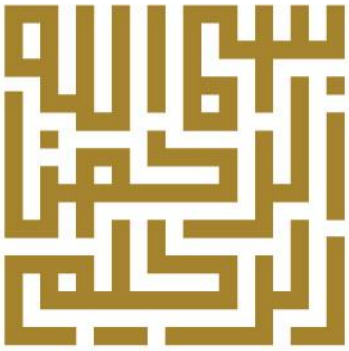
جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
وكالة الجامعة للتطوير والشراكة المجتمعية

سياسات حوكمة البيانات بجامعة الإمام عبد الرحمن بن فيصل

مكتب إدارة البيانات

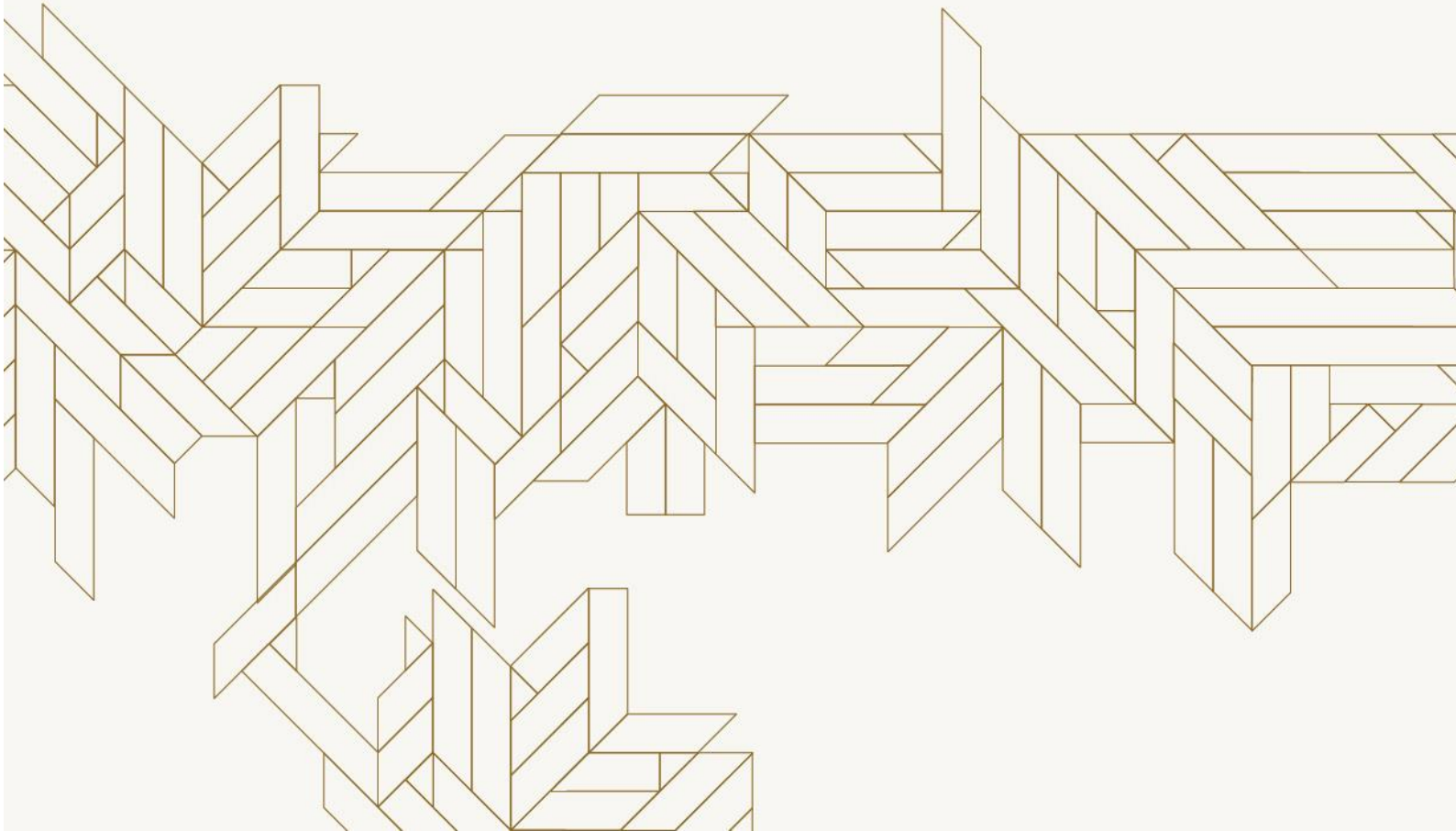
٢٠٢٢م



هذا الدليل معتمد من

مجلس جامعة الإمام عبد الرحمن بن فيصل في جلسته رقم (١٠١) والمنعقد في تاريخ ١٤٤٤/٤/٦هـ

مجلس الأمناء في جلسته رقم (١٤) والمنعقد بتاريخ ١٤٤٤/٨/٢٤هـ



المحتويات

١. مقدمة

في عصر التحول الرقمي، تُعدّ البيانات أحد أهم الأصول التي تمتلكها الجامعة لذلك تم انشاء مكتب ادارة البيانات بجامعة الإمام عبد الرحمن بن فيصل بقرار من معالي رئيس الجامعة برقم (٤٢٧٠٨/٤٢) وتاريخ ١٤٤٢/٧/٤هـ امتثالا للأمر السامي رقم (٥٩٧٦٦) بتاريخ ١٤٣٩/١١/٢٠هـ المتضمن تأسيس مكتب لإدارة البيانات بالجهات الحكومية ترتبط بالمسؤول الاول بالجهة، حيث تكمن اهمية مكتب ادارة البيانات في المحافظة على هذه الاصول وتمكينها وتعزيز القيمة المستفادة منها في اتخاذ القرار واستشراف المستقبل.

١-١ رؤية مكتب إدارة البيانات بجامعة الإمام عبد الرحمن بن فيصل

جامعة متميزة في حوكمة البيانات وتمكينها بما يعزز رؤية الجامعة واهدافها.

١-٢ الرسالة

إدارة البيانات الوطنية التابعة للجامعة ورقمنتها وتنميتها وتمكينها لتعزيز الأصول والقدرات وحماية البيانات الشخصية والحساسة، من خلال تطوير الاستراتيجيات والتشريعات والسياسات والضوابط اللازمة الصادرة من مكتب إدارة البيانات الوطنية ودعم تطبيقها وضمان الامتثال لها.

١-٣ الاهداف

١. تطوير أنظمة وسياسيات ومعايير وضوابط لإدارة البيانات وحماية البيانات الشخصية على مستوى الجامعة.
٢. دعم الجهات الداخلية في تطبيق أنظمة ومعايير وسياسات إدارة البيانات وحماية البيانات الشخصية.
٣. متابعة امتثال الجهات الداخلية لأنظمة ومعايير وسياسات إدارة البيانات وحماية البيانات الشخصية عن طريق بناء مؤشرات قياس الاداء ذات الصلة.
٤. تطوير استراتيجيات وبرمجيات للاستفادة من البيانات الخاصة بالجامعة وتوظيفها لدعم اتخاذ القرار ودعم المشاريع البحثية.

١-٤ مهام ومسؤوليات مكتب إدارة البيانات بجامعة الإمام عبد الرحمن بن فيصل

- تحديد الاحتياجات والمتطلبات الخاصة بمكتب إدارة البيانات فيما يساهم في انجاح المهام المنوطة به
- وضع ضوابط الاتصال بين المكتب والجهات ذات العلاقة بالجامعة وخارجها
- ضبط التواصل بين مكتب إدارة البيانات الوطنية وبين الجهات المختلفة بالجامعة
- متابعة بيانات الجهات الأكاديمية والإدارية داخل الجامعة حسب نماذج التقرير السنوي من منصة " اداء"
- تقديم خدمات وحلول تقنية لوحدات الجامعة والجهات ذات العلاقة
- توحيد معايير التعامل مع البيانات في جميع جهات الجامعة
- سهولة ودقة تحديد الوقت الحقيقي لتعزيز البيانات المالية للجامعة
- خفض تكاليف عمليات تكنولوجيا المعلومات وفريق العمل المكرس لإعداد التقارير وتقليل الأخطاء والتعارضات والتكرار غير الضروري
- زيادة مصداقة البيانات المتوفرة وسلامتها
- القيام بأنواع جديدة من التحليلات حسب ما تقتضي الحاجة
- تقليل تكاليف الوصول الى البيانات القديمة
- إكمال المهام الاخرى وفقا لتوجيهات المشرف على إدارة التخطيط الاستراتيجي
- إتاحة البيانات والاستفادة منها للأغراض البحثية

١-٥ إعداد سياسات حوكمة البيانات بجامعة الإمام عبد الرحمن بن فيصل

تم اعداد سياسات حوكمة البيانات بجامعة الإمام عبد الرحمن بن فيصل بالموائمة مع سياسات حوكمة البيانات الصادرة من مكتب ادارة البيانات الوطنية وبالاعتماد على الدليل الصادرة من المكتب وهو:

- سياسات حوكمة البيانات الوطنية

الاصدار الثاني بتاريخ ٢٠٢١/٠٥/٢٦م

PoliciesAr.pdf (sdaia.gov.sa)

NDMO
مكتب إدارة البيانات الوطنية
National Data Management Office

٢. المصطلحات والتعريفات

فيما يلي توضيح بما يُقصد بالكلمات والمصطلحات الواردة في الوثيقة حسب ما تمَّ تعريفها به في دليل سياسات حوكمة البيانات الوطنية المنشور على موقع مكتب ادارة البيانات الوطنية.

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.

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

الوصول إلى البيانات:
القدرة على الوصول المنطقي والمادي إلى البيانات الموارد التقنية للجهة لغرض استخدامها.

مستوى الوصول إلى البيانات:
مستوى يعتمد على الأذونات والصلاحيات التي تقيد الوصول إلى البيانات والموارد التقنية على الأشخاص المصرح لهم وفقاً لما هو مطلوب لإنجاز المهام والمسؤوليات المناطة بهم.

الإفصاح عن البيانات:
تمكين أي شخص - عدا جهة التحكم -من الحصول على البيانات واستعمالها أو الاطلاع عليها بأي وسيلة ولأي غرض.

التحقق:
التأكد من هوية أي مستخدم أو عملية أو جهاز بصفته متطلباً أساسياً للسماح بالوصول إلى الموارد التقنية.

التصريح:
تعريف حقوق وصلاحيات الوصول إلى البيانات والموارد التقنية لأي مستخدم أو برنامج أو عملية، والتحكم بمستويات الوصول إليها

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 غيرمصرّح به نظاماً.

البيانات المقروءة آلياً:
يُقصد بها البيانات المُهيكلة بصيغة معينة يمكن قراءتها ومعالجته آلياً باستخدام أجهزة الحاسب الآلي أو الأجهزة اللوحية وغيرها من الأجهزة.

مستويات تصنيف البيانات:
مستويات التصنيف التالية: (سري للغاية)، (سري)، (مقيّد)، (عام).

الإفصاح عن البيانات الشخصية:
تمكين أي شخص - عدا جهة التحكم -من الحصول على البيانات الشخصية أو استعمالها أو الاطلاع عليها بأي وسيلة اولأيّ غرض.

المعلومات العامة:
البيانات بعد المعالجة – غير المحمية – التي تتلقاها أو تنتجها أو تتعامل معها الجهات العامة مهما كان مصدرها، أو شكلها أو طبيعتها.

البيانات المفتوحة:
مجموعة محددة من المعلومات العامة –مقروءة آلياً - تكون متاحة للعموم مجاناً ودون قيود ويمكن لأي فرد، أو جهة عامة، أو خاصة استخدامها، أو مشاركتها.

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.

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

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.

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

البيانات المحمية:
البيانات المصنّفة على أنها (سري للغاية، سري، مقيّد).

معالجة البيانات الشخصية:
جميع العمليات التي تُجرى 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.

البيانات الوصفية:
هي المعلومات التي تصف البيانات وخصائصها، ومن بينها بيانات الأعمال والبيانات التقنية والتشغيلية.

المنصة الوطنية للبيانات المفتوحة:
هي منصة وطنية موحّدة على مستوى المملكة تُعنى بإدارة وحفظ ونشر مجموعات البيانات المفتوحة.

ترخيص البيانات المفتوحة:
رخصة تنظم استخدام البيانات المفتوحة.

الصيغة المفتوحة:
أي صيغة مقبولة على نطاق واسع وغير مسجلة الملكية وغير خاصة بمنصة معينة ويمكن قراءتها آلياً وتمكّن المعالجة الآلية لتلك البيانات، كما تيسّر قدرات التحليل والبحث.

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.

الجهة العامة:
أي جهة حكومية أو جهة اعتبارية عامة مستقلة في المملكة، أو أي من الجهات التابعة لها، وتعد في حكم الجهة العامة أي شركة تقوم بإدارة المرافق العامة أو البنى التحتية الوطنية أو تشغيلها أو صيانتها، أو تقوم بمباشرة خدمة عامة فيما يخص إدارة تلك المرافق أو البنى التحتية.

الأطراف الخارجية:
أي جهة حكومية أو جهة اعتبارية عامة مستقلة في المملكة، وأي شخصية ذات صفة طبيعية أو اعتبارية خاصة بخلاف صاحب البيانات أو جهة التحكم أو جهة المعالجة والأشخاص المصرح لهم، تُعنى بمعالجة البيانات الشخصية.

ممثل بيانات أعمال:
هو الشخص المسؤول عن البيانات التي يتم جمعها والاحتفاظ بها من قبل الجهة العامة التي يعمل بها، وغالباً ما يكون في مستوى إداري عالٍ، ويمكن أن يوجد في الجهة العامة أكثر من ممثل بيانات أعمال.

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.

مقدم الطلب:
أي جهة من القطاعين العام، أو الخاص، أو القطاع الثالث، أو أي فرد يتقدم بطلب لمشاركة البيانات.

طلب مشاركة البيانات:
النموذج المخصص لطلب مشاركة البيانات والذي يتضمن معلومات عن مقدم الطلب، والبيانات المطلوبة، والغرض الذي من أجله تم طلب مشاركة البيانات.

اتفاقية مشاركة البيانات:
اتفاقية رسمية موقعة بين طرفين – جهة حكومية مع أي طرف أخر - للموافقة على مشاركة البيانات وفقاً لشروط وأحكام محددة ومتوافقة مع مبادئ مشاركة البيانات.

الضوابط الأمنية:
الأجهزة والإجراءات والسياسات والضمانات المادية المستخدمة لضمان سلامة البيانات وحمايتها ووسائل معالجتها والوصول إليها.

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.

جهة المعالجة:
أي جهة حكومية أو جهة اعتبارية عامة مستقلة في المملكة، وأي شخصية ذات صفة طبيعية أو اعتبارية خاصة؛ تعالج البيانات الشخصية لمصلحة جهة التحكم ونيابةً عنها.

الجهة الحكومية:
أي جهة حكومية أو جهة عامة مستقلة بالمملكة، أو أي من الجهات التابعة لها، ويعد في حكم الجهة الحكومية أي شركة تقوم بإدارة المرافق العامة، أو البنى التحتية الوطنية ،أو تشغيلها أو صيانتها، أو تقوم بمباشرة خدمة عامة فيما يخص إدارة تلك المرافق أو البنى التحتية.

مكتب الجهة:
مكتب إدارة البيانات والخصوصية في الجهة العامة.

المكتب:
مكتب إدارة البيانات الوطنية.

الطفل:
كل شخص لم يتجاوز الثامنة عشرة من عمره.

الفرد:
الشخص المتقدم بطلب الاطلاع او الحصول على المعلومات العامة.

إشعار الخصوصية:
هو بيان خارجي موجّه 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.

آلية مشاركة البيانات:
الطريقة التي يتم عن طريقها مشاركة البيانات - تشمل كلًا من وسيلة نقل البيانات، والأطراف المشاركة في مشاركة البيانات، ونموذج المشاركة: المشاركة المباشرة، المشاركة عن طريق مزود خدمة، المشاركة عن طريق أطراف متعددة.

الأهلية:
صلاحية الشخص لصدور التصرفات منه على وجه يعتد به شرعاً ونظاماً.

ناقص الأهلية:
من لديه أهلية غير مكتملة كالصغير المميز- وهو من أكمل السابعة ولم يتم الثامنة عشرة من العمر – وذي الغفلة، والسفيه، ومن به عاهة عقلية، ونحوهم. ومن في حكمه: فاقد أو ناقص الأهلية.

الولي:
أحد الوالدين أو من تكون له الولاية على شؤون الطفل حسب أحكام الشريعة أو الأنظمة ذات العلاقة.

الولاية:
سلطة يثبتها الشرع للولي تخوله صلاحية التصرف وإدارة شؤون الطفل نيابة عنه فيما يتعلق ببدنه ونفسه وماله وبما يحقق مصالحه، ومنها اتخاذ القرارات الخاصة بمعالجة بياناته الشخصية.

البيانات الشخصية الحساسة:
كل بيان شخصي يتضمن الإشارة إلى أصل الطفل ومن في حكمه العرقي، أو القبلي، أو معتقده الديني، أو الفكري أو السياسي، أو يدل على عضويته في جمعيات أو مؤسسات أهلية. وكذلك البيانات الجنائية والأمنية، أو بيانات السمات الحيوية التي تحدد الهوية، أو البيانات الوراثية، أو البيانات الائتمانية، أو البيانات الصحية، وبيانات تحديد الموقع، والبيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهما.

التسويق المباشر:
أي اتصال، بأي وسيلة كانت، يتم عن طريقه توجيه مادة تسويقية أو دعائية إلى شخص بعينه.

سياسة الخصوصية:
هي وثيقة داخلية موجهة إلى العاملين في الجهات توضح حقوق أصحاب البيانات والالتزامات التي يجب الامتثال لها للمحافظة على خصوصية أصحاب البيانات وحماية حقوقهم.

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.

قائمة الاعتماد:
قائمة معتمدة من مكتب إدارة البيانات الوطنية تتضمن أسماء الدول التي تتمتع بمستوى كافٍ من الحماية لحقوق أصحاب البيانات فيما يتعلق بمعالجة بياناتهم الشخصية.

البيانات الحكومية:
هي البيانات التي تنتجها الجهات الحكومية.

البيانات غير المعالجة:
هي البيانات التي لم تخضع لعمليات متقدمة من المعالجة ويتم تبادلها في صيغتها الأولية كالبيانات الأساسية للمواطن التي يتم عرضها في بطاقة الهوية الوطنية، باستثناء المعالجة التي تفرضها الأنظمة واللوائح والسياسات لغرض مشاركة البيانات.

الخدمات الحكومية:
الخدمات الأساسية التي تقدمها الجهات الحكومية، والتي يمكن تقديمها عن طريق طرف ثالث نيابةً عن الجهة الحكومية.

مزود البيانات:
أي فرد أو جهة حكومية أو جهة خاصة تقوم بتزويد البيانات أو تقديم منتجات البيانات بمقابل مالي بشكل مباشر أو غير مباشر.

النقل المباشر:
نقل البيانات الشخصية من الجهة المرسلة إلى الجهة المستقبلة دون مرور البيانات بأي جهة أخرى.

النقل غير المباشر:
نقل البيانات الشخصية من الجهة المرسلة إلى الجهة المستقبلة مروراً بجهة أخرى أو أكثر.

النقل العرضي:
نقل البيانات الشخصية بشكل غير متكرر أومنتظم – عادةً ما يكون لمرة واحدة – لعدد محدود من الأشخاص، ومنها على سبيل المثال، نقل البيانات لغرض الاستفادة من خدمة في دولة أخرى لمصلحة صاحب البيانات.

منتجات البيانات:
الخدمات أو التطبيقات المعتمدة على البيانات بعد معالجتها بهدف خلق قيمة مضافة عن طريق دمجها مع بيانات أخرى، أو إثرائها أو تهيئتها أو تحليلها أو تمثيلها، ومنها على سبيل المثال لا الحصر: الرؤى و التحليلات التنبؤية أو الوصفية، ولوحات المعلومات التفاعلية (المنصات) وغيرها.

تحقيق الإيرادات من البيانات:
تحويل القيمة غير الملموسة للبيانات إلى قيمة حقيقية أو مادية بشكل مباشر (عن طريق تزويد البيانات غير المعالجة) أو غير مباشر (عن طريق تقديم منتجات البيانات).

نموذج تحقيق الإيرادات:
استراتيجية إدارة تدفقات إيرادات الجهة والموارد المطلوبة لكل تدفق الايرادات والمستهلكين المستهدفين.

نموذج العمل:
الهيكل الذي يصف الطريقة التي عن طريقها يمكن خلق قيمة سوقية باستغلال الفرص التجارية، بما في ذلك الشركاء الرئيسين، الأنشطة الرئيسة شرائح العملاء، نموذج الإيرادات وتدفقات الإيرادات، ويوضح الروابط المنطقية بينها وكيفية عملهما معاً.

المستفيد من البيانات:
أي فرد أو جهة حكومية أو جهة خاصة تقوم بطلب البيانات أو الاستفادة من منتجات البيانات بمقابل مالي.

التسويق:
نشاط تبادل، أو تداول، أو تزويد البيانات الخام، أو البيانات المعالجة مقابل مبلغ نقدي أو قيمة عينية أخرى.

عينة البيانات:
البيانات التي يتم استخدامها في بناء وتدريب واختبار النماذج التنبؤية وخوارزميات الذكاء الاصطناعي للوصول إلى نتائج معينة.

تقنيات الذكاء الاصطناعي:
هي مجموعة من النماذج التنبؤية والخوارزميات المتقدمة التي يمكن استخدامها لتحليل البيانات واستشراف المستقبل أو تسهيل عملية اتخاذ قرارات على أحداث متوقعة بالمستقبل.

تقنيات التعرف على الوجه:
تقنيات توفر إمكانية تحليل ملامح الوجه الرئيسية (القياسات الحيوية) لتحديد الهوية الشخصية للأفراد في الصور الثابتة أو الصور المتحركة (المرئية).

المطوّر:
أي شخصية ذات صفة طبيعية أو اعتبارية تقوم بتطوير أنظمة الذكاء الاصطناعي عن طريق بناء نماذج تنبؤية باستخدام البيانات والخوارزميات لتحقيق أهداف محددة.

صاحب البيانات:
الفرد الذي تتعلق به البيانات الشخصية أو من من يمثله أو من له الولاية الشرعية عليه.

المستخدم:
أي شخصية ذات صفة طبيعية أو اعتبارية تقوم بتطبيق أو استخدام أنظمة الذكاء الاصطناعي لتحقيق أهداف محددة.

نموذج التسعير: الآلية المستخدمة لتحديد القيمة العينية (سعر) للبيانات ومنتجات البيانات. **الجهة غير الربحية:** أي جهة غير حكومية مرخصة بالعمل في المملكة وتقدم خدماتها ومنتجاتها بشكل غير ربحي.	**الجهة الخاصة:** أي شخصية ذات صفة اعتبارية خاصة مرخصة بالعمل في المملكة – سواء أكانت محلية أو أجنبية –، ويعد في حكم الجهة الخاصة الفرد المواطن أو المقيم بشكل رسمي في المملكة الذي يقوم بتزويد البيانات أو تقديم منتجات البيانات.

٣. سياسات حوكمة البيانات

للمساهمة في رفع مستوى نضج مجال البيانات والذكاء الاصطناعي و تعزيز الاستفادة القصوى من ثروة البيانات وحمايتها، تتبنى جامعة الإمام عبد الرحمن بن فيصل مجموعة من السياسات المتوائمة والمشتقة من السياسات الصادرة من مكتب إدارة البيانات الوطنية فيما يخص حوكمة البيانات الوطنية و تتلخص في:

سياسة تصنيف البيانات

حماية سرية البيانات الوطنية وتصنيفها على أربعة مستويات.

سياسة حماية البيانات الشخصية

تنظيم عملية جمع البيانات الشخصية ومعالجتها ومشاركتها والحفاظ على السيادة الوطنية الرقمية عليها.

سياسة مشاركة البيانات

تعزيز مشاركة البيانات لتحقيق التكامل بين الجهات الحكومية والحصول على البيانات من مصادرها.

سياسة حرية المعلومات

تنظيم إطلاع المستفيدين على المعلومات العامة أو الحصول عليها بكافة أشكالها من الجهات الحكومية.

سياسة البيانات المفتوحة

إتاحة البيانات والمعلومات المفتوحة (غير المحمية) لعموم المستفيدين.

سياسة حماية البيانات الشخصية للأطفال ومن في حكمهم

مساعدة الجهات ذات الاختصاص في حماية الأطفال ومن في حكمهم من المخاطر المحتملة (العنف، الإساءة، الاعتداء، التهديد، الإيذاء أو الاستغلال) والمترتبة على جمع ومعالجة بياناتهم الشخصية عن طريق المواقع الإلكترونية والتطبيقات الرقمية.

القواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة

المحافظة على السيادة الوطنية الرقمية على البيانات الشخصية والعمل على توفير أفضل مستويات الحماية عند نقل البيانات الشخصية خارج الحدود الجغرافية للمملكة لضمان المحافظة على خصوصية أصحابها وحماية حقوقهم.

٤. السياسة الأولى: سياسة تصنيف البيانات

تنطبق أحكام هذه السياسة على جميع البيانات التي تجمعها وتمتلكها أو تنتجها أو تتعامل معها جامعة الامام عبد الرحمن بن فيصل مهما كان مصدرها، أو شكلها أو طبيعتها، ويشمل ذلك السجلات الورقية، الاجتماعات، والاتصالات عبر وسائل التواصل والتطبيقات، ورسائل البريد الإلكتروني، والبيانات المخزنة على وسائط إلكترونية، وأشرطة الصوت أو الفيديو، والخرائط، والصور الفوتوغرافية، والمخطوطات، والوثائق المكتوبة بخط اليد، وأي شكل آخر من أشكال البيانات المسجلة.

٤-١ المبادئ الرئيسية لتصنيف البيانات

المبدأ الأول: الأصل في البيانات الإتاحة

الاصل في البيانات أن تكون متاحة (في المجال التنموي) ما لم تقتِض طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية، والسرية للغاية (في المجال السياسي والأمني) ما لم تقتض طبيعتها أو حساسيتها مستويات أدنى من التصنيف والحماية.

المبدأ الثاني: الضرورة والتناسب

يتم تصنيف البيانات إلى مستويات وفقاً لطبيعتها، ومستوى حساسيتها، ودرجة أثرها مع الأخذ بعين الاعتبار الموازنة بين قيمتها ودرجة سريتها.

المبدأ الثالث: التصنيف في الوقت المناسب

يتم تصنيف البيانات عند إنشائها أو حين تلقيها من جهات أخرى ويكون التصنيف خلال فترة زمنية محددة.

المبدأ الرابع: المستوى الأعلى من الحماية

يتم اعتماد المستوى الأعلى من التصنيف عندما يتضمن محتوى مجموعة متكاملة من البيانات مستويات تصنيف مختلفة.

المبدأ الخامس: فصل المهام

يتم الفصل بين مهام ومسؤوليات العاملين - فيما يتعلق بتصنيف البيانات أو الوصول إليها أو الإفصاح عنها أو استخدامها أو التعديل عليها أو إتلافها - بطريقة تحول دون تداخل الاختصاص وتتلافى تشتيت المسؤولية.

المبدأ السادس: الحاجة إلى المعرفة

يتم تقييد الوصول إلى البيانات واستخدامها على أساس الاحتياج الفعلي للمعرفة، ولأقل عدد ممكن من العاملين.

المبدأ السابع: الحد الأدنى من الامتيازات

يتم تقييد إدارة صلاحيات العاملين على الحد الأدنى من الامتيازات اللازمة لأداء المهام والمسؤوليات المناطة بهم.

٤-٢ مستويات تصنيف البيانات

يتم تصنيف البيانات التي تمتلكها جامعة الامام عبد الرحمن بن فيصل او تتلقاها من جهات داخلية اوخارجية, او تتعامل معها بحسب مستويات تصنيف البيانات الرئيسية الواردة من مكتب ادارة البيانات الوطنية بما يتوافق مع مستوى الاثر المترتب على الافصاح عن هذه البيانات او تسريبها, وكما هو موضح في الجدول ادناه:

مستوى التصنيف	درجة الأثر	الوصف
سري للغاية	عالي	تصنف البيانات على أنها **بيانات سرية للغاية**، إذا كان الوصول غير المصرح به إلى هذه البيانات أو الافصاح عنها أو عن محتواها يؤدي إلى ضرر جسيم واستثنائي لا يمكن تداركه أو إصلاحه على: • المصالح الوطنية بما في ذلك الاخلال بالاتفاقيات والمعاهدات أو إلحاق الضرر بسمعة المملكة أو بالعلاقات الدبلوماسية والانتماءات السياسية أو الكفاءة التشغيلية للعمليات الامنية، أو العسكرية، أو الاقتصاد الوطني أو البنية التحتية الوطنية أو الاعمال الحكومية. • أداء الجهات العامة مما يلحق ضرر بالمصلحة الوطنية. • صحة الافراد وسلامتهم على نطاق واسع وخصوصية كبار المسؤولين • الموارد البيئية أو الطبيعية.
سري	متوسط	تصنف البيانات على أنها **بيانات سرية**، إذا كان الوصول غير المصرح به إلى هذه البيانات أو الافصاح عنها أو عن محتواها يؤدي إلى ضرر جسيم على: • المصالح الوطنية مثل إلحاق ضرر جزئي بسمعة المملكة والعلاقات الدبلوماسية أو الكفاءة التشغيلية للعمليات الامنية، أو العسكرية، أو الاقتصاد الوطني أو البنية التحتية الوطنية والأعمال الحكومية

		• يحدث خسارة مالية على المستوى التنظيمي تؤدي إلى إفلاس أو عجز الجهات عن أداء مهامها أو خسارة جسيمة للقدرة التنافسية أو كليهما معاً • يتسبب في حدوث أذى جسيم أو إصابة تؤثر على حياة مجموعة من الافراد. • تؤدي إلى ضرر على المدى الطويل للموارد البيئية أو الطبيعية. • التحقيق في القضايا الكبرى المحددة نظاماً، كقضايا تمويل الإرهاب.
مقيّد	**منخفض**	تصنف البيانات على أنها **مقيدة**، إذا كان الوصول غير المصرح به إلى هذه البيانات أو الافصاح عنها أو عن محتواها يؤدي إلى: • تأثير سلبي محدود على عمل الجهات العامة أو الانشطة الاقتصادية في المملكة أو على عمل شخص معين. • ضرر محدود على أصول أي جهة وخسارة محدودة على وضعها المالي والتنافسي. • ضرر محدود على المدى القريب للموارد البيئية أو الطبيعية.
عام	**لا يوجد**	تصنف البيانات على أنها **بيانات عامة**, عندما لا يترتب على الوصول غير المصرح به إلى هذه البيانات أو الافصاح عنها أو عن محتواها أي من الاثار المذكورة أعلاه في حال عدم وجود تأثير على ما يأتي: • المصلحة الوطنية • أنشطة الجهات • مصالح الأفراد • الموارد البيئة

جدول ١: مستوى تصنيف البيانات

بناء على مستويات التصنيف المذكورة في الجدول السابق، تقوم كل جهة مالكة للبيانات في الجامعة بالتعاون مع مكتب ادارة البيانات بالجامعة بتحديد وتطبيق الضوابط الامنية المناسبة لحماية البيانات وذلك لضمان التعامل معها ومعالجتها ومشاركتها والتخلص منها بشكل آمن.

٤-٣ ضوابط تصنيف البيانات

بناءً على مستويات التصنيف، تقوم الجامعة بتحديد وتطبيق الضوابط الأمنية المناسبة لحماية البيانات وذلك لضمان التعامل معها ومعالجتها ومشاركتها والتخلص منها بشكل آمن، وفي حال عدم تصنيف البيانات عند إنشائها أو تلقيها وفقاً لمعايير التصنيف، تُعامل هذه البيانات على أنها "مقيّدة" حتى يتم تصنيفها بشكل صحيح. كما يجب تصنيف

البيانات التي لم يتم تصنيفها وقت إصدار هذه السياسة خلال فترة زمنية محددة بموجب خطة عمل تعدها الجامعة ويتم اعتمادها من معالي رئيس الجامعة.

أدناه بعض الأمثلة على الضوابط التي يمكن استخدامها عند تصنيف البيانات، ويمكن الرجوع إلى ما يصدر من الهيئة الوطنية للأمن السيبراني من ضوابط وإرشادات تتعلق بحماية البيانات:

علامات الحماية

تُطبق علامات الحماية النصية على الوثائق الورقية والإلكترونية (بما في ذلك رسائل البريد الإلكتروني) وفقاً لكل مستوى من مستويات التصنيف.

الوصول

- يُمنح الوصول – المنطقي والمادي - للبيانات بناءً على مبدأ "الحد الأدنى من الامتيازات" و"الحاجة إلى المعرفة".
- يجب منع حق الوصول إلى البيانات بمجرد انتهاء أو إنهاء الخدمة المهنية للعاملين بالجهة.

الاستخدام

تُستخدم البيانات المصنفة وفقاً لمتطلبات مستويات التصنيف، على سبيل المثال، يتم تقييد استخدام البيانات المصنفة "سرية للغاية" على مواقع محددة سواء مادية – كالمكاتب – أو افتراضية باستخدام ترميز الأجهزة أو تطبيقات خاصة.

التخزين

- لا تُترك البيانات المصنفة على أنها "سري للغاية" و "سري" و "مقيّد" وكذلك الأجهزة المحمولة التي تعالج أو تخزن هذه البيانات دون مراقبة.
- يجب حماية البيانات المصنفة على أنها "سري للغاية" و "سري" و "مقيّد" غير المراقبة أثناء تخزينها مادياً أو إلكترونياً باستخدام أحد طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.

مشاركة البيانات

- تقوم الجهات بتحديد الوسائل المادية والرقمية المناسبة لتبادل البيانات بشكل آمن بما يضمن تقليل المخاطر المحتملة والامتثال لأنظمة مشاركة البيانات.
- يجب الاتفاق على آلية تبادل البيانات، سواء كانت الجهات ستستخدم الوسائل المستخدمة حالياً لتبادل البيانات أم لا، على سبيل المثال قناة التكامل الحكومية وشبكة مركز المعلومات الوطني والشبكة الحكومية الآمنة، أو إعداد اتصال مباشر جديد أو وسائط التخزين القابلة للإزالة أو الشبكة اللاسلكية، أو الوصول عن بعد، أو الشبكة الخاصة الافتراضية...الخ.

الاحتفاظ بالبيانات

- يتم إعداد جدول زمني يحدد فترة الاحتفاظ بجميع البيانات.
- يتم تحديد فترة الاحتفاظ بناءً على ما تحدده المتطلبات التجارية والتعاقدية والتنظيمية والقانونية ذات العلاقة.
- تتم مراجعة الجدول الزمني لفترة الاحتفاظ بشكل دوري - سنوي أو إذا طرأت تغييرات على المتطلبات ذات العلاقة.

التخلص من البيانات

- يتم التخلص من جميع البيانات بشكل آمن وفقاً للجدول الزمني للاحتفاظ بالبيانات بعد الحصول على موافقة ممثل بيانات الأعمال.
- يتم التخلص من البيانات التي تم تصنيفها على أنها "سرية للغاية" و"سري" التي يتم التحكم بها إلكترونياً باستخدام أحدث طرق التخلص من الوسائط الإلكترونية.
- يتم التخلص من جميع الوثائق الورقية باستخدام آلة تمزيق الورق.
- يتم إعداد سجل مفصّل عن جميع البيانات التي تم التخلص منها.

الأرشفة

- تتم أرشفة البيانات في مواقع تخزين آمنة وفقاً للطريقة التي يوصي بها ممثل بيانات الأعمال.
- يتم الاحتفاظ بنسخ احتياطية من البيانات المؤرشفة.
- تتم حماية البيانات المؤرشفة التي تم تصنيفها على أنها "سري للغاية" و"سري" باستخدام إحدى طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.
- يتم إعداد وتوثيق قائمة مفصلة تتضمن المستخدمين المصرح لهم بالوصول إلى البيانات المؤرشفة.

إلغاء التصنيف (رفع السرية)

- يجب إلغاء تصنيف البيانات أو خفض مستوى تصنيفها إلى الحد المناسب بعد انتهاء مدة التصنيف عندما لا تكون الحماية مطلوبة أو أنها لم تعد مطلوبة على المستوى الأصلي للتصنيف.
- في حال تم تصنيف البيانات بشكل خاطئ، يجب على مستخدم البيانات إشعار ممثل بيانات الأعمال لتحديد مدى الحاجة إلى إعادة تصنيفها بشكل مناسب.
- يجب تحديد عوامل تساعد على إلغاء تصنيف البيانات عند تحديد مستويات التصنيف لأول مرة، كما يجب تسجيلها في سجل أصول البيانات، قد تتضمن هذه العوامل ما يلي:

- فترة زمنية محددة بعد إنشاء البيانات أو تلقيها (على سبيل المثال: عامين بعد الإنشاء).
- فترة زمنية محددة بعد اتخاذ اخر إجراء على البيانات (على سبيل المثال: ستة أشهر من تاريخ آخر استخدام).
- بعد انقضاء تاريخ محدد (على سبيل المثال، من المقرر مراجعتها في ١ يناير ٢٠٢٣م)
- بعد ظروف أو أحداث معينة تؤثر تأثيراً مباشرًا على البيانات (على سبيل المثال: إحداث تغيير في الأولويات الاستراتيجية أو تغيير موظفي الجهات الحكومية).

- يتطلب إلغاء التصنيف - رفع السرية - أو خفض مستويات التصنيف، بعيداً عن العوامل المساعدة على إلغاء التصنيف الواضحة تماماً، فهماً سليماً لمحتوى البيانات السرية والسياق الذي وردت فيه.

٤-٤ خطوات تصنيف البيانات

الخطوة ١ – حصر الأصول وتحديد بيانات جامعة الامام عبد الرحمن بن فيصل

تتمثل الخطوة الاولى في جرد وتحديد جميع البيانات التي تمتلكها الجامعة والتي يمكن حصرها في بيانات الطلاب لدى عمادة القبول والتسجيل، بيانات الموظفين لدى ادارة الموارد البشرية , بيانات طلاب الدراسات العليا لدى عمادة الدراسات العليا, بيانات المستشفى الجامعي, وغيرها من البيانات الاخرى الخاصة بالاصول المختلفة.

الخطوة ٢ - تعيين مسؤول تصنيف البيانات على الجهة

تتولى الجامعة تفويض شخص يتولى مسؤولية عملية التصنيف بمجرد تحديد جميع البيانات، وهو ممثل من مكتب ادارة البيانات بالجامعة بالتعاون مع ممثل من الجهة المالكة للبيانات بحيث يكون على فهم ودراية بطبيعة البيانات وقيمتها داخل الجهة.

الخطوة ٣ - إجراء عملية تقييم الاثر

يجب على ممثل بيانات الأعمال اتباع الخطوات اللازمة لعملية تقييم الاثر المحتمل الذي يترتب على الاجراءات التالية:

- الافصاح عن هذه البيانات أو الوصول غير المصرح به إليها
- إجراء تعديل على هذه البيانات أو إتلافها أو كليهما
- عدم الوصول إلى هذه البيانات في الوقت المناسب

الخطوة ٤ – تحديد الانظمة ذات العلاقة (فقط إذا كان مستوى الاثر منخفضا)

يجب إجراء تقييمات إضافية إذا كان مستوى الاثر المحدد" منخفض" وذلك بهدف زيادة مستوى تصنيف البيانات المصنفة على أنها بيانات "عامة" إلى الحد الأقصى. حيث يتولى مكتب ادارة البيانات بالجامعة بالتعاون مع ممثل ملاك البيانات بدراسة ما إذا كان الإفصاح عن هذه البيانات يتعارض مع أنظمة المملكة العربية السعودية مثل نظام مكافحة الجرائم المعلوماتية ونظام التجارة الإلكترونية ... الخ، وإذا كان الإفصاح عن البيانات مخالفاً للأنظمة، فيجب حينها تصنيف البيانات على أنها بيانات "مقيدة".

الخطوة ٥ ـ الموازنة بين مزايا الإفصاح عن البيانات والأثار السلبية

بعد التأكد من مستوى الأثر المنخفض وضمان أن الافصاح لن يكون انتهاكاً لأي نظام نافذ، يجب أيضاً تقييم المزايا المحتملة للإفصاح عن مثل هذا البيانات والتأكد مما إذا كانت هذه المزايا ستفوق الاثار السلبية أم لا، وتشمل المزايا المحتملة استخدام البيانات لتطوير خدمات جديدة ذات قيمة مضافة، أو زيادة شفافية العمليات. إذا كانت المزايا أكبر من الاثار السلبية، تصنف البيانات على أنها "عامة". إذا كانت المزايا أقل من الاثار السلبية، تصنف البيانات على أنها "مقيدة".

الخطوة ٦ ـ مراجعة مستوى التصنيف

يجب أن يفحص تصنيف البيانات من قبل المكتب والتأكد بان البيانات مصنفة طبقا لطبيعتها واثرها.

الخطوة ٧ ـ تطبيق الضوابط المناسبة

تتمثل الخطوة الأخيرة من عملية تصنيف البيانات في حماية جميع البيانات وفقاً لمستوى التصنيف عن طريق تطبيق عناصر التحكم ذات الصلة.

٥. السياسة الثانية: سياسة حماية البيانات الشخصية

تطبق جامعة الامام عبد الرحمن بن فيصل احكام هذه السياسة كونها تقوم بمعالجة البيانات الشخصية المتعلقة بالأفراد مثل الموظفين، الطلاب، المرضى ومنسوبي المستشفى الجامعي ومن في حكمهم. علما بان البيانات الشخصية المتعلقة بالأفراد تجمع من اصحابها مباشرة وبعلمهم وتعالج للغرض الذي جمعت من اجله.

٥-١ المبادئ الرئيسية لحماية البيانات الشخصية

المبدأ الأول: المسؤولية

ان يتم تحديد وتوثيق سياسات وإجراءات الخصوصية الخاصة بجامعة الإمام عبد الرحمن بن فيصل عن طريق مكتب ادارة البيانات بالجامعة بالموائمة مع مكتب ادارة البيانات الوطنية واعتمادها من قبل معالي رئيس الجامعة (أو من يفوضه) ونشرها إلى جميع الاطراف المعنية بتطبيقها.

المبدأ الثاني: الشفافية

أن يتم إعداد إشعار عن سياسات وإجراءات الخصوصية الخاصة بجامعة الإمام عبد الرحمن بن فيصل 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 الافصاح عنها.

المبدأ الرابع: الحد من جمع البيانات

أن يقتصر جمع البيانات الشخصية على الحد الأدنى من البيانات الذي يمكن 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، و الاحتفاظ بها طالما كان ذلك ضرورياً لتحقيق الاغراض المحددة أو لما تقتضيه الانظمة واللوائح والسياسات المعمول بها في المملكة و اتلافها 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 عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية لمراجعتها، وتحديثها، وتصحيحها.

المبدأ السابع: الحدّ من الإفصاح عن البيانات

أن يتم تقييد الافصاح 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، او التعديل او 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.

٥-٢ حقوق صاحب البيانات

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

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

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

٥-٣ التزامات جامعة الإمام عبد الرحمن بن فيصل

١- أن تكون جامعة الامام عبد الرحمن بن فيصل مسؤولة عن إعداد وتطبيق السياسات والإجراءات المتعلقة بحماية البيانات الشخصية، ويكون معالي رئيس الجامعة – أو من يفوضه – مسؤولاً عن الموافقة عليها واعتمادها.

٢- أن تقوم جامعة الإمام عبد الرحمن بن فيصل بإنشاء مكتب لإدارة البيانات تتولى اعداد سياسات لحوكمة البيانات تكون مرتبطة بمكاتب إدارة البيانات في الجهات الحكومية التي تم تأسيسها بموجب الأمر السامي الكريم رقم ٥٩٧٦٦ وتاريخ١٤٣٩/١١/٢٠هـ على أن تتضمن مهام ومسؤوليات المكتب وضع المعايير المناسبة لتحديد مستويات حساسية البيانات الشخصية.

٣- أن تقوم جامعة الإمام عبد الرحمن بن فيصل بتقييم المخاطر والآثار المحتملة لأنشطة معالجة البيانات الشخصية وعرض نتائج التقييم على معالي رئيس الجامعة – أو من يفوضه – لتحديد مستوى قبول المخاطر وإقرارها.

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

٥- أن تقوم الجامعة 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 - بناء على قياس شدة الاثر.

٦- أن تقوم الجامعة متمثلة بمكتب ادارة البيانات ومن يسانده بإعداد برامج توعوية لتعزيز ثقافة الخصوصية ورفع مستوى الوعي وفقا لسياسات وإجراءات الخصوصية المعتمدة من الإدارة العليا.

٧- أن يتم إشعار صاحب البيانات - بطريقة ملائمة وقت جمع البيانات - بالغرض والاساس 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.

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

٩- أن يتم تزويد صاحب البيانات بالخيارات المتاحة فيما يتعلق بمعالجة البيانات الشخصية والآلية المستخدمة لممارسة هذه الخيارات.

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

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

١٢- أن يكون محتوى البيانات مقتصرا على الحد الأدنى من البيانات اللازمة لتحقيق الغرض من جمعها.

١٣- أن يتم تقييد جمع البيانات على المحتوى المعدّ سلفا ويكون بطريقة عادلة مباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التضليل.

١٤- أن يقتصر استخدام البيانات على الغرض التي جمعت من أجله.

١٥- أن تقوم جامعة الامام عبد الرحمن بن فيصل بإعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات وفقا للأغراض المحددة والأنظمة والتشريعات ذات العلاقة.

١٦- أن تقوم جامعة الامام عبد الرحمن بن فيصل متمثلة في قطاعاتها التي تتولى جمع وتخزين البيانات بتخزين البيانات الشخصية ومعالجتها داخل الحدود الجغرافية للمملكة لضمان المحافظة على السيادة الوطنية الرقمية لهذه البيانات، ولا تجوز معالجتها خارج المملكة إلا بعد حصول الجامعة على موافقة كتابية من الجهة التنظيمية، بعد تنسيق الجهة التنظيمية مع المكتب.

١٧- أن تقوم جامعة الامام عبد الرحمن بن فيصل بإعداد وتوثيق سياسة وإجراءات التخلص من البيانات لإتلاف البيانات بطريقة آمنة تمنع إساءة استخدامها أو الوصول غير المصرح به إليها – وتشمل البيانات التشغيلية، المؤرشفة، والنسخ الاحتياطية – وذلك وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني.

١٨- أن تقوم جامعة الإمام عبد الرحمن بن فيصل بتضمين أحكام سياستي الاحتفاظ والتخلص من البيانات في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.

١٩- أن تقوم جامعة الإمام عبد الرحمن بن فيصل بتحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية وذلك لمراجعتها وتحديثها.

٢٠- أن تقوم جامعة الامام عبد الرحمن بن فيصل بالتحقق من هوية الأفراد قبل منحهم الوصول إلى بياناتهم الشخصية وفقاً للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.

٢١- يحظر مشاركة البيانات الشخصية مع جهات أخرى إلا وفقاً للأغراض المحددة بعد موافقة صاحب البيانات ووفقاً للأنظمة واللوائح والسياسات على أن تزود الجهات الاخرى بسياسات وإجراءات الخصوصية المتبعة وتضمينها في العقود و الاتفاقيات.

٢٢- أن يُشعَر أصحاب البيانات وتؤخذ الموافقة منهم في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الاغراض المحددة.

٢٣- أن تقوم جامعة الإمام عبد الرحمن بن فيصل بأخذ موافقة مكتب ادارة البيانات الوطنية - بعد التنسيق مع الجهة التنظيمية - قبل مشاركة البيانات الشخصية مع جهات أخرى خارج المملكة.

٢٤- أن تقوم جامعة الإمام عبد الرحمن بن فيصل بإعداد وتوثيق وتطبيق الإجراءات اللازمة لضمان دقة البيانات الشخصية واكتمالها وحداثتها وارتباطها بالغرض الذي جمعت من أجله.

٢٥- أن يتم استخدام الضوابط الإدارية والتدابير التقنية المعتمدة في سياسات الجامعة لأمن المعلومات لضمان حماية البيانات الشخصية ومنها على سبيل المثال:

- منح صلاحيات الوصول إلى البيانات وفقا 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 إلاّ 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.

٢٦- أن تكون جامعة الإمام عبد الرحمن بن فيصل متمثلة في مكتب ادارة البيانات 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 والمكتب حسب التسلسل التنظيمي.

٦. السياسة الثالثة: سياسة مشاركة البيانات

تحدد هذه السياسة ضوابط مشاركة البيانات التابعة لجامعة الامام عبد الرحمن بن فيصل مع الجهات الحكومية الاخرى او الجهات الخاصة او الافراد مهما كان مصدر هذه البيانات، او شكلها او 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. علما بانه لا تنطبق أحكام هذه السياسة في حال كانت الجهة الطالبة للبيانات جهة حكومية وكان الطلب لأغراض أمنية أو لاستيفاء متطلبات قضائية.

٦-١ المبادئ الرئيسية لمشاركة البيانات

المبدأ الأول: تعزيز ثقافة المشاركة

على جميع الجهات الحكومية مشاركة البيانات الرئيسية التي تنتجها وذلك لتحقيق التكامل بين هذه الجهات 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 – 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 الافراد، أو سلامة البيئة – ويستثنى من ذلك البيانات والجهات المستثناة بأوامر سامية.

المبدأ الثالث: الوصول المصرّح به

أن يكون لدى جميع الاطراف المُشاركة في مشاركة البيانات صلاحية الاطلاع على هذه البيانات والحصول عليها واستخدامها (والتي قد تتطلب المسح الأمني حسب طبيعة وحساسية البيانات) , بالإضافة إلى المعرفة، والمهارة، و الأشخاص 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، الغرض من جمعها، ووسائل نقلها، وطرق حفظها، والضوابط المستخدمة لحمايتها وآلية التخلص منها.

المبدأ الخامس: المسؤولية المشتركة

ان تكون جميع الاطراف المُشاركة 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

ان تقوم جميع الاطراف المُشاركة في عملية 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

ان تقوم جميع الاطراف المُشاركة 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 فقط.

٦-٢ خطوات عملية مشاركة البيانات

١- يقوم مقدم الطلب - سواء كان جهة حكومية أو خاصة أو فردا- بإرسال طلب مشاركة بيانات إلى مكتب ادارة البيانات بجامعة الامام عبد الرحمن بن فيصل، على أن يرسل الطلب عن طريق مكتب ادارة البيانات في الجهة مقدمة الطلب في حال كان مقدم الطلب جهة حكومية.

٢- يقوم مكتب ادارة البيانات بالجامعة بإحالة الطلب إلى ممثل بيانات الأعمال والذي بدوره يقوم بتوجيه هذا الطلب إلى أحد مختصي بيانات الأعمال لتقييم الطلب ومعالجته.

٣- يقوم مختص بيانات الأعمال بالتحقق من مستوى تصنيف البيانات المطلوبة:

أ. في حالة عدم تحديد مستوى التصنيف، يجب على مكتب ادارة البيانات بجامعة الامام عبد الرحمن بن فيصل 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.

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

٤- يجب على مختص بيانات الأعمال في مكتب ادارة البيانات بالجامعة استكمال عملية المشاركة إذا تم استيفاء جميع مبادئ مشاركة البيانات بالكامل.

٥- لا يجوز لمختص بيانات الأعمال في مكتب ادارة البيانات بالجامعة 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.

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

٧- يقوم مختص بيانات الأعمال في مكتب ادارة البيانات بجامعة الامام عبد الرحمن بن فيصل بتحديد الضوابط المناسبة لضمان الالتزام بمبادئ مشاركة البيانات وتحقيق الأهداف المحددة لكل منها، كما يجب أن يتم الاتفاق بين مختص بيانات الأعمال في الجامعة ومقدم الطلب والأطراف الأخرى المُشارِكة في عملية المشارَكة على تطبيق هذه الضوابط.

٨- بعد الاتفاق على ضوابط مشاركة البيانات والالتزام بتطبيقها، ينبغي لمختص بيانات الأعمال توضيحها بالتفصيل في الاتفاقية ويجب على جميع الأطراف المشارِكة التوقيع على اتفاقية مشاركة البيانات.

٩- يمكن لمكتب ادارة البيانات بالجامعة مشاركة البيانات المطلوبة مع الجهة الطالبة بعد توقيع اتفاقية مشاركة البيانات.

٦-٣ الإطار الزمني لعملية مشاركة البيانات

تقوم الجهة الحكومية - المطلوب منها مشاركة البيانات - بتقييم الطلب خلال فترة زمنية لا تتجاوز ٣٠ يوما من تاريخ استلام الطلب، وإشعار مقدم الطلب بقرار المشاركة على أن يكون القرار مكتوباً ومسبّباً (الخطوات من ٢ إلى ٤ من عملية مشاركة البيانات الموضحة اعلاه). 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 ١٤ يوماً من تاريخ استلامه (الخطوة ٥ من عملية مشاركة البيانات).

بعد الحصول على موافقة ممثل بيانات الأعمال على الاستمرار في عملية المشاركة (الخطوة ٦ من عملية مشاركة البيانات)، يقوم مختص بيانات الأعمال بتطوير وتطبيق الضوابط المناسبة لمشاركة البيانات وإعداد اتفاقية مشاركة بيانات خلال فترة زمنية لا تتجاوز ٦٠ يوماً من تاريخ موافقة ممثل بيانات الأعمال (الخطوة ٧ من عملية مشاركة البيانات).

بعد توقيع اتفاقية مشاركة البيانات (الخطوة ٨ من عملية مشاركة البيانات) يقوم مختص بيانات الأعمال بمشاركة البيانات مع مقدم الطلب خلال ٧ أيام من تاريخ توقيع الاتفاقية (الخطوة ٩ من عملية مشاركة البيانات).

٦-٤ ضوابط مشاركة البيانات

يجب على جميع الأطراف المشاركة في عملية مشاركة البيانات الموافقة على الضوابط اللازمة لإدارة البيانات المشتركة وحمايتها بشكل مناسب:

الأساس النظامي

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

- أن يوضح الأساس النظامي أو الاحتياج الفعلي لمشاركة البيانات، ومنها على سبيل المثال: تنظيم الجهة، الأمر الملكي/السامي الذي يسمح للجهة بمشاركة البيانات، أو الاتفاقية الموقعة.
- أن يُلتزم بمستويات تصنيف البيانات والمحافظة على حقوق الملكية الفكرية وخصوصية البيانات الشخصية.

التفويض

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

- أن تُحدد الجهات و الأشخاص المخولين بطلب البيانات وتلقيها (يمكن التحقق من الامتثال لسياسة تصنيف البيانات – ضوابط الاستخدام والوصول إلى البيانات)

نوع البيانات

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

- أن يتم التأكد من أن البيانات المطلوبة ضمن البيانات الرئيسية التي تنتجها الجامعة 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 أو بيانات معالجة).

المعالجة المسبقة للبيانات

(المبادئ ذات العلاقة: المبدأ السادس: أمن البيانات)

- أن تحدد 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 ان لا تتم معالجة البيانات بشكل يغير المحتوى.
- أن تّقيم جودة البيانات المطلوبة وصحتها وسلامتها وتحديد ما إذا كانت تتطلب إجراء تحسين قبل مشاركتها، وفي حال الحاجة لذلك يجب على مكتب ادارة البيانات بالجامعة 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 الامنة المعتمدة بين الجهات.
- أن يتم تحديد آلية مشاركة البيانات، وما إذا كان مختص بيانات الأعمال سيقوم بنقل البيانات مباشرة 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 (شبكة الانترنت 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: المبدأ الثاني: مشروعية الغرض، المبدأ الرابع: الشفافية، المبدأ السادس: أمن البيانات، المبدأ السابع: الاستخدام الاخلاقي)

- أن تحدد متطلبات حماية البيانات عند مشاركتها، وتطبيق الضوابط المحددة لحماية البيانات بعد مشاركتها.
- أن تُفرض قيود مناسبة على الاستخدام أو المعالجة المسموح بها للبيانات (إن وجدت)، 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 تحدد ما إذا كان هناك طرف ثالث للاستفادة من البيانات بعد مشاركتها والاتفاق على الالية المنظمة لذلك.

مدة مشاركة البيانات وعدد مرات المشاركة وإلغاء المشاركة

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

- أن تحدد مدة مشاركة البيانات والموعد النهائي للوصول إلى البيانات أو تخزينها.
- أن تحدد عدد مرات مشاركة البيانات، والمتطلبات اللازمة للمراجعة، وإجراء التعديلات، والاجراءات التي سيتم اتخاذها عند انتهاء الاتفاقية (مثل إخفاء هوية أصحاب البيانات أو إلغاء الوصول إلى البيانات أو اتلافها).
- أن تحدد الاطراف 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 يُتفق على تحديد المسؤوليات في حال عدم الالتزام ببنود الاتفاقية، وغيرها من الالتزامات بين الاطراف المشاركة كإنهاء الاتفاقية والاجراءات التصحيحية.

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

٦-٥ القواعد العامة لمشاركة البيانات

تلتزم جامعة الامام عبد الرحمن بن فيصل بالقواعد التالية عند مشاركة البيانات مع اي جهة اخرى:

١- إعطاء الاولوية لوسائط المشاركة المعتمدة والامنة لتبادل البيانات.

٢- يتولى مختص بيانات الأعمال في مكتب ادارة البيانات بالجامعة مسؤولية مشاركة البيانات بعد استيفاء جميع مبادئ مشاركة البيانات، بالإضافة إلى تحديد الضوابط المناسبة للمشاركة.

٣- يجب على الجامعة تعيين أو تفويض الشخص المناسب – حسب المؤهلات والتدريب المطلوب - للتعامل مع البيانات بطريقة صحيحة، على أن يكون مصرح له طلب البيانات المشتركة وتلقيها والوصول إليها وتخزينها واتلافها.

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

٥- يجب إرفاق البيانات الوصفية metadata عند مشاركة البيانات في الحالات التي تتطلب ذلك.

٦- تكون الجهات المُشاركة في مشاركة البيانات مسؤولة عن حماية البيانات واستخدامها وفقا للأغراض المحددة، ويحق لمكتب ادارة البيانات بالجامعة مراجعة مدى الالتزام بشكل دوري أو عشوائي بما يتوافق مع الضوابط المحددة في اتفاقية مشاركة البيانات.

٧- يقوم المكتب بإعداد الدليل الارشادي لمشاركة البيانات والمتضمن نموذج طلب مشاركة البيانات ونموذج اتفاقية قياسية لمشاركة البيانات.

٨- تقوم الجهات التنظيمية – بعد التنسيق مع المكتب – بإعداد الاليات والاجراءات والضوابط المتعلقة بتسوية النزاع وفقاً لإطار زمني محدد.

٩- في حال وجود نزاع بين الاطراف المشاركة في عملية مشاركة البيانات، يحق للجهات التابعة لنفس الجهة التنظيمية إشعار الجهة التنظيمية والمطالبة بتسوية النزاع بين الاطراف المشاركة، وفي حال لم يتم حل النزاع، يتم إشعار مكتب ادارة البيانات الوطنية بذلك، ويتولى المكتب تسوية النزاع.

١٠- في حال وجود جانب من جوانب مشاركة البيانات لا تشملها هذه السياسة، يحق لمكتب ادارة البيانات بجامعة الامام عبد الرحمن بن فيصل وضع قواعد إضافية لا تتعارض مع مبادئ مشاركة البيانات مع تقديم مسوغ كافٍ وإشعار مكتب ادارة البيانات الوطنية بذلك.

١١- تحرص جامعة الامام عبد الرحمن بن فيصل في مشاركة بياناتها على إيجاد التوازن المناسب بين الحاجة إلى مشاركة البيانات وضمان حماية سرية البيانات والمخاطر المحتملة على الفرد أو المجتمع

١٢- تقوم الجامعة بالاحتفاظ بجميع طلبات مشاركة البيانات والقرارات المتعلقة بها.

١٣- تقوم جامعة الامام عبد الرحمن بن فيصل بتطوير واعتماد ونشر سياسة مشاركة البيانات الخاصة بها.

١٤- يجب على الجهات داخل الجامعة وخارجها عند استلامها للبيانات المشتركة عدم مشاركتها مع طرف آخر أو جهة أخرى دون موافقة الجهة المنتجة للبيانات.

١٥- تكون جامعة الإمام عبد الرحمن بن فيصل متمثلة في مكتب ادارة البيانات مسؤولة عن مراقبة وتنفيذ هذه السياسة.

٧. السياسة الرابعة: سياسة حرية المعلومات

تنطبق هذه السياسة على جميع طلبات الاطلاع أو الحصول على المعلومات العامة – غير المحمية – التي تنتجها جامعة الامام عبد الرحمن بن فيصل مهما كان مصدرها، أو شكلها أو طبيعتها – ويشمل ذلك السجلات الورقية ورسائل البريد الالكتروني 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 والمتمثلة في:

١- المعلومات التي يؤدي إفشاؤها إلى الاضرار بالأمن الوطني للدولة، أو سياساتها، أو مصالحها أو حقوقها.
٢- المعلومات العسكرية والأمنية.
٣- المعلومات والوثائق التي يتم الحصول عليها بمقتضى اتفاق مع دولة أخرى وتصنف على أنها محمية.
٤- التحريات والتحقيقات وأعمال الضبط وعمليات التفتيش والمراقبة المتعلقة بجريمة أو مخالفة أو تهديد.
٥- المعلومات التي تتضمن توصيات أو اقتراحات أو استشارات من أجل إصدار تشريع أو قرار حكومي لم يصدر بعد.
٦- المعلومات ذات الطبيعة التجارية، أو الصناعية، أو المالية أو الاقتصادية التي يؤدي الافصاح عنها إلى تحقيق ربح أو تلافي خسارة بطريقة غير مشروعة.
٧- الابحاث العلمية أو التقنية، أو الحقوق المشتملة على حق من حقوق الملكية الفكرية التي يؤدي الكشف عنها إلى المساس بحق معنوي.
٨- المعلومات المتعلقة بالمنافسات والعطاءات والمزايدات التي يؤدي الافصاح عنها إلى الاخلال بعدالة المنافسة.
٩- المعلومات التي تكون سرية أو شخصية بموجب نظام آخر، أو تتطلب إجراءات نظامية معينة للوصول إليها أو الحصول عليها.

٧-١ المبادئ الرئيسة لحرية المعلومات

المبدأ الأول: الشفافية

للفرد الحق في معرفة المعلومات المتعلقة بأنشطة جامعة الامام عبد الرحمن بن فيصل العامة تعزيزاً لمنظومة النزاهة والشفافية والمساءلة.

المبدأ الثاني: الضرورة والتناسب

أي قيود على طلب الاطلاع أو الحصول على المعلومات المحمية التي تتلقاها أو تنتجها أو تتعامل معها جامعة الامام عبد الرحمن بن فيصل 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 الافراد.

٧-٢ حقوق الأفراد بما يتعلق بالاطلاع على المعلومات العامة أو الحصول عليها من جامعة الإمام عبد الرحمن بن فيصل

اولاً: لدى الافراد حق الاطلاع والحصول على أي معلومة غير محمية لدى جامعة الامام عبد الرحمن بن فيصل.

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

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

٧-٣ التزامات جامعة الإمام عبد الرحمن بن فيصل فيما يخص المعلومات العامّة

١- أن تكون جامعة الامام عبد الرحمن بن فيصل مسؤولة عن إعداد وتطبيق السياسات و الاجراءات المتعلقة بممارسة حق الوصول إلى المعلومات العامة أو الحصول عليها، ويكون معالي رئيس الجامعة (او من ينوب عنه) مسؤولاً عن الموافقة عليها واعتمادها.

٢- أن تقوم جامعة الإمام عبد الرحمن بن فيصل بإنشاء وحدة إدارية تكون مرتبطة بمكتب ادارة البيانات بالجامعة ويسند لها مسؤولية تطوير وتوثيق ومراقبة تنفيذ السياسات و الاجراءات المعتمدة من الإدارة العليا بالجامعة 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.

٣- أن تقوم الجامعة 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.

٤- ان تقوم الجامعة بتحديد وتوفير الوسائل الممكنة (نماذج طلب المعلومات العامة) – سواء كانت نماذج ورقية أو إلكترونية – والتي من خلالها يمكن للفرد طلب الاطلاع على المعلومات العامة أو الحصول عليها.

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

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

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

٨- أن تقوم الجامعة بإشعار الفرد - بطريقة ملائمة – في حال تم رفض الطلب كلياً أو جزئيا، مع إيضاح أسباب الرفض والحقّ في التظلم وكيفية ممارسة هذا الحق خلال مدة لا تتجاوز ١٥ يوما من اتخاذ القرار.

٩- أن تقوم الجامعة بإعداد برامج توعوية لتعزيز ثقافة الشفافية ورفع مستوى الوعي وفقا لسياسات وإجراءات حرية المعلومات المعتمدة من الإدارة العليا للجامعة.

١٠- ان تكون الجامعة متمثلة في مكتب ادارة البيانات مسؤولة عن مراقبة الامتثال لسياسات وإجراءات حرية المعلومات 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 ادارة البيانات الوطنية حسب التسلسل الإداري.

٧-٤ الخطوات الرئيسة للاطلاع على المعلومات أو الحصول عليها

أولاً: يتم تقديم الطلبات عن طريق ملء" نموذج طلب معلومات عامة"– إلكتروني أو ورقي – وتقديمه للجامعة باعتبارها جهة المعلومات المطلوبة.

ثانياً: تقوم الجامعة، في فترة زمنية محددة (لا تتجاوز ٣٠ يوماً) باستلام طلب الاطلاع أو الحصول على المعلومات العامة، باتخاذ أحد القرارات التالية:

١- **الموافقة**: في حال تمت موافقة الجامعة على طلب الوصول إلى المعلومات أو الحصول عليها كلياً أو جزئياً، فيجب إشعار الفرد خطياً أو إلكترونياً بالرسوم المطبقة، ويجب على الجامعة إتاحة هذه المعلومات للفرد خلال فترة زمنية لا تتجاوز (١٠) أيام عمل من استلام المبلغ.

٢- **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 كلياً أو جزئيا
- أسباب الرفض، إن أمكن
- الحق في التظلم على هذا الرفض وكيفية ممارسة هذا الحق.

٣- **التمديد**: في حال عدم إمكانية معالجة طلب الوصول إلى المعلومات في الوقت المحدد، ينبغي للجامعة تمديد الفترة التي سيتم الرد فيها بمدة معقولة حسب حجم وطبيعة المعلومات المطلوبة – على سبيل المثال لا تتجاوز (٣٠) 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.

٤- **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:

- نـوع الإشعار، علـى سـبيل المثـال، البيانـات المطلوبـة متاحـة علـى موقـع الجهـة، أو ليسـت مـن اختصاصهـا.
- الحق في التظلم على هذا الإشعار وكيفية ممارسة هذا الحق.

ثالثاً: فـي حالـة رغبة الفرد فـي التظلّم علـى رفض الطلـب مـن قبـل الجامعة، فيمكنـه تقديـم إشـعار خطـي أو إلكترونـي بالتظلـم إلـى مكتـب ادارة البيانات بالجامعة خلال فتـرة زمنيـة لا تتجـاوز (١٠) أيـام عمـل مـن استلامه لقرار الجامعة، وتقوم لجنـة التظلم بمكتـب ادارة البيانات بالجامعة بمراجعـة الطلـب واتخـاذ القـرار المناسـب وإشـعار الفـرد برسـوم المراجعـة – يتـم اسـترجاعها فـي حـال موافقـة اللجنـة علـى الطلـب – وقـرار الاستئناف.

٧-٥ احكام عامة

أولاً: تتولـى جامعة الإمام عبد الرحمن بن فيصل مواءمـة هـذه السياسـة مـع وثائقهـا التنظيميـة – السياسـات والاجراءات – وتعميمهـا علـى جميـع الجهـات التابعـة لهـا أو المرتبطـة بهـا بمـا يحقـق التكامـل ويضمـن تحقيـق الهـدف المنشـود مـن إعدادهـا.

ثانياً: يجـب علـى جامعة الامام عبد الرحمن بن فيصل موازنـة حـق الاطلاع والحصـول علـى المعلومـات مـع المتطلبـات الضروريـة الأخرى كتحقيـق الامن الوطنـي والمحافظـة علـى خصوصيـة البيانـات الشـخصية.

ثالثاً: يجـب علـى الجهـات العامـة الامتثال لهـذه السياسـة وتوثيـق الامتثال بشـكل دوري وفقـاً للآليات والاجراءات التـي تحددهـا الجامعة بعـد التنسـيق مـع مكتب ادارة البيانات الوطنية.

رابعـاً: تقـوم الجامعة – بعـد التنسـيق مـع مكتب ادارة البيانات الوطنية – بإعـداد الآليات والاجراءات والضوابـط المتعلقـة بمعالجـة الشـكاوى وفقـاً لإطار زمنـي محـدد وحسـب التسلسـل التنظيمـي.

خامساً: يجـب علـى الجهات العامة إشـعار مكتب ادارة البيانات الوطنية فـي حـال تـم رفض طلـب الاطلاع أو الحصـول علـى المعلومـات العامـة أو تمديـد الفتـرة المحـددة لتقديـم هـذه المعلومـات وهـي ضمـن النطـاق.

سادساً: يجـب علـى الجهـة العامـة عنـد تعاقدهـا مـع جهـات أخـرى – كالشـركات التـي تقـوم بمباشـرة الخدمـات العامـة – أن تتحقـق بشـكل دوري مـن امتثـال الجهـات الأخرى لهـذه السياسـة وفقـاً للآليات والاجراءات التـي تحددهـا الجهـة، علـى أن يشـمل ذلـك أي تعاقدات لاحقة تقوم بهـا الجهـات الاخرى.

سابعاً: يحـق للجامعة وضـع قواعـد إضافيـة لمعالجـة الطلبـات المتعلقـة بأنـواع محـددة مـن المعلومـات العامـة وفقـاً لطبيعتهـا وحساسـيتها بعـد التنسـيق مـع مكتب ادارة البيانات الوطنية.

ثامناً: يجب على الجامعة إعداد نماذج للاطلاع أو الحصول على المعلومات العامة – سواء أكانت ورقية أو إلكترونية – يحدد فيها المعلومات اللازمة والوسائل الممكنة لتقديم المعلومات المطلوبة.

٦-٧ حرية المعلومات والبيانات المفتوحة

عادة 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 و روّاد الأعمال والمبتكرين والشركات الناشئة يساعد على تهيئة بيئة مواتية لنمو الاعمال 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.

٨. السياسة الخامسة: سياسة البيانات المفتوحة

تعد البيانات المفتوحة مجموعة فرعية من المعلومات العامة وفقاً لمستويات التصنيف الموضحة في سياسة تصنيف البيانات.

تنطبق أحكام هذه السياسة على جميع البيانات والمعلومات العامة – غير المحمية – التي تنتجها جامعة الإمام عبد الرحمن بن فيصل مهما كان مصدرها، أو شكلها أو طبيعتها – ويشمل ذلك السجلات الورقية ورسائل البريد الالكتروني 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.

٨-١ المبادئ الرئيسة للبيانات المفتوحة

المبدأ الأول: الأصل في البيانات الإتاحة

يضمن هذا المبدأ إتاحة بيانات الجامعة العامة للجميع من خلال الإفصاح عنها أو تمكين الوصول إليها أو استخدامها مالم تقتضِ طبيعتها عدم الافصاح عنها أو حماية خصوصيتها أو سريتها.

المبدأ الثاني: الصيغة المفتوحة وإمكانية القراءة آليا

يتم إتاحة البيانات وتوفيرها بصيغة مقروءة آلياً تسمح بمعالجتها بشكل آلي – بحيث يتم حفظها بصيغ الملفات شائعة الاستخدام (مثل CSV أو XLS، أو JSON ،أو XML)

المبدأ الثالث: حداثة البيانات

يتم نشر أحدث إصدار من مجموعات البيانات المفتوحة بصفة منتظمة وإتاحتها للجميع حال توافرها. كما يتم نشر البيانات المجمّعة من قبل الجهات العامة في أسرع وقت ممكن بمجرد جمعها، كلما أمكن ذلك، وتُعطى الاولوية للبيانات التي تقل فائدتها بمرور الوقت.

المبدأ الرابع: الشمولية

يجب أن تكون مجموعات البيانات المفتوحة شاملة وتتضمن أكبر قدر ممكن من التفاصيل، وأن تعكس البيانات المسجلة بما لا يتعارض مع سياسة حماية البيانات الشخصية. كما يجب إدراج البيانات الوصفية التي توضح وتشرح البيانات الأولية، مع تقديم التفسيرات أو المعادلات التي توضح كيفية استخلاص البيانات أو احتسابها.

المبدأ الخامس: عدم التمييز

يجب إتاحة مجموعات البيانات للجميع دون تمييز ودون حاجة للتسجيل – يكون بإمكان أي شخص الوصول إلى البيانات المفتوحة المنشورة في أي وقت دون الحاجة إلى التحقق من الهوية أو تقديم مسوغ للوصول إليها.

المبدأ السادس: بدون مقابل مالي

يجب إتاحة البيانات المفتوحة للجميع مجاناً.

المبدأ السابع: ترخيص البيانات المفتوحة في المملكة

تخضع البيانات المفتوحة لترخيص يحدد الأساس النظامي لاستخدام البيانات المفتوحة وكذلك الشروط والالتزامات والقيود المفروضة على المستخدم. كما يدل استخدام البيانات المفتوحة على قبول شروط الترخيص.

المبدأ الثامن: تطوير نموذج الحوكمة وإشراك الجميع

تمكّن البيانات المفتوحة عملية الاطلاع والمشاركة للجميع، وتعزز شفافية ومساءلة الجهات العامة ودعم عملية صنع القرار وتقديم الخدمات.

المبدأ التاسع: التنمية الشاملة والابتكار

من المفترض أن تلعب الجهات دوراً فعالاً في تعزيز إعادة استخدام البيانات المفتوحة وتوفير الموارد والخبرات اللازمة الداعمة، ويجب على الجهات أن تعمل بتكامل بين الاطراف المعنية على تمكين الجيل القادم من المبتكرين في مجال البيانات المفتوحة وإشراك الافراد والمؤسسات والجميع بوجه عام في إطلاق قدرات البيانات المفتوحة.

٢-٨ تقييم قيمة البيانات العامة لتحديد مجموعات البيانات المفتوحة

تعمل جامعة الامام عبد الرحمن بن فيصل على تقييم قيمة البيانات لتمكين نشر أكبر قدر ممكن من البيانات المفتوحة وذلك عبر الخطوات التالية:

الخطوة الأولى: تحديد البيانات والمعلومات العامة

لتقييم قيمة البيانات، يجب على الجامعة متمثلة في مكتب ادارة البيانات بتصنيف البيانات (وفقاً لسياسة تصنيف البيانات) وتحديد جميع مجموعات البيانات التي يمكن تصنيفها على المستوى" عام" والتي قد تتكون من ملفات أو جداول أو سجلات محددة ضمن قاعدة بيانات، ... إلخ. بعد ذلك، يجب تحديد الفوائد والتطبيقات والاستخدامات الممكنة لكل مجموعة من مجموعات البيانات. ويمكن الاخذ بعين الاعتبار مجال البيانات أو القطاع او مصدر البيانات عند تحليل حالات الاستخدام المحتملة، ايضا يمكن الاخذ بعين

الاعتبار مصادر البيانات: بيانات تم جمعها عن طريق المستخدمين بشكل مباشر، بيانات تم جمعها آلياً عن طريق سجلات الاحداث مثل التعاملات الالكترونية، بيانات مجمعة أو بيانات تم تطوريها من بيانات أخرى ... إلخ

الخطوة الثانية: تقييم الفائدة من البيانات

بعد تحديد مجموعات البيانات في الخطوة السابقة، يتم دراسة العوامل الرئيسة المتعلقة بفائدة البيانات والتي تلعب دورا رئيسياً في تقييم قيمتها، ومنها اكتمال البيانات، دقتها، تناسقها، حداثتها، القيود المفروضة عليها، حصريتها للجهة، المخاطر المحتملة من نشرها إمكانية الوصول إليها ودمجها مع بيانات أخرى.

الخطوة الثالثة: تحديد ذوي المصلحة المحتملين

بعد تقييم الفائدة من البيانات في الخطوة السابقة، يتم تحديد جميع الجهات أو الاشخاص ذوي المصلحة المحتملين.

بعد الانتهاء من تقييم قيمة البيانات، يمكن البدء بمراحل دورة حياة البيانات المفتوحة حسب ما هو موضح ادناه:

٨-٣ القواعد العامة للبيانات المفتوحة

تحدد سياسة البيانات المفتوحة القواعد العامة والالتزامات التي يجب على الجامعة الامتثال لها خلال مراحل دورة حياة البيانات المفتوحة وتشمل:

- التخطيط للبيانات المفتوحة
- تحديد البيانات المفتوحة
- نشر البيانات المفتوحة
- تحديث البيانات المفتوحة
- متابعة أداء البيانات المفتوحة

التخطيط للبيانات المفتوحة

يجب على جامعة الامام عبد الرحمن بن فيصل متمثلة في مكتب ادارة البيانات:

١- تعيين مسؤول البيانات المفتوحة والمعلومات في مكتب ادارة البيانات وتتمثل مسؤوليته الاساسية في دعم التخطيط والتنفيذ وإعداد التقارير بشأن أجندة البيانات المفتوحة لدى الجامعة وبما يتماشى مع هذه السياسة.

٢- وضع خطة للبيانات المفتوحة، تتضمن ما يلي:

- الاهداف الاستراتيجية للبيانات المفتوحة على مستوى الجامعة
- تحديد مجموعات البيانات الخاصة بالجامعة المطلوب نشرها على المنصة الوطنية للبيانات المفتوحة وترتيب تلك المجموعات بحسب الأولوية.
- مؤشرات الأداء الرئيسية والأهداف المتعلقة بالبيانات المفتوحة بالنسبة للجامعة.
- منهجية ومعايير تحديد الاولوية
- احتياجات التدريب ذات الصلة بالبيانات المفتوحة
- الجداول الزمنية لنشر وتحديث البيانات المفتوحة.

٣- تطوير وتوثيق العمليات المطلوبة في جميع مراحل دورة حياة البيانات المفتوحة، ويشمل ذلك، على سبيل المثال لا الحصر:

- عمليات تحديد مجموعات البيانات العامة التي سيتم نشرها من جانب الجامعة.
- عمليات التحقق من التزام البيانات المفتوحة بالمتطلبات المتعلقة بأمن المعلومات وخصوصية البيانات الشخصية وجودة البيانات ومراجعة ذلك بشكل منتظم والتعامل مع المخاوف المتعلقة بذلك.
- عمليات ضمان نشر مجموعات البيانات وتحديثها بالصيغة المناسبة ووفق الجدول الزمني المحدد وضمان شموليتها وجودتها العالية وضمان استبعاد أي بيانات مقيدة.
- عمليات جمع الملاحظات وتحليل الأداء على مستوى الجامعة وتحسين التأثير العام للبيانات المفتوحة على الصعيد الوطني.

٤- ضمان مراجعة خطة البيانات المفتوحة وتحديثها بصفة دورية.

٥- تقديم تقرير سنوي لمكتب ادارة البيانات الوطنية حول خطة البيانات المفتوحة ومستوى التقدم في تحقيق أهداف البيانات المفتوحة المحددة في الخطة.

٦- تنظيم دورة تدريبية عن جميع ما يتعلق بالبيانات المفتوحة بدعم من مكتب ادارة البيانات المفتوحة أو بالتنسيق معه.

٧- . إطلاق حملات توعية لضمان معرفة المستخدمين المحتملين بتوافر البيانات المفتوحة المنشورة من جانب الجامعة وطبيعتها وجودتها.

تحديد البيانات المفتوحة

١- تحديد جميع البيانات المصنفة على أنها بيانات عامة بصفة منتظمة وتقييم مدى أولوية كل مجموعة من مجموعات البيانات المحددة لنشرها كبيانات مفتوحة.

٢- تقدير قيمة مجموعة البيانات وتحديد مدى أولوية نشرها بمجرد استلام طلب النشر أو حينما يُلغى تصنيف أي مجموعة بيانات باعتبارها مقيدة وتصنيفها كمجموعة بيانات عامة.

٣- تسجيل البيانات الوصفية Metadata لمجموعات البيانات المفتوحة المحددة ونشرها.

٤- دراسة ما إذا كان الجمع بين عدة مجموعات من البيانات المفتوحة سيؤدي إلى رفع مستوى تصنيف البيانات إلى بيانات محمية.

نشر البيانات المفتوحة

١- يجب على الجامعة نشر مجموعات البيانات المفتوحة الخاصة بها على المنصة الوطنية للبيانات المفتوحة.

٢- التأكد من نشر البيانات بصيغ معيارية موحدة وهيكلة مقروءة آليا وغير مسجلة الملكية، تشمل على سبيل المثال (CSV، JSON، XML،RDF) ويجب أن تكون ملفات مجموعات البيانات مصحوبة بالوثائق ذات الصلة بالصيغة والتعليمات المتعلقة بكيفية استخدامها.

٣- توفير البيانات بعدة صيغ كلما أمكن.

تحديث البيانات المفتوحة

يجب على الجامعة:

١- ضمان تحديث جميع مجموعات البيانات المفتوحة المنشورة بصفة منتظمة بحسب الالية المحددة في البيانات الوصفية.

٢- المراجعة المستمرة لمجموعات البيانات المنشورة لضمان استيفائها للمتطلبات التنظيمية المحددة.

٣- ضمان تحديث البيانات الوصفية وخاصة تحديثها كلما تغيرت عناصر البيانات في مجموعات البيانات المفتوحة المنشورة.

٤- الحفاظ على إمكانية تتبع البيانات من خلال توثيق مصادر البيانات والحفاظ على سجل إصدارات مجموعة البيانات.

٥- نشر مجموعات البيانات المفتوحة مع تحديد القيود المتعلقة بالجودة وتوثيقها في البيانات الوصفية.

متابعة أداء البيانات المفتوحة

يجب على جامعة الامام عبد الرحمن بن فيصل:

١- تحليل حجم الطلب على البيانات المفتوحة ومعدل استخدامها لفهم حجم الطلب العام وإعادة ترتيب مجموعات البيانات بحسب الأولوية وفقاً لذلك.

٢- جمع طلبات المستخدمين المقدمة بصورة مباشرة أو من خلال المنصة الوطنية للبيانات المفتوحة لنشر مجموعات بيانات إضافية وتحليل تلك الطلبات والرد عليها في حينها.

٨-٤ الادوار والمسؤوليات فيما يخص البيانات المفتوحة

تتمثل المسؤولية الاساسية لجامعة الإمام عبد الرحمن بن فيصل في ضمان نشر بياناتها المفتوحة وفقاً لسياسة البيانات المفتوحة. وبالتالي، يجب على الجامعة تعيين من يتولون مسؤولية تنفيذ الانشطة المتعلقة بالبيانات المفتوحة على النحو المنصوص عليه ويتحمل مدير مكتب ادارة البيانات بالجامعة ومسؤول البيانات المفتوحة والمعلومات المسؤولية الاساسية المتعلقة بأنشطة البيانات المفتوحة لدى الجامعة.

مسؤوليات معالي رئيس جامعة الامام عبد الرحمن بن فيصل:

يعد معالي رئيس الجامعة - أو من يفوضه - هو الشخص المسؤول عن الممارسات المتعلقة بالبيانات المفتوحة داخل الجامعة، وتشمل مسؤولياته:

- **اعتماد خطة البيانات المفتوحة:** الموافقة على تنفيذ خطة البيانات المفتوحة لدى الجامعة والاشراف عليها.
- **تخصيص الادوار المتعلقة بالبيانات المفتوحة:** تخصيص الادوار المختلفة المتعلقة بالبيانات المفتوحة.
- **اعتماد التقرير السنوي للبيانات المفتوحة:** اعتماد التقرير السنوي للبيانات المفتوحة الذي يُعدّه مدير مكتب ادارة البيانات.

مسؤوليات مدير مكتب ادارة البيانات بجامعة الامام عبد الرحمن بن فيصل:

يعتبر المدير الاستراتيجي للعمليات المتعلقة بالبيانات المفتوحة في الجامعة، وتتضمن مسؤولياته ما يلي:

- **التخطيط الاستراتيجي للبيانات المفتوحة:** الاشراف على وضع خطة البيانات المفتوحة وتقديمها إلى رئيس الجامعة. كما يتولى مراجعة أداء البيانات المفتوحة وتحديد فرص التحسين والاسترشاد بذلك في خطة البيانات المفتوحة.
- **الإشراف على البيانات المفتوحة:** مراجعة أنشطة تحديد البيانات المفتوحة وترتيبها بحسب الأولوية والموافقة على نشرها وضمان تنفيذ أنشطة تحديثها.
- **الامتثال لسياسة البيانات المفتوحة:** ضمان امتثال أنشطة البيانات المفتوحة لدى الجهة للسياسات الوطنية المتعلقة بالبيانات، ويشمل ذلك على سبيل المثال: تصنيف البيانات وحماية خصوصية البيانات الشخصية وحرية المعلومات.

- **التنسيق مع مكتب ادارة البيانات الوطنية**: يعد مدير مكتب ادارة البيانات المنسق الأول بين الجامعة ومكتب ادارة البيانات الوطنية فيما يتعلق بالبيانات المفتوحة. ويتولى حل المشاكل المتعلقة بالبيانات المفتوحة بالنسبة للجامعة وتصعيدها إلى مكتب ادارة البيانات الوطنية إذا لزم الأمر.

مسؤول البيانات المفتوحة والمعلومات:

هو المدير التشغيلي للبيانات المفتوحة داخل الجامعة وتشمل مسؤولياته:

- **التخطيط للبيانات المفتوحة**: وضع خطة البيانات المفتوحة، بما في ذلك منهجية تحديد البيانات المفتوحة ذات الأولوية ووضع الأهداف ومؤشرات الأداء الرئيسية التي سيتم الاتفاق عليها مع مدير مكتب ادارة البيانات بالجامعة ورئيس الجامعة .
- **إدارة البيانات المفتوحة:** إدارة أنشطة البيانات المفتوحة داخل الجهة، وعلى وجه التحديد:
  - تحديد البيانات المفتوحة
  - ترتيب مجموعات البيانات بحسب أولوية النشر
  - إعداد مجموعات البيانات للنشر وتوثيق البيانات الوصفية
  - نشر مجموعات البيانات المفتوحة على المنصة الوطنية للبيانات المفتوحة
  - تحديث مجموعات البيانات المنشورة وصيانتها ومراجعة جودتها.
- **جمع طلبات البيانات المفتوحة:** مراجعة الملاحظات على البيانات المفتوحة ذات الصلة بالجامعة وتسجيل وتحليل طلبات نشر البيانات المحددة كبيانات مفتوحة.
- **التثقيف والتوعية بالبيانات المفتوحة:** تثقيف موظفي الجهة وتوعيتهم بشأن البيانات المفتوحة ودعم حملات التوعية الوطنية بالتنسيق مع مدير مكتب ادارة البيانات.
- **التنسيق مع مكتب ادارة البيانات الوطنية (بشكل ثانوي):** يقوم مسؤول البيانات المفتوحة والمعلوماتٍ بالتنسيق مع المكتب عند الحاجة كمستوى ثان.

ممثل بيانات أعمال:

يتولى المسؤوليات التالية:

- **التصديق على خطة البيانات المفتوحة:** المساهمة في تطوير خطة البيانات المفتوحة وإدارة الفرق المسؤولة عن تنفيذ الخطة بالتنسيق مع مسؤول البيانات المفتوحة والمعلومات.

- **تحديد أولوية البيانات المفتوحة:** تقديم المشورة إلى مسؤول البيانات المفتوحة والمعلومات بشأن قيمة مجموعات البيانات العامة والاستثمارات المطلوبة لنشرها وتحديثها.
- **مراجعة مجموعات البيانات واعتمادها:** مراجعة مجموعات البيانات واعتمادها للتأكد من استيفائها للمواصفات المحددة في اللائحة من حيث الجودة والكمال وتوثيق البيانات الوصفية قبل تقديمها للنشر.

مختص بيانات الأعمال:

يعد أحد أفراد فريق ممثلي بيانات الأعمال المسؤول عن:

- **تحديد مجموعات البيانات المفتوحة:** يتولى مختص بيانات الأعمال مراجعة وتحديد البيانات التي يتم إنشاؤها ومعالجتها من قبل الإدارة التي يعمل فيها بصفة منتظمة وتصنيفها بصفتها بيانات عامة إذا لزم الأمر.
- **إعداد مجموعات البيانات المفتوحة:** إعداد مجموعات البيانات المفتوحة التي سيتم نشرها لضمان استيفائها للمواصفات المحددة في السياسة من حيث الجودة والكمال وتوثيق البيانات الوصفية قبل تقديمها للنشر.
- **تحديث مجموعات البيانات المفتوحة:** تحديث مجموعات البيانات المفتوحة المنشورة والبيانات الوصفية ذات الصلة.

٨-٥ الامتثال

يقوم مكتب ادارة البيانات الوطنية – بصفته الجهة التنظيمية للبيانات الوطنية – بمراقبة الامتثال لسياسة البيانات المفتوحة بدعم من مكتب ادارة البيانات بجامعة الامام عبد الرحمن بن فيصل.

شروط الامتثال:

١- يجب على جامعة الامام عبد الرحمن بن فيصل الالتزام بسياسة البيانات المفتوحة وتقديم تقرير سنوي إلى مكتب ادارة البيانات الوطنية يشمل، على سبيل المثال، ما يلي:

- التقدم ومستوى الإنجاز الذي حققته الجامعة في خطتها المحددة
- الأهداف ومؤشرات الأداء الرئيسة المحددة في خطة البيانات المفتوحة
- عدد مجموعات البيانات المفتوحة المحددة
- عدد مجموعات البيانات المفتوحة المنشورة

٢- تقوم الجامعة – بعد التنسيق مع مكتب ادارة البيانات الوطنية – بإعداد الاليات والاجراءات والضوابط المتعلقة بتسوية النزاعات المتعلقة بالبيانات المفتوحة وفقاً لاطار زمني محدد وحسب التسلسل التنظيمي.

٣- يقوم مكتب ادارة البيانات الوطنية بمراجعة التقارير السنوية التي تم إعدادها من قبل جامعة الامام عبد الرحمن بن فيصل حول الامتثال العام بسياسة البيانات المفتوحة ومشاركتها مع الجهات ذات العلاقة.

٤- يقوم المكتب بإجراء عمليات التدقيق بشكل دوري أو عشوائي للتحقق من امتثال الجهة العامة ومراجعة القرارات المتعلقة بنشر البيانات أو رفض نشرها واتخاذ ما يلزم من إجراءات بهذا الخصوص.

٨-٦ التعامل مع حالات عدم الامتثال

عند مراجعة حالات عدم الامتثال، يقوم مكتب ادارة البيانات الوطنية باتباع منهجية تدريجية لتحليل سبب عدم الامتثال ومدى الاثار والمخاطر المترتبة على ذلك، والتعامل مع هذه الحالات وفقاً للمستويات التالية:

التوعية يقوم المكتب باستخدام التوعية عند التعامل مع حالات عدم الامتثال العرضية أو غير المقصودة ذات الاثار السلبية المحدودة جداً.

التعاون يقوم المكتب بالتعاون مع الجامعة لمنع أو ردع أو معالجة حالات عدم الامتثال ذات الاثار السلبية المحدودة الناجمة عن الاهمال وعدم الامتثال بأحكام وقواعد هذه السياسة.

التدخل المباشر يقوم المكتب بالتحقيق في حالات عدم الامتثال المستمرة والمتكررة أو المتعمدة أو ذات الاثار السلبية الشديدة واتخاذ القرارات التي تتناسب مع حجم وطبيعة الاثار السلبية.

٩. السياسة السادسة: سياسة حماية البيانات الشخصية للأطفال ومن في حكمهم

تتضمن الحقوق والقواعد العامة التي يجب على جامعة الإمام عبد الرحمن بن فيصل مراعاتها و الالتزام بها للحد من الممارسات الخاطئة المتعلقة بمعالجة البيانات الشخصية للأطفال ومن في حكمهم وضمان حمايتهم من الآثار السلبية والمخاطر المحتملة، بالإضافة إلى المحافظة على خصوصيتهم وحماية حقوقهم.

تنطبق أحكام هذه السياسة على جميع الجهات في القطاعين العام والخاص وكذلك الجهات غير الربحية التي تقوم بجمع ومعالجة البيانات الشخصية للأطفال ومن في حكمهم بشكل كلي أو جزئي وبأي وسيلة سواء أكانت يدوية أو إلكترونية. كما تنطبق أحكام هذه السياسة على جميع الجهات – خارج المملكة – التي تقوم بجمع البيانات الشخصية للأطفال ومن في حكمهم المقيمين في المملكة عن طريق شبكة الإنترنت.

٩-١ حقوق الطفل ومن في حكمه فيما يتعلق بمعالجة بياناته الشخصية

يتمتع الطفل ومن في حكمه بجميع حقوق صاحب البيانات المنصوص عليها في سياسة حماية البيانات الشخصية الصادرة من مكتب ادارة البيانات الوطنية، ويتم ممارسة هذه الحقوق من قبل الولي. كما يحق للطفل ومن في حكمه طلب إتلاف بياناته الشخصية بعد بلوغه السن النظامية أو انتهاء الولاية في حال كانت الموافقة على جمع ومعالجة بياناته الشخصية مقدمة من قبل الولي.

٩-٢ القواعد العامة

دون اخلال بالقواعد العامة المنصوص عليها في سياسة حماية البيانات الشخصية، تلتزم جامعة الإمام عبد الرحمن بن فيصل بالقواعد الإضافية التالية التي تضمن المحافظة على خصوصية الاطفال ومن في حكمهم وحماية حقوقهم:

١- أن تكون جامعة الامام عبد الرحمن بن فيصل مسؤولة عن إعداد وتطبيق السياسات والاجراءات المتعلقة بحماية البيانات الشخصية للأطفال ومن في حكمهم، ويكون معالي رئيس الجامعة – أو من يفوضه – مسؤولاً عن الموافقة عليها واعتمادها.

٢- تلتزم الجامعة بتقييم الاثار السلبية والمخاطر المحتملة المترتبة على جميع أنشطة معالجة البيانات الشخصية للأطفال ومن في حكمهم، مع الاخذ بعين الاعتبار مصالحهم وحقوقهم وجميع ما يتعلق بأحوال أسرهم، وعرض نتائج التقييم على معالي رئيس الجامعة – أو من يفوضه – لتحديد مستوى قبول المخاطر وإقرارها.

٣- تلتزم جامعة الامام عبد الرحمن بن فيصل بمراجعة وتحديث العقود واتفاقيات مستوى الخدمة والتشغيل بما يتوافق مع السياسات والاجراءات المتعلقة بحماية البيانات الشخصية للأطفال ومن في حكمهم المعتمدة من الادارة العليا للجهة.

٤- تلتزم جامعة الامام عبد الرحمن بن فيصل بإعداد وتوثيق الاجراءات اللازمة لإدارة ومعالجة انتهاكات الخصوصية المتعلقة بالأطفال ومن في حكمهم وتحديد المهام والمسؤوليات المتعلقة بفريق العمل المختص، والحالات التي يتم بها إشعار الجهة التنظيمية والمكتب حسب التسلسل الإداري بناء على قياس شدة الأثر.

٥- تلتزم جامعة الامام عبد الرحمن بن فيصل بإعداد برامج توعوية لتعزيز ثقافة الخصوصية ورفع مستوى الوعي فيما يتعلق بجمع ومعالجة البيانات الشخصية للأطفال ومن في حكمهم.

٦- تلتزم جامعة الامام عبد الرحمن بن فيصل بإعداد وتطوير إشعار الخصوصية بشكل واضح ودقيق وبلغة تناسب هذه الفئة ونشره على الموقع الالكتروني أو التطبيق الخاص (حسب الدليل الارشادي لتطوير إشعار الخصوصية الصادر من مكتب ادارة البيانات الوطنية) وإشعار الولي – بطريقة تناسب وقت جمع البيانات – بالغرض و الاساس النظامي أو الاحتياج الفعلي والوسائل والطرق المستخدمة لجمع ومعالجة ومشاركة البيانات الشخصية للأطفال ومن في حكمهم وكذلك كيفية ممارسة الحقوق، والتدابير الامنية لحماية خصوصيتهم، وأي تغييرات جوهرية تطرأ عليه

٧- تلتزم جامعة الامام عبد الرحمن بن فيصل بإشعار الولي عن المصادر الاخرى التي يتم استخدامها في حال تم جمع بيانات إضافية بطريقة غير مباشرة (من جهات أخرى).

٨- تلتزم الجامعة بتزويد الولي بالخيارات المتاحة فيما يتعلق بمعالجة البيانات الشخصية للأطفال ومن في حكمهم والآلية المستخدمة لممارسة هذه الخيارات، ومنها على سبيل المثال، التفضيلات الشخصية التي من خلالها يمكن التعبير عن الرغبة في مدى مشاركة بياناتهم لأغراض أخرى.

٩- تلتزم الجامعة بتبني مفهوم الخصوصية بالتصميم وبشكل افتراضي – يضمن مستوى الحماية دون تدخل مباشر من الطفل أو من في حكمه – عند تقديم الخدمات التي تستهدف هذه الفئة على وجه التحديد.

١٠- تلتزم جامعة الامام عبد الرحمن بن فيصل بأخذ موافقة الولي – التي يمكن التحقق منها بعد بذل الجهود المعقولة – على معالجة البيانات الشخصية للأطفال ومن في حكمهم بعد تحديد نوع الموافقة (صريحة أو ضمنية) بناءً على طبيعة البيانات وطرق جمعها.

١١- أن يكون الغرض من جمع البيانات الشخصية للأطفال ومن في حكمهم متوافقا مع الأنظمة ذات الصلة وذو علاقة مباشرة بنشاط جهة التحكم.

١٢- أن يكون محتوى البيانات مقتصرا على الحد الأدنى من البيانات اللازمة لتحقيق الغرض من جمعها.

١٣- أن يتم تقييد جمع البيانات الشخصية للأطفال ومن في حكمهم على المحتوى المعدّ سلفا (الموضح في القاعدة ١٢) ويكون بطريقة عادلة (مباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التضليل).

١٤- أن يقتصر استخدام البيانات على الغرض التي جُمعت من أجله والذي تمت الموافقة عليه من قبل الولي.

١٥- تلتزم الجامعة بإعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات الشخصية للأطفال ومن في حكمهم وفقاً للأغراض المحددة والانظمة والتشريعات ذات العلاقة.

١٦- تلتزم الجامعة بتخزين البيانات الشخصية للأطفال ومن في حكمهم ومعالجتها داخل الحدود الجغرافية للمملكة لضمان المحافظة على السيادة الوطنية على هذه البيانات، ولا يجوز معالجتها خارج المملكة إلاّ بعد حصول الجامعة على موافقة كتابية من الجهة التنظيمية (وفقاً للقواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة) بعد تنسيق الجهة التنظيمية مع مكتب ادارة البيانات الوطنية متى ما استدعى الأمر ذلك.

١٧- تلتزم 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 وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني.

١٨- تلتزم الجامعة بتضمين أحكام سياستي الاحتفاظ والتخلص من البيانات في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.

١٩- تلتزم الجامعة بتحديد وتوفير الوسائل التي من خلالها يمكن للولي الوصول إلى البيانات الشخصية للطفل ومن في حكمه وذلك لمراجعتها وتحديثها.

٢٠- تلتزم الجامعة بالتحقق من هوية الولي قبل منحه الوصول إلى بيانات الطفل الشخصية ومن في حكمه وفقاً للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.

٢١- يحظر مشاركة البيانات الشخصية للأطفال ومن في حكمهم مع جهات أخرى الا وفقا للأغراض المحددة بعد موافقة الولي ووفقاً للأنظمة واللوائح والسياسات ذات الصلة على أن يتم تزويد الجهات الأخرى بالسياسات والإجراءات المتعلقة بحماية البيانات الشخصية للأطفال ومن في حكمهم وتضمينها في العقود والاتفاقيات.

٢٢- تلتزم الجامعة بإشعار الولي وأخذ الموافقة منه في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الأغراض المحددة.

٢٣- تلتزم الجامعة بإشعار الولي في حال الرغبة في التواصل مع الطفل أو من في حكمه بطريقة مباشرة لأي غرض كان وإتاحة الفرصة له لرفض هذا التواصل مع إيضاح كيفية قيامه بذلك.

٢٤- تلتزم الجامعة بأخذ موافقة مكتب ادارة البيانات الوطنية – بعد التنسيق مع الجهة التنظيمية – قبل مشاركة البيانات الشخصية للأطفال ومن في حكمهم مع جهات أخرى خارج المملكة.

٢٥- يحظر على الجامعة جمع بيانات شخصية من الطفل أو من في حكمه تتعلق بأحد أفراد أسرته في أي حال من الأحوال، ماعدا البيانات الشخصية للولي.

٢٦- تلتزم الجامعة بمتطلبات حماية خصوصية الأطفال ومن في حكمهم منذ المراحل الأولى من تصميم الخدمات والمنتجات التي تستهدف هذه الفئة، بما في ذلك المواقع الإلكترونية أو التطبيقات الرقمية.

٢٧- تلتزم الجامعة بتطبيق التدابير المناسبة التي تمنع الأطفال ومن في حكمهم من إتاحة بياناتهم الشخصية والحساسة للجمهور بطريقة يمكن من خلالها التعرف عليهم وعلى أسرهم بشكل مباشر.

٢٨- تلتزم الجامعة بتطبيق التدابير المناسبة والممكنة عملياً في حدود المعقول لحذف البيانات الشخصية والحساسة من منشورات الطفل ومن في حكمه قبل نشرها، بما في ذلك عرض الملفات الشخصية والنشر عبر حسابات التواصل الاجتماعي.

٢٩- تلتزم جامعة الامام عبد الرحمن بن فيصل بعدم اتخاذ قرارات آلية بناء على معالجة البيانات الشخصية للأطفال ومن في حكمهم واستخدامها لأغراض متعددة لها تأثير كبير عليهم، ومنها على سبيل المثال التسويق المباشر.

٣٠- تلتزم الجامعة باستخدام الضوابط الإدارية والتدابير التقنية والضمانات القانونية الكافية لحماية البيانات الشخصية للأطفال ومن في حكمهم.

٣١- تلتزم الجامعة بمراقبة الامتثال للسياسات والإجراءات المتعلقة بحماية البيانات الشخصية للأطفال ومن في حكمهم 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 والمكتب حسب التسلسل التنظيمي.

٩-٣ الاستثناءات

١- لا يشترط الحصول على موافقة الولي في حال كانت الخدمة المقدمة للطفل أو من في حكمه هي خدمة وقائية أو استشارية وفقاً لمهام واختصاصات الجامعة، على أن تلتزم الجامعة بجمع الحد الأدنى من البيانات اللازمة لتحقيق الغرض، وإتلافها فور الانتهاء من تقديم الخدمة.

٢- لا يشترط الحصول على موافقة الولي في حال الإفصاح عن بياناته الشخصية لطرف ثالث من أجل تنفيذ التزام مشروع على الجامعة أو لتنفيذ نظام آخر أو لتنفيذ اتفاقية تكون المملكة طرفاً فيه أو كانت الجهة التي سيتم الإفصاح لها جهة قضائية أو أمنية.

٣- لا يشترط الحصول على موافقة الولي عندما يكون الغرض الوحيد من جمع بيانات الاتصال بالطفل أو من في حكمه هو الرد مباشرة على طلب محدد من الطفل ومن في حكمه، ولا تستخدم هذه البيانات بمعاودة الاتصال به مرّه اخرى او لاي غرض اخر، ولا يتم الافصاح عنها، وتقوم الجامعة بحذفها من سجلاتها فور الاستجابة لطلب الطفل.

٤- لا يشترط الحصول على موافقة الولي عندما يكون الغرض من جمع بيانات الاتصال للولي والطفل ومن في حكمه هو الاستجابة مباشرة – مرة أو أكثر – لطلب الطفل ومن في حكمه المحدد، ولا يتم استخدام هذه البيانات لأي غرض آخر، ولا يتم الإفصاح عنها، أو دمجها مع أي بيانات أخرى، ويتم تزويد الولي بإشعار بذلك.

٥- لا يشترط الحصول على موافقة الولي عندما يكون الغرض من جمع اسم الطفل ومن في حكمه واسم الولي وبيانات الاتصال هو حماية سلامة الطفل ومن في حكمه، ولا يتم استخدام هذه البيانات أو الكشف عنها لأي غرض لا علاقة له بسلامة الطفل ومن في حكمه، ويجب على الجامعة تزويد الولي بإشعار بذلك.

٩-٤ أحكام عامة

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

ثانياً: تلتزم الجامعة بمراقبة وتوثيق الامتثال لهذه السياسة بشكل دوري.

ثالثاً: تلتـزم الجامعة بالامتثال لهـذه السياسـة وتوثيـق الامتثال وفقـاً للآليات والاجراءات التـي تحددهـا الجهـات التنظيميـة.

رابعاً: تلتـزم الجامعة بإبلاغ الجهـات التنظيميـة فـوراً ودون تأخيـر وبمـا لا يتجـاوز (٧٢) سـاعة مـن وقـوع أو اكتشـاف أي حادثـة تسـريب للبيانـات الشـخصية وفقـاً للآليات والإجراءات التـي تحددهـا الجهـات التنظيميـة.

خامساً: تلتـزم الجامعة عنـد تعاقدهـا مـع جهـات معالجـة أخـرى بـأن تتحقق بشـكل دوري مـن امتثـال الجهـات الأخرى لهـذه السياسـة وفقـاً للآليات والاجراءات التـي تحددهـا الجهـة التنظيميـة، علـى أن يشـمل ذلـك أي تعاقـدات لاحقة تقـوم بهـا الجهـة.

سادساً: يحـق للجهـة التنظيميـة وضـع قواعـد إضافيـة لمعالجـة أنـواع محـددة مـن البيانـات الشـخصية للأطفال ومـن فـي حكمهـم وفقـاً لطبيعـة وحساسـية هـذه البيانـات بعـد التنسـيق مـع المكتـب.

سابعاً: تلتـزم الجهـة التنظيميـة – بعـد التنسـيق مـع المكتـب – بإعـداد الآليات والاجراءات التـي تنظـم عمليـة معالجـة الشكاوى والاعتراضات وفقـاً لإطار زمنـي محـدد وحسـب التسلسـل التنظيمـي للجهـات.

٩-٥ الأحكام الخاصة المتعلقة بالولي الشرعي

١- يجـوز للجامعة أن تحصـل علـى البيانـات الشـخصية للولـي مـن الطفـل ومـن فـي حكمـه مباشـرة، علـى أن تلتـزم بالحصـول علـى الحـد الأدنى مـن البيانـات اللازمة – الاسم وطريقـة التواصـل مـع الولـي – فقـط مـن أجـل إشـعار الولـي والحصـول علـى موافقتـه.

٢- تلتـزم الجامعة باسـتخدام الوسـائل المناسـبة للتحقـق مـن هويـة الولـي قبـل أخـذ موافقتـه ومنحـه الوصـول إلـى بيانـات الطفـل الشـخصية ومـن فـي حكمـه وفقـاً للضوابـط المعتمـدة مـن قبـل الهيئـة الوطنيـة للأمن السـيبراني والجهـات ذات الاختصاص.

٣- فـي حـال تـم طلـب موافقـة الولـي ولـم يقـدم موافقتـه خلال (١٠) أيـام مـن تاريـخ التواصـل معـه، تلتـزم الجامعة بإتلاف بيانـات الطفـل الشـخصية ومـن فـي حكمـه وبيانـات الولـي التـي جمعـت.

٤- تلتـزم جهـة التحكم بعـدم اسـتخدام البيانـات الشـخصية للولـي لغيـر الغـرض الـذي جمعـت مـن أجلـه فـي حـدود الموافقـة علـى جمـع ومعالجـة البيانـات الشـخصية للطفـل ومـن فـي حكمـه.

٥- تلتـزم الجامعة بإشـعار الولـي بالطلبات المقدمـة مـن الطفـل ومـن فـي حكمـه فيمـا يتعلـق بالبيانـات الشـخصية لـه وأخـذ موافقتـه عليهـا.

١٠. القواعد العامة لنقل البيانات 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 الجامعة 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.

١٠-١ 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 الجامعة 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:

أولاً: 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 حماية للمصالح الحيوية للأفراد، أو تنفيذاً لمتطلبات نظامية.

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

١٠-٢ التزامات جامعة الإمام عبد الرحمن بن فيصل فيما يخص نقل البيانات خارج الحدود الجغرافية للمملكة

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 إلاّ بعد التحقق من الحالات الموضحة أدناه حسب التسلسل التالي:

١- إذا كانت جهة المعالجة الخارجية المسند إليها أنشطة معالجة البيانات الشخصية في دولة ضمن قائمة الاعتماد، فتقوم الجامعة/ جهة المعالجة الداخلية بأخذ موافقة كتابية من الجهة التنظيمية على نقل البيانات، وعلى الجهة التنظيمية التنسيق مع مكتب ادارة البيانات الوطنية.

٢- إذا كانت جهة المعالجة الخارجية في دولة ليست ضمن قائمة الاعتماد، فإن نقل البيانات الشخصية خارج الحدود الجغرافية للمملكة يتطلب مستوى كاف 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.

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

٤- 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 (٢) و (٣) و (٤) أعلاه، يجب على جامعة الإمام عبد الرحمن بن فيصل أو المعالجة الداخلية الحصول على موافقة كتابية من الجهة التنظيمية على نقل البيانات، وعلى الجهة التنظيمية التنسيق مع المكتب.

أولاً: تقييم مستوى الحماية:

يجب أن تقوم الجهة التي ترغب بنقل البيانات خارج الحدود الوطنية بإجراء تقييم الآثار والمخاطر المحتملة – كل حالة على حدة – لتحديد ما إذا كانت الجامعة/جهة المعالجة الخارجية ستوفر مستوى كاف من الحماية لحقوق أصحاب البيانات وعرض نتائج التقييم على(معالي رئيس الجامعة) لتحديد مستوى قبول المخاطر وإقرارها. وللقيام بذلك يجب أن تقوم الجهة بالالتزام بمعايير التقييم سواء المعايير العامة أو القانونية وذلك لضمان أن يكون مستوى الحماية ملائما 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 عالٍ من الحماية.

- **الغرض من معالجة البيانات**: يجب على الجهة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار الغرض من المعالجة والفئة المستهدفة من أصحاب البيانات ونطاق المعالجة والجهات التي سيتم مشاركة البيانات معها، حيث إن معالجة بيانات شخصية حساسة على نطاق واسع يتطلب مستوى عالٍ 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 مقيد أو عرضي – لمرة واحدة فقط أو لفترة محدودة – أو ستتم بشكل متكرر ومنتظم، حيث إن البيانات الشخصية التي سيتم معالجتها بشكل منتظم وعلى المدى الطويل تتطلب مستوى عالٍ من الحماية.

- **منشأ البيانات**: يجب على الجامعة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار الدولة التي ُجمعت منها البيانات – ليس 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 – آخر مرحلة من مراحل النقل.

- **الضوابط الأمنية:** يجب على الجامعة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار الاجراءات الادارية 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 – بناء على المعايير القانونية – ضرورياً في هذه الحالة.

ب- **معايير التقييم القانونية:**

يجب أن تقوم الجهة التي ترغب 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 الجهة 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 الجهة 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 الجهة 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 ِ كاف، فيجب عليها توفير الضمانات المناسبة لحماية البيانات الشخصية، ومنها:

- **البنود التعاقدية القياسيّة**: يجب على الجهة أن تضمن 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 الجامعة وجهة المعالجة – كل على حدة – التي تعمل ضمن مجموعة متعددة الجنسيات أن تقوم بإعداد قواعد مشتركة داخلية ملزمة قانونياً تنطبق على عمليات نقل البيانات الشخصية خارج الحدود بما في ذلك معالجة انتهاكات الخصوصية والاشعار عنها على أن تتم الموافقة عليها من قبل مكتب ادارة البيانات الوطنية، ويتم تضمين هذه القواعد المشتركة بصفتها ملحقاً لاتفاقيات مستوى الخدمة أو العقود المبرمة بين الجهتين. كما يجب على الجامعة 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 الاحكام 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:

يمكن للجهات نقل البيانات الشخصية خارج الحدود الجغرافية دون الالتزام بالشروط و الأحكام الموضحة في البند (أولاً) والبند (ثانياً) أعلاه في حالات محددة، ومنها أن يكون نقل البيانات خارج الحدود الجغرافية للمملكة:

١- استناداً على موافقة أصحاب البيانات.
٢- تنفيذاً لالتزام تعاقدي ويكون صاحب البيانات طرفا فيه.
٣- تنفيذاً لمتطلبات قضائية.
٤- تنفيذاً لأحكام نظام آخر أو اتفاقية دولية تكون المملكة طرفا فيها.
٥- للمحافظة على المصلحة العامة بما في ذلك حماية الصحة أو السلامة العامة.
٦- لحماية المصالح الحيوية لأصحاب البيانات.

في جميع هذه الحالات الواردة في الفقرات (١)،(٢) ،(٣) ،(٤) ،(٥) يجب على الجامعة 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 (٦) فيجب على الجامعة أو جهة المعالجة إشعار الجهة التنظيمية فقط، وعلى الجهة التنظيمية إشعار المكتب بذلك.

١٠-٣ احكام عامة

١- يجب على جامعة الامام عبد الرحمن بن فيصل وجهات المعالجة الامتثال لهذه القواعد وتوثيق الامتثال وفقاً للآليات والاجراءات التي تحددها الجهات التنظيمية

٢- يجب على الجامعة 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.

٣- يمارس مكتب ادارة البيانات الوطنية أدوار الجهات التنظيمية ومهامها على الجامعة في حال كانت غير خاضعة لجهات تنظيمية.

٤- يحق للجهات التنظيمية وضع قواعد إضافية لنقل أنواع محددة من البيانات الشخصية وفقاً لطبيعة وحساسية هذه البيانات بعد التنسيق مع المكتب.

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

٦- يقوم مكتب ادارة البيانات الوطنية بوضع قائمة محددة للعوامل الرئيسة التي تحدد مستوى الحماية المناسب، ومنها على سبيل المثال، الأنظمة والتشريعات، حماية الحقوق والحريات، الأمن الوطني، قواعد حماية البيانات الشخصية، الجهة الإشرافية لحماية البيانات، الالتزامات الملزمة التي تعهدت بها الدولة.

٧- يقوم مكتب ادارة البيانات الوطنية بإعداد قائمة الاعتماد ومراجعتها ونشرها وتحديثها بشكل دوري وذلك بناء على تقييم مستوى الحماية المناسب بحيث لا يقلّ عن مستوى الحماية الذي كفلته سياسة حماية البيانات الشخصية الصادرة من المكتب.

٨- يقوم مكتب ادارة البيانات الوطنية بإعداد البنود القياسية ومراجعتها لحماية البيانات الشخصية.