكون مرتبطة بمكاتب إدارة البيانات في الجهات الحكومية التي تم تأسيسها بموجب الأمر السامي الكريم رقم 59766 وتاريخ 20/ 11/ 1439هـ، ويسند إليها مسؤولية تطوير وتوثيق ومراقبة تنفيذ السياسات والإجراءات المعتمدة من الإدارة العليا بالجهة والمتعلقة بحق الوصول إلى المعلومات، على أن تتضمن مهام ومسؤوليات الوحدة وضع المعايير المناسبة لتحديد مستويات تصنيف البيانات في حال عدم وجودها- وفقاً لسياسة تصنيف البيانات - واستخدامها كمرجع رئيسي عند معالجة طلبات الاطلاع على المعلومات العامة أو الحصول عليها.

3.أن تقوم بتحديد وتوفير الوسائل الممكنة (نماذج طلب المعلومات العامة)، سواء أكانت نماذج ورقية أو إلكترونية، والتي من خلالها يمكن للفرد طلب الاطلاع على المعلومات العامة أو الحصول عليها.

4.أن تقوم بالتحقق من هوية الأفراد قبل منحهم حق الاطلاع على المعلومات العامة أو الحصول عليها وفقاً للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات العلاقة.

5.أن تقوم بوضع المعايير اللازمة لتحديد الرسوم المترتبة على معالجة طلبات الاطلاع على المعلومات العامة أو الحصول عليها بناءً على طبيعة البيانات وحجمها والجهد المبذول والوقت المستغرق، وفقاً لوثيقة سياسة تحقيق الدخل من البيانات.

6. أن تقوم بتوثيق جميع سجلات طلبات الوصول إلى المعلومات أو الحصول عليها والقرارات المتخذة حيال الطلبات، على أن تتم مراجعة هذه السجلات لمعالجة حالات سوء الاستخدام أو عدم الاستجابة.

7.أن تقوم بإعداد وتوثيق سياسات وإجراءات الاحتفاظ بسجلات الطلبات والتخلص منها وفقاً للأنظمة والتشريعات ذات العلاقة بأعمال وأنشطة الجامعة.

8.أن تقوم بإعداد وتوثيق الإجراءات اللازمة لإدارة ومعالجة وتوثيق طلبات التمديد، والطلبات المرفوضة، وتحديد المهام والمسؤوليات المتعلقة بفريق العمل المختص، والحالات التي يتم بها إشعار الجهة التنظيمية والمكتب حسب التسلسل الإداري وفقاً للفترة الزمنية المحددة لمعالجة الطلبات.

9.أن تقوم بإشعار الفرد - بطريقة ملائمة - في حال تم رفض الطلب كلياً أو جزئياً، مع إيضاح أسباب الرفض والحق في التظلّم وكيفية ممارسة هذا الحق خلال مدة لا تتجاوز (15) يوماً من اتخاذ القرار.

10.أن تقوم بإعداد برامج توعوية لتعزيز ثقافة الشفافية ورفع مستوى الوعي وفقاً لسياسات وإجراءات حرية المعلومات المعتمدة من الإدارة العليا للجامعة.

11. أن تكون مسؤولة عن مراقبة الامتثال لسياسات وإجراءات حرية المعلومات بشكل دوري، ويتم عرضها على سعادة رئيس الجامعة أو من يفوضه، كما يتم تحديد وتوثيق الإجراءات التصحيحية التي سيتم اتخاذها في حال عدم الامتثال وإشعار الجهة التنظيمية والمكتب حسب التسلسل الإداري.

خامساً: الخطوات الرئيسة للاطلاع على المعلومات أو الحصول عليها

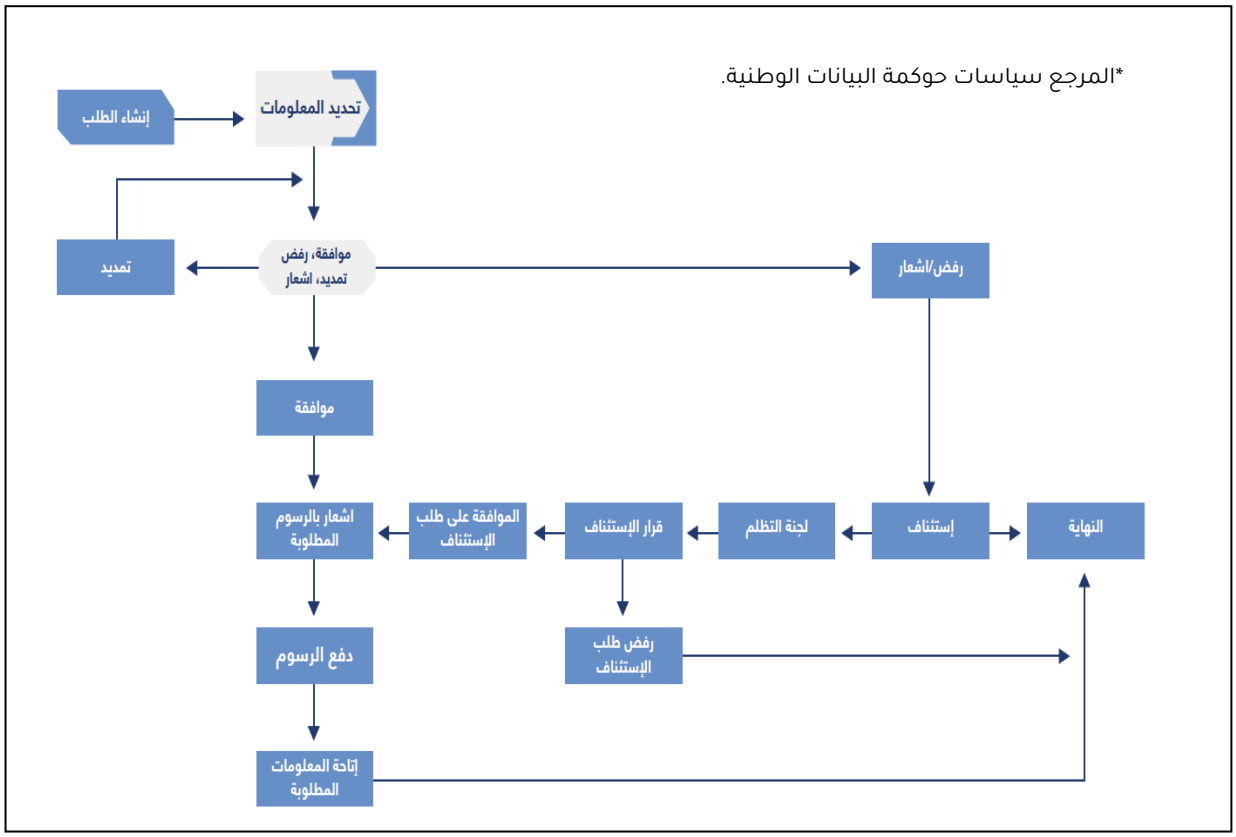
المتطلبات الرئيسية لطلبات الوصول إلى المعلومات العامة أو الحصول عليها:

1.يجب أن يكون الطلب خطياً أو إلكترونياً.

2.يجب تعبئة "نموذج طلب معلومات عامة" المعتمد من قبل الجامعة.

3.يجب أن يكون الطلب لأغراض الوصول إلى المعلومات العامة أو الحصول عليها.

4.يجب أن يتضمن نموذج الطلب تفاصيل حول كيفية إرسال القرار النهائي والإشعارات إلى الفرد (العنوان الوطني أو البريد الإلكتروني أو موقع الجهة... إلخ).



5.يجب إرسال نموذج الطلب مباشرة إلى الجهة العامة.

الخطوات الرئيسة لطلب الاطلاع أو الحصول على المعلومات العامة:

أولًا: يتم تقديم الطلبات عن طريق ملء "نموذج طلب معلومات عامة" - إلكترونيًا أو ورقيًا -وتقديمه للجهة التي لديها المعلومات.

ثانياً: تقوم الجهة، في فترة زمنية محددة (30 يوماً) باستلام طلب الاطلاع أو الحصول على المعلومات العامة، باتخاذ أحد القرارات التالية:

1.الموافقة: في حال تمت موافقة الجهة على طلب الوصول إلى المعلومات أو الحصول عليها كليًا أو جزئيًا، فيجب إشعار الفرد خطياً أو إلكترونياً بالرسوم المطبقة، ويجب على الجهة إتاحة هذه المعلومات للفرد خلال فترة زمنية لا تتجاوز (10) أيام عمل من استلام المبلغ.

2.الرفض: في حال تم رفض طلب الوصول إلى المعلومات أو الحصول عليها، فيجب أن يكون الرفض خطياً أو إلكترونياً على أن يتضمن المعلومات التالية:

- تحديد ما إذا كان رفض الطلب كليًا أو جزئيًا.
- أسباب الرفض، إن أمكن.
- الحق في التظلّم على هذا الرفض وكيفية ممارسة هذا الحق.

3.التمديد: في حال عدم إمكانية معالجة طلب الوصول إلى المعلومات في الوقت المحدد، ينبغي للجهة تمديد الفترة التي سيتم الرد فيها بمدة معقولة حسب حجم وطبيعة المعلومات المطلوبة - على سبيل المثال لا تتجاوز (30) يوماً إضافية - وتزويد الفرد بالمعلومات التالية:

- إشعار التمديد والتاريخ المتوقع فيه إكمال الطلب.
- أسباب التأخير.
- الحق في التظلّم على هذا التمديد وكيفية ممارسة هذا الحق.

4.الإشعار: في حال كانت المعلومات المطلوبة متاحة على موقع الجامعة، أو ليست من اختصاصها، فيجب إشعار الفرد بذلك خطياً أو إلكترونياً، على أن يتضمن المعلومات التالية:

- نوع الإشعار، على سبيل المثال، البيانات المطلوبة متاحة على موقع الجامعة، أو ليست من اختصاصها.
- الحق في التظلّم على هذا الإشعار وكيفية ممارسة هذا الحق.

ثالثاً: في حالة رغبة الفرد في التظلّم على رفض الطلب، فيمكنه تقديم إشعار خطي أو إلكتروني بالتظلم في فترة زمنية لا تتجاوز (10) أيام عمل من استلامه لقرار الرفض، وتقوم لجنة التظلم بمراجعة الطلب واتخاذ القرار المناسب وإشعار الفرد برسوم المراجعة - يتم استرجاعها في حال موافقة اللجنة على الطلب - وقرار الاستئناف.

سادساً: أحكام عامة

أولًا: يجب على الجهات موازنة حق الاطلاع والحصول على المعلومات مع المتطلبات الضرورية الأخرى، كتحقيق الأمن الوطني والمحافظة على خصوصية البيانات الشخصية.

ثانياً: يجب على الجهات الامتثال لهذه السياسة وتوثيق الامتثال بشكل دوري وفقاً للآليات والإجراءات التي تحددها هذه الجهات بعد التنسيق مع مكتب إدارة البيانات الوطنية.

ثالثاً: تقوم الجهات التنظيمية بالجامعة - بعد التنسيق مع مكتب إدارة البيانات الوطنية - بإعداد الآليات والإجراءات والضوابط المتعلقة بمعالجة الشكاوى وفقاً لإطار زمني محدد وحسب التسلسل التنظيمي.

رابعاً: يجب على مكتب إدارة الأعمال وعمادة تقنية المعلومات إشعار مكتب إدارة البيانات الوطنية في حال تم رفض طلب الاطلاع أو الحصول على المعلومات العامة أو تمديد الفترة المحددة لتقديم هذه المعلومات وهي ضمن النطاق.

خامساً: يجب على الجامعة عند تعاقدها مع جهات أخرى، كالشركات التي تقوم بمباشرة خدمات عامة، أن تتحقق بشكل دوري من امتثال الجهات الأخرى لهذه السياسة وفقاً للآليات والإجراءات التي تحددها الجامعة، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها.

سادساً: يحق للجامعة وضع قواعد إضافية لمعالجة الطلبات المتعلقة بأنواع محددة من المعلومات العامة وفقاً لطبيعتها وحساسيتها بعد التنسيق مع مكتب إدارة البيانات الوطنية.

سابعاً: يجب على عمادة تقنية المعلومات بالجامعة إعداد نماذج للاطلاع أو الحصول على المعلومات العامة، سواء أكانت ورقية أو إلكترونية، تحدد فيها المعلومات اللازمة والوسائل الممكنة لتقديم المعلومات المطلوبة.

سابعاً: حرية المعلومات والبيانات المفتوحة

عادةً ما يتم إعداد وتطوير برامج وسياسات البيانات المفتوحة حول العالم لدعم نمو أجندة الاقتصاد الوطني والابتكار، ومما لا شك فيه أن إتاحة ونشر مجموعة محددة من المعلومات العامة للباحثين وروّاد الأعمال والمبتكرين والشركات الناشئة يساعد على تهيئة بيئة مواتية لنمو الأعمال التجارية، ويشير إلى وجود حكومة منفتحة وشفافة.

كما تعد برامج وسياسات البيانات المفتوحة خطوة استباقية من الجهات في المحافظة على حق الوصول إلى المعلومات العامة من خلال إتاحة أو نشر مجموعة محددة من المعلومات - كبيانات مفتوحة - قبل طلب الوصول إليها أو الحصول عليها، وبالتالي فإن برامج وسياسات البيانات المفتوحة الفعّالة تقلل من حجم طلبات الوصول إلى المعلومات العامة مما يؤدي إلى خفض النفقات الحكومية المتعلقة بمعالجة الطلبات.

الفصل الرابع: القواعد العامة لنقل المعلومات الشخصية خارج الحدود الجغرافية للمملكة

تسعى المملكة إلى وضع السياسات والمعايير الخاصة بنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة بما يضمن المحافظة على السيادة الوطنية على هذه البيانات، وكذلك المحافظة على خصوصية أصحاب البيانات الشخصية وحماية حقوقهم من خلال تحديد التزامات جهات التحكم والمعالجة حيال عمليات نقل البيانات الشخصية خارج الحدود الجغرافية، وتوفير الوسائل المناسبة التي تمكّن أصحاب البيانات من ممارسة حقوقهم، وتحديد أدوار ومسؤوليات هذه الجهات، بالإضافة إلى الجهات التنظيمية والجهات الإشرافية على تطبيق أحكام هذه السياسات.

أولاً: النطاق

تنطبق أحكام هذه الوثيقة على جميع الجهات بالجامعة المشمولة بنطاق تطبيق سياسة حماية البيانات الشخصية، والتي تقوم بنقل البيانات الشخصية إلى جهات أخرى خارج الحدود الجغرافية للمملكة بغرض معالجتها، ويستثنى من ذلك نقل البيانات الشخصية من وإلى الأفراد مباشرة.

ثانياً: حقوق أصحاب البيانات

إشارةً إلى سياسة حماية البيانات الشخصية، فإن المبادئ الأساسية للحماية تمنح الأفراد حقوقاً محددة فيما يتعلق بمعالجة بياناتهم الشخصية، بينما تحدد التزامات جهات التحكم القواعد العامة التي يجب الالتزام بها عند معالجتها. وفيما يتعلق بنقل البيانات الشخصية عبر الحدود، فإن لصاحب البيانات نفس الحقوق الموضحة في سياسة حماية البيانات الشخصية، مع التأكيد على الحقوق التالية:

أولًا: الحق في العلم، ويشمل ذلك إشعاره بالأساس النظامي أو الاحتياج الفعلي لنقل بياناته الشخصية خارج الحدود الجغرافية للمملكة ومكان تخزينها أو استضافتها، والجهات التي سيتم الإفصاح لها عن بياناته الشخصية عند

نقلها، والغرض من هذا النقل، وأخذ موافقته على ذلك، والتدابير الأمنية المتخذة لحماية بياناته الشخصية في أثناء النقل وبعده.

ثانياً: الحق في الرجوع عن موافقته على معالجة بياناته الشخصية خارج الحدود - في أي وقت -، ما لم يكن الغرض من نقل البيانات تحقيقاً للمصلحة العامة، أو حمايةً للمصالح الحيوية للأفراد، أو تنفيذاً لمتطلبات نظامية.

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

ثالثاً: القواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة

التزامات الجامعة: الأصل في المعالجة أن تكون داخل الحدود الجغرافية للمملكة، حيث تقوم الجهة بتخزين البيانات الشخصية ومعالجتها داخل المملكة لضمان المحافظة على السيادة الوطنية على هذه البيانات وحماية خصوصية أصحابها، ولا يجوز نقلها أو معالجتها خارج المملكة إلا بعد التحقق من الحالات الموضحة أدناه حسب التسلسل التالي:

1. إذا كانت جهة المعالجة الخارجية المسند إليها أنشطة معالجة البيانات الشخصية في دولة ضمن قائمة الاعتماد، فتقوم عمادة تقنية المعلومات باعتبارها جهة المعالجة الداخلية بأخذ موافقة كتابية من الجامعة على نقل البيانات، وعلى العمادة التنسيق مع مكتب إدارة البيانات الوطنية.

2. إذا كانت جهة المعالجة الخارجية في دولة ليست ضمن قائمة الاعتماد، فإن نقل البيانات الشخصية خارج الحدود الجغرافية للمملكة يتطلب مستوى كافيًا من الحماية - لا يقل عن مستوى الحماية الذي كفلته سياسة حماية البيانات الشخصية الصادرة من المكتب، بعد إجراء تقييم مستوى الحماية التي توفرها جهة المعالجة الخارجية.

3.إذا لم يكن هناك مستوى كافٍ من الحماية، فتقوم الجهة بوضع ضمانات مناسبة لحماية حقوق أصحاب البيانات، ومنها على سبيل المثال، استخدام البنود القياسية، أو القواعد الملزمة.

4.إذا لم تتمكن الجهة من توفير الضمانات الكافية، فيمكن الاعتماد على أحد الاستثناءات النظامية التي تتطلب نقل البيانات والموضحة في البند (ثالثاً) أدناه.

في جميع الحالات الواردة في الفقرات (2) و (3) و(4) أعلاه، يجب على مكتب إدارة الأعمال باعتباره جهة التحكم أو المعالجة الداخلية الحصول على موافقة كتابية من عمادة تقنية المعلومات باعتبارها الجهة التنظيمية على نقل البيانات، وعلى العمادة التنسيق مع مكتب إدارة البيانات الوطنية.

أولًا: تقييم مستوى الحماية

يجب أن تقوم الجامعة قبل نقل البيانات خارج الحدود الوطنية بإجراء تقييم الآثار والمخاطر المحتملة في - كل حالة على حدة؛ لتحديد ما إذا كانت جهة التحكم/جهة المعالجة الخارجية ستوفر مستوى كافيًا من الحماية لحقوق أصحاب البيانات وعرض نتائج التقييم على (سعادة رئيس الجامعة)؛ لتحديد مستوى قبول المخاطر وإقرارها. وللقيام بذلك يجب أن تقوم الجامعة بالالتزام بمعايير التقييم الصادرة من مكتب إدارة البيانات الوطنية سواء المعايير العامة أو القانونية، وذلك لضمان أن يكون مستوى الحماية ملائماً في جميع الظروف.:

أ- معايير التقييم العامة

- طبيعة وحساسية البيانات: يجب على الجامعة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار نوع وقيمة وحجم البيانات المراد نقلها ودرجة حساسيتها، حيث إن نقل البيانات الشخصية الحساسة يتطلب مستوى عاليًا من الحماية.

-الغرض من معالجة البيانات: يجب على الجامعة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار الغرض من المعالجة والفئة المستهدفة من أصحاب البيانات ونطاق المعالجة والجهات التي ستتم مشاركة البيانات معها، حيث إن معالجة بيانات شخصية حساسة على نطاق واسع يتطلب مستوى عاليًا من الحماية.

-الفترة التي يتم خلالها معالجة البيانات: يجب على الجامعة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار ما إذا كانت المعالجة ستتم بشكل مقيّد أو عرضي - لمرة واحدة فقط أو لفترة محدودة -، أو ستتم بشكل متكرر ومنتظم، حيث إن البيانات الشخصية التي ستتم معالجتها بشكل منتظم وعلى المدى الطويل تتطلب مستوى عاليًا من الحماية.

- منشأ البيانات: يجب على الجامعة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار الدولة التي جُمعت منها البيانات، وليست بالضرورة الدولة التي سيتم نقل البيانات منها؛ وذلك لتحديد توقعات أصحاب البيانات فيما يتعلق بمستوى الحماية، حيث إن نقل البيانات الشخصية التي تم جمعها من دول تخضع لمستوى حماية عالٍ جداً يتطلب مستوى لا يقل عن مستوى الحماية في هذه الدول.

- الوجهة النهائية للبيانات: يجب على الجامعة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار المراحل التي يتم بها نقل البيانات الشخصية - والتي قد تمر بأكثر من دولة أحياناً-، وتقييم مستوى الحماية في الدولة التي تعد هي الوجهة النهائية - وآخر مرحلة من مراحل النقل.

- الضوابط الأمنية: يجب على الجامعة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار الإجراءات الإدارية والتدابير التقنية والضوابط المادية المعتمدة في سياسات الجهة لأمن المعلومات، كالتشفير والضوابط الأمنية والمعايير الدولية، إذا أظهرت نتائج تقييم مستوى الحماية - بناءً على المعايير العامة - أنه بالظروف الخاصة للحالة تكون الآثار السلبية على حقوق أصحاب البيانات

محدودة والمخاطر المحتملة منخفضة، فقد لا يكون تقييم مستوى الحماية - بناءً على المعايير القانونية - ضرورياً في هذه الحالة.

ب- معايير التقييم القانونية:

يجب أن تقوم الجامعة عند الرغبة بنقل البيانات خارج الحدود الوطنية بمراعاة هذه المعايير عندما تكون نتائج تقييم الآثار والمخاطر المحتملة في الفقرة (أ) أعلاه غير كافية، ومن هذه الحالات على سبيل المثال، أن يتم نقل بيانات شخصية حساسة بشكل دائم ومنتظم وعلى نطاق واسع.

- الأنظمة والتشريعات النافذة: يجب على الجامعة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار ما إذا كان في الدولة - المراد نقل البيانات لها - أنظمة وتشريعات تحمي حقوق أصحاب البيانات فيما يتعلق بمعالجة بياناتهم الشخصية، وتضمن قدرة الأطراف المشاركة على التعاقد والالتزام بموجب هذه العقود.

- الالتزامات الدولية: يجب على الجامعة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار ما إذا كانت الدولة - المراد نقل البيانات لها - طرفاً في اتفاقيات دولية، أو تتبنى مبادئ ومعايير دولية لحماية البيانات الشخصية.

- القواعد والممارسات المعتمدة: يجب على الجامعة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار ما إذا كانت الدولة - المراد نقل البيانات لها - تعتمد قواعد سلوكية أو ممارسات عامة، أو معايير خاصة لحماية البيانات الشخصية.

ثانياً: الضمانات المناسبة

إذا كانت الجهة في دولة ليست من ضمن قائمة الاعتماد ولم تخضع لتقييم مستوى الحماية، أو كان مستوى الحماية غير كافٍ، فيجب عليها توفير الضمانات المناسبة لحماية البيانات الشخصية، ومنها ما ذكره مكتب إدارة البيانات الوطنية:

- البنود التعاقدية القياسية: يجب على الجهة أن تضمّن في العقود والاتفاقيات بنوداً نموذجية أو قياسية - يتم الموافقة عليها من قبل المكتب -؛ لتقييد نقل البيانات الشخصية خارج الحدود الجغرافية للمملكة بما يضمن المحافظة على خصوصية أصحابها وحماية حقوقهم.

- القواعد المشتركة الملزمة: يجب على جهة التحكم وجهة المعالجة - كل على حدة -اللتين تعملان ضمن مجموعة متعددة الجنسيات أن تقوما بإعداد قواعد مشتركة داخلية ملزمة قانونياً تنطبق على عمليات نقل البيانات الشخصية خارج الحدود، بما في ذلك معالجة انتهاكات الخصوصية والإشعار عنها، على أن تتم الموافقة عليها من قبل المكتب، ويتم تضمين هذه القواعد المشتركة بصفتها ملحقاً لاتفاقيات مستوى الخدمة أو العقود المبرمة بين الجهتين. كما يجب على جهة التحكم أخذ موافقة الجهة التنظيمية عند وجود أي التزام قانوني تخضع له هذه الجهة أو إحدى الجهات التابعة لها في دولة أخرى يرجّح أن يكون له أثر سلبي على الضمانات التي توفرها القواعد المشتركة الملزمة.

- قواعد السلوك المعتمدة: أن تقوم الجهات باستخدام قواعد السلوك المعتمدة من الجهات التنظيمية أو المكتب بصفتها أداة فعّالة تحدّد الالتزامات على جهات التحكم والمعالجة، لضمان المحافظة على خصوصية أصحاب البيانات وحماية حقوقهم.

- الشهادات المعتمدة: أن تقوم الجهات بالاستعانة بأطراف خارجية مستقلة تتولى إصدار شهادات اعتماد تؤكد وجود الضمانات المناسبة التي توفرها جهات التحكم أو جهات المعالجة الخارجية. كما تقوم هذه الجهات بتقديم التزامات قابلة للتنفيذ لتطبيق هذه الضمانات، بما في ذلك الأحكام المتعلقة بحقوق أصحاب البيانات.

- الاتفاقيات الملزمة بين الجهات العامة: أن تقوم الجهات العامة - سواء أكانت جهات التحكم أو جهات المعالجة - بتوقيع اتفاقية ملزمة قانونياً لنقل البيانات الشخصية، على أن تتضمن هذه الاتفاقية بنوداً تعاقدية ملزمة تضمن المحافظة على خصوصية أصحاب البيانات وتحمي حقوقهم.

ثالثاً: الاستثناءات لحالات محددة

ذكر مكتب إدارة البيانات الوطنية بأنه يمكن للجهات نقل البيانات الشخصية خارج الحدود الجغرافية دون الالتزام بالشروط والأحكام الموضحة في البند (أولًا)والبند (ثانياً) أعلاه في حالات محددة، ومنها أن يكون نقل البيانات خارج الحدود الجغرافية للمملكة:

1.استنادًا على موافقة أصحاب البيانات.

2.تنفيذاً لالتزام تعاقدي ويكون صاحب البيانات طرفاً فيه.

3.تنفيذاً لمتطلبات قضائية.

4.تنفيذاً لأحكام نظام آخر، أو اتفاقية دولية تكون المملكة طرفاً فيها.

5.للمحافظة على المصلحة العامة بما في ذلك حماية الصحة أو السلامة العامة.

6.لحماية المصالح الحيوية لأصحاب البيانات.

في جميع هذه الحالات الواردة في الفقرات السابقة من (1-5)، يجب على جهة التحكم أو المعالجة الداخلية الحصول على موافقة كتابية من الجهة التنظيمية على نقل البيانات - كل حالة على حدة - وعلى الجهة التنظيمية التنسيق مع المكتب. أما ما يتعلق بالحالة الواردة في الفقرة (6)فيجب على جهة التحكم أو جهة المعالجة إشعار الجهة التنظيمية فقط، وعلى الجهة التنظيمية إشعار المكتب بذلك.

رابعاً: أحكام عامة

أولًا: تتولى عمادة تقنية المعلومات باعتبارها الجهة التنظيمية بالجامعة بمواءمة هذه الوثيقة مع وثائقها التنظيمية وتعميمها على جميع الجهات التابعة للجامعة أو المرتبطة بها، بما يحقق التكامل ويضمن تحقيق الهدف المنشود من إعداد هذه القواعد.

ثانياً: تقوم عمادة تقنية المعلومات بمراقبة امتثال الجهات التابعة للجامعة أو المرتبطة بها لهذه القواعد بشكل دوري.

ثالثاً: يجب على جهات التحكم وجهات المعالجة الامتثال لهذه القواعد وتوثيق الامتثال وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية.

رابعاً: يجب على جهات التحكم عند تعاقدها مع جهات المعالجة - داخل أو خارج المملكة - أن تتحقق بشكل دوري من امتثال جهات المعالجة لهذه القواعد وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها جهات المعالجة.

خامساً: يحق للجامعة وضع قواعد إضافية لنقل أنواع محددة من البيانات الشخصية وفقاً لطبيعة وحساسية هذه البيانات بعد التنسيق مع المكتب.

سادساً: يقوم مكتب إدارة البيانات الوطنية بمراجعة معايير التقييم - العامة والقانونية - المتعلقة بحماية البيانات الشخصية عند نقلها خارج الحدود الجغرافية للمملكة واتخاذ القرارات المنظمة لها.

سابعاً: تقوم الجامعة بإعداد قائمة الاعتماد ومراجعتها ونشرها وتحديثها بشكل دوري، وذلك بناءً على ما يصدر من معلومات من مكتب إدارة البيانات الوطنية، خاصة فيما يتعلق بمستوى الحماية المناسب بحيث لا يقل عن مستوى الحماية الذي كفلته سياسة حماية البيانات الشخصية الصادرة من المكتب.

الفصل الخامس: القواعد العامة لحوكمة البيانات عند تطوير أو استخدام أنظمة الذكاء الاصطناعي

تتضمن المبادئ الأساسية والقواعد العامة والممارسات الأخلاقية التي يجب مراعاتها أثناء استخدام أنظمة الذكاء الاصطناعي وتطويرها، للحد من المخاطر والآثار السلبية المحتملة وضمان الاستخدام بشكل مسؤول.

أولاً: النطاق

تنطبق أحكام هذه الوثيقة على جميع الجهات في الجامعة، التي تقوم -بأي وسيلة كانت- بجمع البيانات، بما في ذلك البيانات الشخصية والبيانات بعد التعتيم (Data Masking) أو المزج (Data Scrambling) أو التعمية، (Data Anonymisation) وتحليلها باستخدام أنظمة الذكاء الاصطناعي لتحقيق أهداف محددة.

ثانياً: المبادئ الأساسية لتطوير واستخدام أنظمة الذكاء الاصطناعي

المبدأ الأول: العدالة

أن يتم اختيار عينة البيانات وكذلك البيانات المراد تحليلها بشكل عادل وموضوعي دون أي تحيز أو تمييز بأي شكل من الأشكال، سواء أكان تمييزاً عنصرياً أو عرقياً أو مناطقياً أو فكرياً ... إلخ.

المبدأ الثاني: الشفافية

أن يتم بناء أنظمة الذكاء الاصطناعي والنماذج التنبؤية بدرجة عالية من الشفافية والوضوح وبطريقة قابلة للشرح والتفسير، مع توفير إمكانية تتبع مراحل اتخاذ القرارات المهمة التي تمت بشكل آليّ، والتي قد تؤدي إلى أضرار مادية أو معنوية على صاحب البيانات.

المبدأ الثالث: المساءلة/ المسؤولية

أن تكون أنظمة الذكاء الاصطناعي والنماذج التنبؤية خاضعة للمساءلة، وذلك بإجراء تقييم الآثارالسلبية والمخاطر المحتملة عند تطويرها أو استخدامها

بشكل غير مسؤول، مع توفير إمكانية الاعتراض على القرارات المهمة التي تتعلق بمصالح الأفراد.

المبدأ الرابع: الشمولية

أن تكون عينة البيانات والبيانات المراد تحليلها شاملة ومتنوعة وتمثل جميع شرائح المجتمع أو الفئات المستهدفة بشكل عادل دون أي تحيز أو تمييز.

المبدأ الخامس: الإنسانية

أن يتم بناء النماذج التنبؤية عن طريق منهجية أخلاقية آمنة قائمة على الحقوق والقيم الإنسانية؛ لضمان استخدام أنظمة الذكاء الاصطناعي لما فيه خير البشرية.

المبدأ السادس: الأمان

أن يتم بناء أنظمة الذكاء الاصطناعي بطريقة آمنة تحد من تحكم وسيطرة الآلة، مع توفير إمكانية التحكم بها طوال فترة حياتها بما يضمن عدم تمكينها من إلحاق أي ضرر أو أذى.

المبدأ السابع: جودة البيانات

أن تكون عينة البيانات أو البيانات المراد تحليلها دقيقة وصحيحة ومكتملة وذات علاقة بالغرض من استخدامها، مع ضمان تحديثها بشكل مستمر والتأكد من صحتها وموثوقية مصادرها.

ثالثاً: حقوق أصحاب البيانات

لصاحب البيانات الشخصية الحقوق المنصوص عليها في سياسة حماية البيانات الشخصية، بالإضافة إلى الحقوق المتعلقة باتخاذ القرارات بالوسائل الآلية دون تدخّل بشري، (Automated Decisions)بما في ذلك التنميط/ تحليل الخصائص النفسية والسلوكية للأفراد أو تقييم بعض الجوانب الشخصية (Profiling)، والتي قد يترتب عليها:

1.تبعات نظامية تتمثل في قيام الجهات المختصة باتخاذ الإجراءات اللازمة في حقه، ومن ذلك استدعاؤه وسماع أقواله وطلب التحقق من معلوماته وغيرها من الإجراءات.

2.أضرار مادية أو معنوية تتمثل في زوال منفعة أو إساءة سمعة ونحوها من الأضرار الأخرى.

وبناءً على ذلك، لصاحب البيانات الشخصية الحق في عدم اتخاذ قرارات عنه بشكل آلي إلّا في الحالات التالية، مع توفير إمكانية تتبع مراحل اتخاذ القرارات المهمة:

1. إذا كان ذلك ضرورياً لإبرام عقد أو تنفيذ التزام تعاقدي يكون صاحب البيانات الشخصية طرفاً فيه.
2. إذا كان ذلك تنفيذاً لمتطلبات نظامية وفقاً للأنظمة واللوائح المعمول بها، أو مصرحًا به من قبل المكتب بعد اعتماد الضوابط والإجراءات اللازمة لضمان حقوق صاحب البيانات والمصالح المشروعة للجهة.
3. إذا كان ذلك بناءً على موافقة صريحة من قبل صاحب البيانات.

وفي الحالتين المشار إليها في الفقرتين (1) و (3)، يحق لصاحب البيانات الحصول على تدخل بشري (Intervention)من قبل الجهة للتعبير عن وجهة نظره أو الاعتراض على النتائج والقرارات.

رابعاً: القواعد العامة لاستخدام تطبيقات الذكاء الاصطناعي وتطويرها

أولًا: الالتزامات الخاصة بمطوري أنظمة الذكاء الاصطناعي

1.اتخاذ الإجراءات اللازمة والخطوات الكافية لضمان عدم التحيّز أثناء اختيار عينة البيانات، بما في ذلك التحيز للأغلبية ضد الأقليات.

2.اتخاذ الإجراءات اللازمة والخطوات الكافية لضمان تنوع عينة البيانات وتمثيلها لجميع شرائح المجتمع أو الفئات المستهدفة بشكل عادل دون أي تمييز.

3.إجراء تقييم الانحياز وتوثيق النتائج واعتمادها من المسؤول الأول في الجهة أو من يفوضه قبل البدء بتطوير النماذج التنبؤية المبنية على البيانات وخوارزميات الذكاء الاصطناعي.

4.عدم استخدام البيانات الشخصية الحسّاسة بصفتها عينة بيانات أثناء مرحلة تدريب أنظمة الذكاء الاصطناعي وتطويرها أو النماذج التنبؤية.

5.عدم استخدام البيانات الشخصية التي تؤدي إلى معرفة الفرد على وجه التحديد بدون أساس نظامي، سواء موافقة صاحب البيانات أو غيرها من الأسس النظامية المنصوص عليها في سياسة حماية البيانات الشخصية، على أن يتم إيضاح الأغراض الرئيسة لجمع هذه البيانات وتحليلها.

6.إجراء تقييم أثر الخصوصية لتقييم الآثار النفسية والاجتماعية عند استخدام البيانات الشخصية بصفتها عينة بيانات؛ لضمان المحافظة على خصوصية أصحابها وحماية حقوقهم.

7.الالتزام بمبدأ الشفافية عند بناء النماذج التنبؤية المبنية على البيانات وخوارزميات الذكاء الاصطناعي؛ وذلك عن طريق شرح آلية عمل الخوارزميات المستخدمة بطريقة قابلة للفهم والتفسير تساعد على معرفة أسباب وصول هذه النماذج إلى نتائج معينة، بما لا يتعارض مع أنظمة الملكية الفكرية أو الأنظمة الأخرى ذات الصلة.

8.اتخاذ الإجراءات اللازمة والخطوات الكافية للتحقق من صحة تفسير النتائج بشكل دقيق وغير متعارض، وذلك لتفادي القياسات المضللة.

9.إثبات عدالة القرارات المهمة، وذلك بتوفير إمكانية التحقق من العوامل الرئيسة التي تؤدي إلى اتخاذ أي قرار يمكن أن يؤثر على المصالح الحيوية للأفراد.

10. توفير آلية للتدخل اليدوي تتيح للأفراد إمكانية تتبع مراحل اتخاذ القرارات المهمة المتعلقة بمصالحهم الحيوية والاعتراض عليها.

11. إعداد آلية تتضمن مجموعة من المعايير اللازمة لتقييم مدى الاعتمادية على أنظمة الذكاء الاصطناعي في التنبؤ واتخاذ القرارات المستقبلية.

12. تبني منهجية شاملة لاختبار جودة الأنظمة والنماذج التنبؤية المبنية على البيانات وخوارزميات الذكاء الاصطناعي وفقاً للممارسات القياسية.

13.اتخاذ الإجراءات اللازمة والخطوات الكافية لضمان جودة عينة البيانات ودقتها وصحتها وعلاقتها بالغرض من بناء النماذج التنبؤية وأنظمة الذكاء الاصطناعي.

ثانياً: الالتزامات الخاصة بمستخدمي أنظمة الذكاء الاصطناعي

1.إعداد السياسات والإرشادات المتعلقة بدعم الاستخدام الأخلاقي للذكاء الاصطناعي وتمكينه وفقاً لأفضل الممارسات القياسية.

2.الالتزام بسياسات حوكمة البيانات الوطنية الصادرة من المكتب والمعتمدة من مجلس إدارة الهيئة السعودية للبيانات والذكاء الاصطناعي.

3.أخذ موافقة المكتب - بعد التنسيق مع الجهة التنظيمية- قبل تحليل البيانات المصنفة على إحدى درجات السرية وفقاً لسياسة تصنيف البيانات.

4.أن يقتصر تحليل البيانات على مستويات التصنيف (مقيّد، عام) على أن يتم تحديد ما إذا كانت هناك حاجة لمعالجة البيانات قبل تحليلها، ومنها على سبيل المثال لا الحصر: الحجب وإخفاء الهوية والتجميع.

5.اتخاذ الإجراءات اللازمة والخطوات الكافية لضمان جودة البيانات المراد تحليلها ودقتها وصحتها وموثوقية مصادرها ومناسبة طرق جمعها وخلوها من أساليب الخداع أو التضليل.

6.توفير قنوات مناسبة تمكّن الأفراد من الحصول على التفسيرات المتعلقة بالنتائج والقرارات المهمة التي تمس مصالحهم الحيوية، وتمكينهم من الاعتراض على هذه القرارات أو طلب إثبات عدالتها.

7.إعداد الأدلة الاسترشادية المتعلقة بإيضاح آلية عمل النماذج التنبؤية أو خوارزميات الذكاء الاصطناعي المستخدمة، والبيانات المراد تحليلها والفئات المستهدفة والعوامل التي تؤثر في النتائج والقرارات المهمة.

8.إعداد سجل تفصيلي لجميع أنشطة تحليل البيانات إذ يتضمن تاريخ جميع العمليات والإجراءات التي تمت على كل مجموعة من مجموعات البيانات.

9.اتخاذ الخطوات اللازمة لضمان عدم سيطرة الآلة وقيام أنظمة الذكاء الاصطناعي باتخاذ القرارات المهمة بالنيابة عن الأشخاص المعنيين، أو التأثير على قراراتهم دون الحصول على موافقتهم المسبقة.

10. إعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات وفقاً للأغراض المحددة والأنظمة والتشريعات ذات العلاقة.

11. التخلص من البيانات وإتلافها بطريقة آمنة - بما في ذلك البيانات المؤرشفة والنسخ الاحتياطية- وفقاً لسياسة التخلص من البيانات المعتمدة من قبل الجهة، ووفقاً للأنظمة والسياسات ذات العلاقة.

12. إعداد دليل إجرائي يوضح الخطوات اللازمة لتقييم المخاطر والأثار المحتملة المترتبة على تحليل البيانات باستخدام النماذج التنبؤية وخوارزميات الذكاء الاصطناعي، وذلك لقياس مدى تحقيق الأهداف العامة بأقل أثر ممكن على خصوصية الأفراد.

13. إعداد دليل إجرائي يوضح الخطوات اللازمة لتقييم أثر الانحياز في النتائج؛ لضمان تنوع مجموعة البيانات المراد تحليلها وتمثيلها لجميع الفئات المستخدمة بشكل عادل دون أي تمييز.

14. أن يتم تقييد استخدام نتائج تحليل البيانات على الغرض الذي استخدمت من أجله، وأن يكون الغرض متوافقًا مع الأنظمة واللوائح والسياسات ذات العلاقة.

15. يحظر بناء سجلات شخصية شاملة عن الأفراد عن طريق جمع بيانات من مصادر متعددة، مما يساعد على إمكانية تحليلها واستخلاص معلومات شخصية حساسة قد تؤدي بشكل مباشر أو غير مباشر إلى التنبؤ بالظروف الصحية، والمالية، والاجتماعية، والميول والتوجهات الفكرية، وغيرها.

خامساً: الالتزامات المتعلقة بتقنيات التعرّف على الوجه

1.إجراء تقييم الآثار السلبية والمخاطر المحتملة عند تحديد الأغراض المتعلقة باستخدام تقنيات التعرف على الوجه.

2.يحظر استخدام تقنيات التعرف على الوجه لأغراض المراقبة المستمرة - أو تتبع تحركات شخص أو مجموعة من الأشخاص بشكل دائم في الأماكن العامة وعلى نطاق واسع-، سواء كان ذلك لحظياً أو عن طريق الرجوع إلى السجلات التاريخية، ويستثنى من ذلك استخدامها لأغراض محددة وفقاً للأنظمة واللوائح والسياسات المعمول بها في المملكة.

3.تقييد استخدام تقنيات التعرف على الوجه على الحد الأدنى من البيانات لتحقيق الأغراض المحددة بناءً على أسس نظامية، مع تحديد فترة الاحتفاظ بها والأطراف المراد مشاركة هذه البيانات معها.

4.اتخاذ الإجراءات اللازمة والخطوات الكافية لتقييم الجودة والدقة والأداء النسبي للأنظمة المبنية على تقنيات التعرف على الوجه قبل استخدامها، وذلك وفقاً للممارسات القياسية.

5.يحظر استخدام الكاميرات المثبتة على الجسم أو التي يمكن ارتداؤها (Body Worn Cameras) والمدمجة بتقنيات التعرف على الوجه لأغراض المراقبة المستمرة.

6. الالتزام بمبدأ الشفافية وإشعار الأفراد بطريقة ملائمة في حال وجود كاميرات مدمجة بتقنيات التعرف على الوجه في الأماكن المسموح بها استخدام هذه التقنيات، (مثل المطارات ومقرات بعض الجهات الحكومية).

7.إعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات وفقاً للأغراض المحددة والأنظمة والتشريعات ذات العلاقة.

سادساً: أحكام عامة

أولًا: تتولى عمادة تقنية المعلومات باعتبارها الجهة التنظيمية في الجامعة بمواءمة أحكام هذه الوثيقة مع وثائقها التنظيمية وتعميمها على جميع الجهات التابعة أو المرتبطة بالجامعة، بما يحقق التكامل ويضمن تحقيق الهدف المنشود من إعداد هذه القواعد.

ثانياً: تلتزم العمادة بمراقبة وتوثيق الامتثال لهذه القواعد العامة بشكل دوري.

ثالثاً: تلتزم العمادة بالامتثال لهذه القواعد وتوثيق الامتثال وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية.

رابعاً: تلتزم العمادة بإبلاغ الجهات التنظيمية فوراً ودون تأخير وبما لا يتجاوز (72) ساعة من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشخصية، وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية.

خامساً: تلتزم العمادة عند تعاقدها مع جهات معالجة أخرى بأن تتحقق بشكل دوري من امتثال الجهات الأخرى لهذه القواعد وفقاً للآليات والإجراءات التي تحددها الجهة التنظيمية، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها الجامعة.

سادساً: يحق للعمادة وضع قواعد إضافية لاستخدام بعض التقنيات والخوارزميات الخاصة بالذكاء الاصطناعي بعد التنسيق مع المكتب.

سابعاً: تلتزم العمادة - بعد التنسيق مع مكتب إدارة البيانات الوطنية- بإعداد الآليات والإجراءات التي تنظم عملية معالجة الشكاوى والاعتراضات وفقاً لإطار زمني محدد وحسب نموذج الحوكمة الصادر من مكتب إدارة البيانات الوطنية.

تعليم متميز، بحث علمي مؤثر، مجتمع حيوي.