NDMO
مكتب إدارة البيانات الوطنية
National Data Management Office

SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

سياسات حوكمة البيانات الوطنية

الأصدار الثاني
التاريخ 2021/05/26م


بسم الله الرحمن الرحيم

المحتويات

1.مقدمة

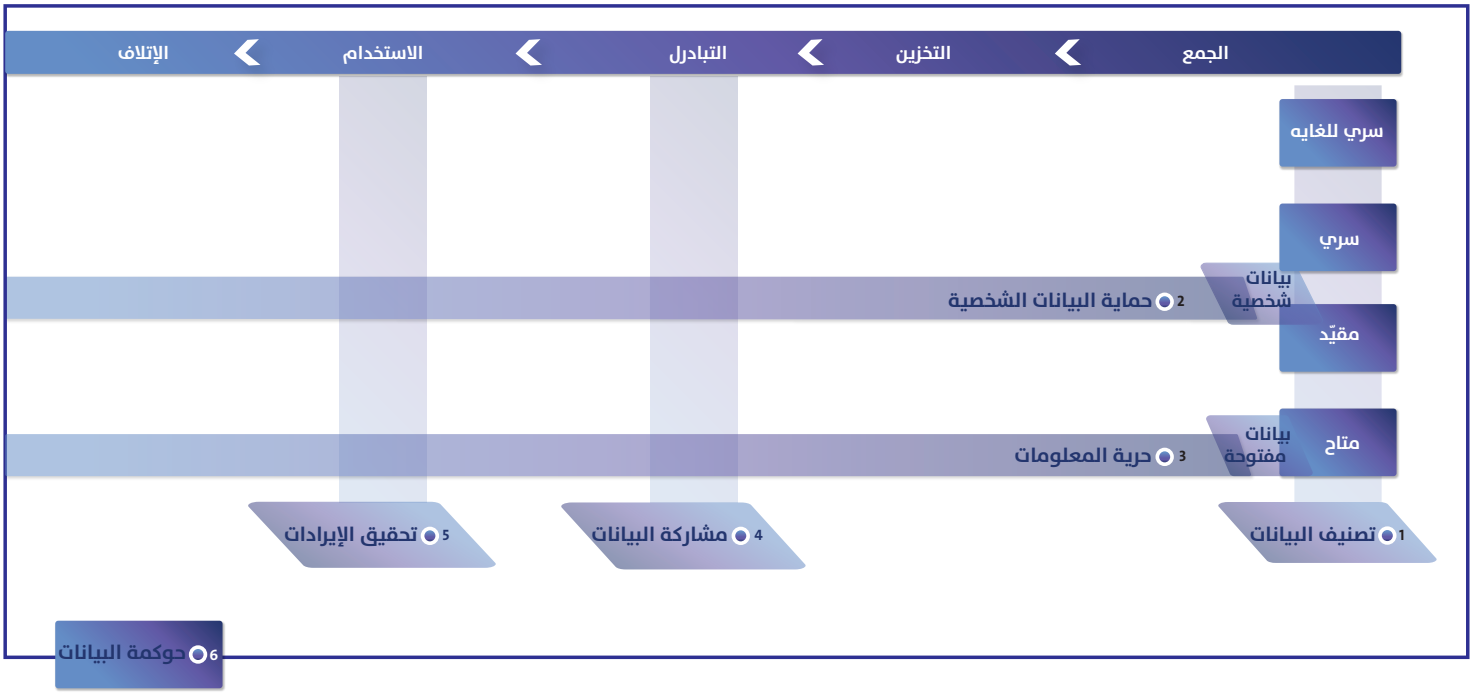
تمثل البيانات التي تنتجها الجهات الحكومية أو تتلقاها أو تتعامل معها أصولاً وطنية يمكن أن تساهم في تحسين الأداء والإنتاجية وتسهيل تقديم الخدمات العامة عن طريق دعم العمليات الفعالة لإدارة البيانات واتخاذ القرارات الاستراتيجية واستشراف المستقبل وتحقيق أعلى مستويات المسؤولية والشفافية، كما تسعى الدول في جميع أنحاء العالم إلى الاستفادة من قيمة البيانات باعتبارها مورداً اقتصادياً يساعد على الابتكار ويساهم في دعم التحولات الاقتصادية وتعزيز المقومات التنافسية للدول، وعلى المستوى الوطني، تقوم الجهات الحكومية بجمع ومعالجة كميات هائلة من البيانات يمكن الاستفادة منها للمساهمة في النمو الاقتصادي والارتقاء بالمملكة إلى الريادة ضمن الاقتصادات القائمة على البيانات.

ولضمان الاستفادة القصوى من هذه البيانات التي تشكّل جزءاً مهماً من الأصول الوطنية، فلابد من تعزيز مبدأ مشاركة البيانات لتحقيق التكامل بين الجهات الحكومية والحد من ازدواجية البيانات وتعارضها وتعدد مصادرها، وهذا يتطلب تصنيف البيانات إلى مستويات موحدة تساعد على تحقيق التوازن بين المزايا والمخاطر المترتّبة على مشاركة البيانات بين الجهات في القطاعين العام والخاص وكذلك القطاع الثالث، حيث يعتبر تصنيف البيانات حجر الزاوية لتنظيم عملية نشر البيانات المفتوحة، وإتاحة المعلومات العامة وتبادل البيانات المحمية بما في ذلك البيانات الشخصية، وهذا بدوره يساعد على رفع مستوى معايير الرقابة المجتمعية على أداء الجهات العامة وزيادة مستوى الشفافية وتعزيز النزاهة وإزالة السرية غير الضرورية عن أنشطة الجهات العامة عن طريق تنظيم ممارسة حق الاطلاع على المعلومات العامة أو الحصول عليها.

ومع التطوّر المطرد في التقنية وسهولة الحصول على البيانات ومشاركتها، تتضاعف أهمية المحافظة على خصوصية البيانات الشخصية مما دعا أغلب الدول إلى سن الأنظمة والتشريعات التي تنظم جمع ومعالجة ومشاركة البيانات الشخصية بما يضمن المحافظة على خصوصية أصحاب هذه البيانات وحماية حقوقهم، وكذلك المحافظة على السيادة الوطنية الرقمية على هذه البيانات.

وفي ظل الرؤية 2030 تسعى المملكة نحو عصر جديد يعزز أداء الجهات الحكومية ويزيد من مستوى شفافيتها ومسؤوليتها، ويشجع على تنويع الاقتصاد والاستفادة من الخدمات المعتمدة على البيانات، مما له دور فعّال في الاقتصاد العالمي الذي يقوم على الثقة والشراكات الدولية.

ومن هذا المنطلق، قام مكتب إدارة البيانات الوطنية – بصفته الجهة التنظيمية للبيانات الوطنية – بتطوير إطار مؤقت لحوكمة البيانات على المستوى الوطني يحدد السياسات الخاصة بتصنيف البيانات، ومشاركتها، وتنظيم جمع ومعالجة البيانات الشخصية، وكيفية ممارسة حق الاطلاع أو الحصول على المعلومات العامة لدى الجهات الحكومية، والبيانات المفتوحة لحين صدور الأنظمة والتشريعات المتعلقة بتصنيف البيانات، ومشاركة البيانات، وحماية البيانات الشخصية، وحرية المعلومات، ونظراً إلى هذه الأنظمة والتشريعات، فقد رأى المكتب دمج السياسات المتعلقة بها في وثيقة واحدة توضح مدى العلاقة والاعتمادية فيما بينها كما هو موضح في الشكل 1 أدناه.



الشكل 1 العلاقة بين الأنظمة والتشريعات والسياسات الخاصة بالبيانات

2. التعريفات

لأغراض تطبيق هذه السياسات، يُقصد بالكلمات والمصطلحات الواردة أدناه -أينما وردت في هذه الوثيقة - المعاني الموضحة أمام كل منها، ما لم يقتضِ سياق النص خلاف ذلك:

البيانات الشخصية:

كل بيان - مهما كان مصدره أو شكله - من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلاً للتعرف عليه بصفة مباشرة أو غير مباشرة عند دمجه مع بيانات أخرى، ويشمل ذلك -على سبيل المثال لا الحصر - الاسم، وأرقام الهويات الشخصية، والعناوين، وأرقام التواصل، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور المستخدم الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي.

البيانات:

مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظّمة مثل الأرقام أو الحروف أو الصور الثابتة أو الفيديو أو التسجيلات الصوتية أو الرموز التعبيرية.

الوصول إلى البيانات:

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

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.

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 غير مصرّح به نظاماً.

البيانات المحمية:

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

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.

مستويات تصنيف البيانات:

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

الفرد:

الشخص المتقدم بطلب الاطلاع أو الحصول على المعلومات العامة.

صاحب البيانات الشخصية:

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

معالجة البيانات الشخصية:

جميع العمليات التي 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.

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.

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.

الإفصاح عن البيانات الشخصية:

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

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.

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، و غالباً 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.

البيانات الوصفية:

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

البيانات المقروءة آلياً:

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

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.

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.

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.

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

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

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.

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.

مكتب الجهة:
مكتب إدارة البيانات والخصوصية في الجهة العامة.

المكتب:
مكتب إدارة البيانات الوطنية.

الطفل:
كل شخص لم يتجاوز الثامنة عشرة من عمره.

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.

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.

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.

الإفصاح عن البيانات:

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

نقل البيانات الشخصية:

إرسال البيانات الشخصية إلى جهة خارج الحدود الجغرافية للمملكة – بأي وسيلة كانت – بهدف معالجتها سواء كانت بطريقة مباشرة أو غير مباشرة وفقاً لأغراض محددة مبنية على أسس نظامية، بما في ذلك النقل لأغراض أمنية أو لحماية الصحة أو السلامة العامة أو تنفيذاً لاتفاقية تكون المملكة طرفاً فيها.

الموافقة الصريحة:

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

التسويق المباشر:

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

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 أو منتظم – 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.

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.

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 بها أو عن طريق جهة المعالجة.

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.

البيانات غير المعالجة:

هي البيانات التي لم تخضع لعمليات متقدمة من المعاجلة 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، ومنها على سبيل المثال لا الحصر، المعالجة المسبقة قبل مشاركة البيانات الشخصية كـ التعتيم (Data Masking) أو المزج (Data Scrambling) أو التعمية (Data anonymization).

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 والتحليلات 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 إيرادات 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.

نموذج التسعير:

الآلية المستخدمة لتحديد القيمة العينية (سعر) للبيانات ومنتجات البيانات.

البيانات الحكومية:

هي البيانات التي تنتجها الجهات الحكومية.

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.

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.

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.

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.

الجهة غير الربحية:

أي جهة غير حكومية مرخصة بالعمل في المملكة وتقدم خدماتها ومنتجاتها بشكل غير ربحي.

المطوّر:

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

المستخدم:

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

صاحب البيانات:

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

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 االرئيسة (القياسات الحيوية) لتحديد الهوية الشخصية للأفراد في الصور الثابتة أو الصور المتحركة (المرئية).

3. الأهداف

إشارةً إلى نص قرار مجلس الوزراء رقم (292) وتاريخ 27/04/1441هـ، القاضي في الفقرة (1) من المادة "عاشراً" بأن يتولى المكتب وضع السياسات وآليات الحوكمة والمعايير والضوابط الخاصة بالبيانات والذكاء الاصطناعي ومتابعة الالتزام بها بعد إقرارها، عليه فقد قام مكتب إدارة البيانات الوطنية بالاستفادة من الممارسات والمعايير العالمية عند السياسات الخاصة بحوكمة البيانات الوطنية والتي تهدف إلى:

1. دعم وتعزيز جهود المملكة في تحقيق الرؤية والاستراتيجيات الوطنية.
2. نشر ثقافة مشاركة البيانات والتعاون لتعزيز وتطوير البيانات والمعلومات والأصول المعرفية.
3. تنظيم عملية نشر وتبادل واستخدام/ إعادة استخدام البيانات المحمية والمعلومات العامة.
4. تحقيق التكامل بين الجهات الحكومية.
5. تمكين الجهات الحكومية من إعداد سياساتها، وتنفيذ خططها، والقيام باستشراف المستقبل.
6. المحافظة على خصوصية البيانات الشخصية، وسرية البيانات الحساسة.
7. المحافظة على حقوق الأفراد عند التعامل مع البيانات الشخصية والمعلومات العامة لدى الجهات الحكومية.
8. تعزيز مفهوم وممارسات البيانات المفتوحة لتحسين الشفافية لدى الجهات العامة وتشجيع البحث والابتكار ودفع النمو الاقتصادي.
9. تعزيز الشفافية وإرساء قواعد الحوكمة عن طريق توزيع الأدوار والمسؤوليات.
10. المحافظة على السيادة الوطنية الرقمية للبيانات الشخصية.
11. رفع مستوى معايير الرقابة المجتمعية على أداء الجهات العامة.
12. دعم جهود تعزيز النزاهة ومكافحة الفساد عن طريق الاطلاع على المعلومات العامة كحق إنساني مكفول.
13. تمكين الجهات من الاستثمار والابتكار في الخدمات المعتمدة على البيانات الشخصية لتعزيز المكاسب التنموية والاقتصادية والتنافسية بما يساهم بشكل إيجابي في رفع الناتج الإجمالي المحلي للمملكة.
14. رفع مستوى الثقة في الخدمات المعتمدة على البيانات.
15. رفع مستوى الخدمات والتعاملات الإلكترونية بما يحقق التكاملية.
16. الإسهام في رفع مستوى الأداء التجاري والاقتصادي بالشفافية وعدالة الوصول إلى المعلومات العامة لتعزيز التنافسية وتكافؤ الفرص.

17. الرقي بالبحوث العلمية عن طريق تشجيع الباحثين للاستفادة من المعلومات العامة والنهوض بالدور التنموي والرقابي للمجتمع ومؤسساته.

18. توفير الفرص المتكافئة لطالبي المعلومات العامة مما يسهم في تعزيز المواطنة المتساوية والشراكة في الوعي بقضايا الوطن العامة.

4. السياسات الخاصة بحوكمة البيانات الوطنية

للمساهمة في رفع مستوى نضج مجال البيانات والذكاء الاصطناعي تم تدشين سبع سياسات خاصة بحوكمة البيانات الوطنية:

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.

سياسة تصنيف البيانات

4.1.سياسة تصنيف البيانات

4.1.1. النطاق

تنطبق أحكام هذه السياسة على جميع البيانات التي تتلقاها أو تنتجها أو تتعامل معها الجهات العامة 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.

4.1.2. المبادئ الرئيسة لتصنيف البيانات

المبدأ الأول: الأصل في البيانات الإتاحة

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

4.1.3.مستويات تصنيف البيانات

الجدول (1) أدناه يوضح المستويات الرئيسة لتصنيف البيانات بما يتوافق مع مستوى الأثر، كما يوضح بعض الأمثلة الاسترشادية لكل مستوى.

مستوى التصنيف	درجة الأثر	الوصف	أمثلة استرشادية
سري للغاية	عالي	تُصنف البيانات على أنها **«بيانات سرية للغاية»**، إذا كان الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي إلى ضرر جسيم واستثنائي لا يمكن تداركه أو إصلاحه على: • المصالح الوطنية بما في ذلك الإخلال بالاتفاقيات والمعاهدات أو إلحاق الضرر بسمعة المملكة أو بالعلاقات الدبلوماسية والانتماءات السياسية أو الكفاءة التشغيلية للعمليات الأمنية أو العسكرية أو الاقتصاد الوطني أو البنية التحتية الوطنية أو الأعمال الحكومية. • أداء الجهات العامة مما يُلحق ضررًا بالمصلحة الوطنية. • صحة الأفراد وسلامتهم على نطاق واسع وخصوصية كبار المسؤولين. • الموارد البيئية أو الطبيعية.	• خطط وتفصيلات العمليات العسكرية أو أي معلومات ذات علاقة بها • المعلومات السياسية الرسمية المتعلقة بالعلاقات الدولية والاتفاقيات أو المعاهدات وكل ما يتعلق بها من مباحثات ودراسات وأعمال تحضيرية. • المعلومات المتعلقة بأعمال وتدابير وتشكيلات الأجهزة الأمنية والاستخباراتية وتجهيزاتها. • المعلومات المتعلقة بآليات ومفاتيح التشفير المستخدمة للبنى التحتية الوطنية. • معلومات القضايا الإرهابية والمخططات المهددة للأمن. • المعلومات المتعلقة بالأسلحة والذخائر أو المواقع العسكرية الاستراتيجية أو أي مصدر من مصادر القوة الدفاعية والهجومية. • معلومات عن تحركات القوات المسلحة، أو القوات العسكرية الأخرى، أو تحركات الشخصيات الهامة. • معلومات تمس سيادة الدولة.
سري	متوسط	تُصنف البيانات على أنها **«بيانات سرية»**، إذا كان الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي إلى ضرر جسيم على: • المصالح الوطنية مثل إلحاق ضرر جزئي بسمعة المملكة والعلاقات الدبلوماسية أو الكفاءة التشغيلية للعمليات الأمنية أو العسكرية أو الاقتصاد الوطني أو البنية التحتية الوطنية والأعمال الحكومية. • يُحدث 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 الأفراد.	• معلومات عن مواقع تخزين المواد اللوجستية أو المخازن الاقتصادية. • معلومات متعلقة بالمنشآت الحيوية. • مذكرات التفاهم مع الشركات الدولية لإنشاء مصالح تجارية أو اقتصادية استراتيجية بالمملكة. • معلومات متعلقة بالاتفاقيات الثنائية ومذكرات التفاهم الدبلوماسية بين المملكة والدول الأخرى.

مستوى التصنيف	درجة الأثر	الوصف	أمثلة استرشادية
سري	**متوسط**	• تـؤدي إلـى ضـرر علـى المـدى الطويـل للمـوارد البيئيـة أو الطبيعيـة. • التحقيـق فـي القضايـا الكبـرى المحـددة نظامـاً، كقضايـا تمويـل الإرهـاب.	
مقيّد	**منخفض**	تُصنـف البيانـات علـى أنهـا «مقيّـدة»، إذا كان الوصـول غير المصرح بـه إلى هـذه البيـانـات أو الإفصـاح عنهـا أو عـن محتواهـا يـؤدي إلـى: • تأثيـر سلبـي محـدود علـى عمـل الجهـات العامة أو الانشطة الاقتصادية في المملكة أو علـى عمـل شـخص معيـن. • ضـرر محـدود علـى أصـول أي جهـة وخسـارة محـدودة علـى وضعهـا المالـي والتنافسـي. • ضـرر محـدود علـى المـدى القريـب للمـوارد البيئيـة أو الطبيعيـة.	• معلومات تضر بسمعة أي شخصية عامة. • بيانات مفصلة للمعاملات الفردية. • نتائـج الأبحـاث والدراسـات العمليـة قبـل نشـرها. • المعلومـات المتعلقـة بالمنتجـات تحـت التطويـر والتـي قـد تضـر بعدالـة المنافسـة. • معلومـات متعلقـة بالتعيينـات والقـرارات الإداريـة الحساسـة. • معلومات الملف الصحي للأفراد. • معلومـات تحديـد الهويـة مثـل ا الاسـم والعنـوان وأرقـام الهويـة الوطنيـة وأرقـام الهواتـف وأرقـام الحسـابات والتراخيـص وبيانـات السـمات الحيويـة. • معلومات رواتب الموظفين. • وثائـق مثـل خطـط المسـتوى التخطيطـي وبرامـج التسـويق قبـل الكشـف عنها للجمهور وخطـط الإبـداع التقنـي. • عقود موردين وعروض أسعارهم. • طلبات تقديم عروض. • مواصفات منتج جديد قبل طرحه للجمهور. • تفاصيـل تصميـم وتطبيـق أنظمـة أمنيـة (جدار الحماية وضوابط الوصول ومخططات الشـبكة وغيرهـا). • سياسيات وإجراءات الجهات الداخلية رسائل/ مذكرات داخلية. • قوائـم هواتـف داخليـة وقوائـم البريـد الإلكترونـي لبعـض الجهـات.

مستوى التصنيف	درجة الأثر	الوصف	أمثلة استرشادية
عام	لا يوجد	تُصنف البيانات على أنها «بيانات عامة» عندما لا يترتب على الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها أي من الآثار المذكورة أعلاه في حال عدم وجود تأثير على ما يأتي: • المصلحة الوطنية • أنشطة الجهات • مصالح الأفراد • الموارد البيئة	• توجهات استراتيجية وطنية معلنة. • الإحصاءات الوطنية حول عدد السكان والبيئة والأعمال حسب الصناعة وغيرها. • التنمية العامة والدراسات الاقتصادية. • إجراءات الحكومة وسياستها. • معلومات متعلقة بالخدمات العامة التي تقدمها الحكومة للمواطنين. • جهات الاتصال في المؤسسات. • إعلانات وظائف. • إعلانات عامة. • تصريحات صحفية. • نتائج مالية معلنة للجمهور. • عروض منتجات (عامة). • معلومات العلاقات العامة. • أي معلومات متاحة علناً على مواقع أي مؤسسة. • الإعلانات.

الجدول1: مستويات تصنيف البيانات

المبدأ الأول: الأصل في البيانات الإتاحة

كما يمكن تصنيف البيانات المصنّفة على مستوى مقيّد إلى مستويات فرعية بناءً على نطاق الأثر على النحو التالي:

مقيد - مستوى (أ): إذا كان نطاق الأثر على مستوى قطاع كامل أو نشاط اقتصادي عام.

مقيد - مستوى (ب): إذا كان نطاق الأثر على مستوى أنشطة عدة جهات أو على مصالح مجموعة من الأفراد.

مقيد - مستوى (ج): إذا كان نطاق الأثر على مستوى أنشطة جهة واحدة أو مصالح فرد معين.

وفي الجدول أدناه توضيح وتحديد لمستوى التصنيف الصحيح الذي يمكّن الجهات من تقييم درجة الأثر المترتبة على الوصول غير المصرح به إلى البيانات أو الإفصاح عنها أو عن محتواها (ولمزيدٍ من المعلومات حول عملية تقييم الأثر، يمكن الاطلاع على "الخطوات اللازمة لتصنيف البيانات").

يجب على كل جهة – على حده – أن تقوم بإجراء تقييم الآثار المترتبة على عملية الوصول أو الإفصاح غير المصرح به، كما تعتبر هذه القائمة غير شمولية.

فئة الأثر الرئيسة	المصلحة الوطنية
فئة الأثر الفرعية	سمعة المملكة
الاعتبارات	هل ستخضع المعلومات لاهتمام وسائل الإعلام المحلية أو الدولية؟ هل ستعطي انطباع سلبي؟

مستوى الأثر			
سري للغاية	سري	مقيّد	عام
عالي	متوسط	منخفض	لا يوجد أثر
تتأثر السمعة بشكل كبير.	تتأثر السمعة إلى حد ما.	لا تتأثر السمعة.	لا يوجد تأثير على المصالح الحيوية الوطنية.

فئة الأثر الرئيسة	المصلحة الوطنية
الاعتبارات	هل تُشكّل المعلومات خطراً على العلاقات مع الدول الصديقة؟ هل ستزيد من حدة التوتر الدولي؟ هل يمكن أن تؤدي إلى احتجاجات أو عقوبات من دول أخرى؟

مستوى الأثر			
سري للغاية	سري	مقيّد	عام
عالي	متوسط	منخفض	لا يوجد أثر
قطع العلاقات الدبلوماسية والانتماءات السياسية أو تهديد الاتفاقيات وشروط المعاهدات أو كليهما	تتأثر العلاقات الدبلوماسية سلباً على المدى الطويل	لن يحدث تأثير على العلاقات الدبلوماسية أو سيحدث تأثير بسيط على المدى القصير	لا يوجد تأثير على المصالح الحيوية الوطنية.

فئة الأثر الرئيسة	المصلحة الوطنية
فئة الأثر الفرعية	الاقتصاد الوطني
الاعتبارات	هل يؤدي الكشف عن المعلومات إلى خسائر اقتصادية على المستوى الوطني؟

مستوى الأثر			
سري للغاية	سري	مقيّد	عام
عالي	متوسط	منخفض	لا يوجد أثر
تأثير طويل المدى على الاقتصاد الوطني مع انخفاض لا يُمكن تداركه في الناتج المحلي الإجمالي أو أسعار الأسواق المالية أو نسبة البطالة أو القوة الشرائية أو المؤشرات الأخرى ذات الصلة؛ مما ينعكس سلباً على جميع القطاعات في المملكة.	تأثير طويل المدى على الاقتصاد الوطني مع انخفاض انخفاض يُمكن تداركه في الناتج المحلي الإجمالي ونسبة البطالة أو أسعار الأسواق المالية أو القوة الشرائية؛ مما ينعكس سلباً على قطاع واحد أو أكثر.	تأثير بسيط على الاقتصاد الوطني مع انخفاض يُمكن تداركه في وقت قصير في الناتج المحلي الإجمالي، ومعدل العمالة أو أسعار الأسواق المالية أو القوة الشرائية؛ مما ينعكس سلباً على قطاع واحد فقط.	

فئة الأثر الرئيسة	المصلحة الوطنية
فئة الأثر الفرعية	البنى التحتية الوطنية
الاعتبارات	هل الوصول إلى المعلومات يؤدي إلى تعطيل البنى التحتية الحيوية الوطنية (مثل الطاقة، النقل، الاتصالات)؟ في حال التعرض لهجمات إلكترونية، هل ستظل الخدمات الأساسية في المملكة متاحة؟

مستوى الأثر			
سري للغاية	سري	مقيّد	عام
عالي	متوسط	منخفض	لا يوجد أثر
التوقف والتعطل في أمن وعمليات البنى التحتية الوطنية الحيوية، كما تتأثر العديد من القطاعات وتتعطل الحياة الطبيعية.	التوقف والتعطل لفترة قصيرة في أمن وعمليات البنى التحتية الوطنية الحيوية، كما يتأثر قطاع واحد أو أكثر.	يحدث ضرر أو تأثير قصير المدى على أمن وعمليات البنى التحتية المحلية / الإقليمية.	

فئة الأثر الرئيسة	المصلحة الوطنية
فئة الأثر الفرعية	مهام الجهات الحكومية
الاعتبارات	هل سيؤدي الكشف عن المعلومات إلى الحد من إمكانية الجهات الحكومية من تنفيذ عملياتها ومهامها اليومية؟

مستوى الأثر			
سري للغاية	سري	مقيّد	عام
عالي	متوسط	منخفض	لا يوجد أثر
عدم قدرة جميع الجهات الحكومية على أداء مهامها وعملياتها الرئيسة لفترة طويلة.	عدم قدرة جهة حكومية واحدة أو أكثر على أداء واحدة أو أكثر من مهامها الرئيسة لفترة قصيرة.	عدم قدرة جهة حكومية أو أكثر على أداء مهمة واحدة أو أكثر من المهام غير الرئيسة لفترة قصيرة.	

فئة الأثر الرئيسة	أنشطة الجهات
فئة الأثر الفرعية	أرباح الجهات الخاصة
الاعتبارات	هل سيؤدي الكشف عن المعلومات إلى خسائر مالية أو إفلاس الجهات الخاصة التي تقوم بإدارة مرافق العامة ؟ على سبيل المثال، احتمالية الاحتيال، وتحويلات الأموال غير القانونية، والمصادرة غير القانونية للأصول؟

مستوى الأثر			
سري للغاية	سري	مقيّد	عام
عالي	متوسط	منخفض	لا يوجد أثر
تأثير سلبي كبير على الجهات الخاصة إلى الحد الذي يتسبب في الإضرار بالمصالح الحيوية الوطنية.	تكبد الجهة خسائر مالية فادحة مما قد يؤدي إلى الإفلاس.	ضرر محدود يتمثل في خسارة مالية محدودة للجهة أو لأيٍ من أصولها.	لا يوجد تأثير على أنشطة الجهات.

فئة الأثر الرئيسة	أنشطة الجهات
فئة الأثر الفرعية	مهام الجهات الخاصة
الاعتبارات	هل سيؤدي الكشف عن المعلومات إلى حدوث أضرار على الجهات الخاصة التي تقوم بإدارة المرافق العامة؟ هل سيؤدي ذلك إلى فقدان الدور الريادي التي تتمتع به الجهة أو خسارة أيٍ من أصولها؟ هل سيؤدي ذلك إلى إنهاء عقود عددٍ كبيرٍ من الموظفين؟ هل سيؤثر على القدرة التنافسية للجهة الخاصة؟

مستوى الأثر			
سري للغاية	سري	مقيّد	عام
عالي	متوسط	منخفض	لا يوجد أثر
تأثير سلبي كبير على الجهات الخاصة إلى الحد الذي يتسبب في الإضرار بالمصالح الحيوية الوطنية.	عدم إمكانية الجهة من القيام بمهامها الرئيسة، وفقدان القدرة على التنافسية إلى حد كبير.	عدم إمكانية الجهة من أداء إحدى مهامها الرئيسة، وفقدان القدرة على التنافسية بشكل محدود.	لا يوجد تأثير على أنشطة الجهات.

فئة الأثر الرئيسة	الأفراد
فئة الأثر الفرعية	صحة/ سلامة الأفراد
الاعتبارات	هل سيؤدي الكشف عن المعلومات إلى إفشاء أسماء أو مواقع أشخاص وما إلى ذلك؟ (على سبيل المثال، أسماء ومواقع العملاء السريين، والأشخاص الخاضعين لأنظمة حماية خاصة)

مستوى الأثر			
سري للغاية	سري	مقيّد	عام
عالي	متوسط	منخفض	لا يوجد أثر
خسارة عامة أو فادحة في الأرواح، وفقدان حياة فرد أو مجموعة من الأفراد.	ضرر جسيم أو إصابة تهدد حياة الفرد.	إصابة بسيطة دون أي خطر يهدد حياة أو صحة الفرد.	لا يوجد تأثير على الأفراد

فئة الأثر الرئيسة	الأفراد
فئة الأثر الفرعية	الخصوصية
الاعتبارات	هل سيؤدي الكشف عن المعلومات إلى انتهاك خصوصية الأفراد؟

مستوى الأثر			
سري للغاية	سري	مقيّد	عام
عالي	متوسط	منخفض	لا يوجد أثر
الكشف عن البيانات الشخصية لشخصية مهمة.	الكشف عن البيانات الشخصية لشخصية مهمة.	الكشف عن البيانات الشخصية للفرد.	لا يوجد تأثير على الأفراد

فئة الأثر الرئيسة	الأفراد
الاعتبارات	سيؤدي ذلك إلى انتهاك أي حقوق ملكية فكرية؟

مستوى الأثر			
سري للغاية	سري	مقيّد	عام
عالي	متوسط	منخفض	لا يوجد أثر
مما يؤثر على المصلحة الوطنية.			

فئة الأثر الرئيسة	البيئة
فئة الأثر الفرعية	الموارد البيئية
الاعتبارات	هل سيتم استخدام هذه المعلومات لتطوير خدمة أو منتج يمكن أن يؤدي إلى تدمير الموارد البيئية أو الطبيعية للمملكة؟

مستوى الأثر			
سري للغاية	سري	مقيّد	عام
عالي	متوسط	منخفض	لا يوجد أثر
تأثير كارثي لا يمكن تداركه على البيئة أو الموارد الطبيعية.	تأثير طويل المدى على البيئة أو الموارد الطبيعية.	تأثير قصير المدى أو محدود على البيئة أو الموارد الطبيعية.	لا يوجد تأثير على البيئة.

الجدول 2: فئات ودرجات تقييم الأثر وفقاً لمستويات تصنيف البيانات

4.1.4.ضوابط تصنيف البيانات

بناءً على مستويات التصنيف، تقوم الجهات 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 الجهة ويتم اعتمادها من المسؤول الأول بالجهة.

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:

o فترة زمنية محددة بعد إنشاء البيانات أو تلقيها (على سبيل المثال: عامين بعد الإنشاء).

o فترة زمنية محددة بعد اتخاذ أخر إجراء على البيانات (على سبيل المثال: ستة أشهر من تاريخ آخر استخدام).

o بعد انقضاء تاريخ محدد (على سبيل المثال، من المقرر مراجعتها في 1 يناير 2021).

o بعد ظروف أو أحداث معينة تأثيراً مباشراً 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.

4.1.5. الخطوات اللازمة لتصنيف البيانات

الخطوة 1 - تحديد جميع بيانات الجهة

تتمثل الخطوة الأولى التي تتخذها الجهات في جرد وتحديد جميع البيانات التي تمتلكها الجهة.

الخطوة 2 - تعيين مسؤول تصنيف البيانات

على الجهة تفويض شخص يتولى مسؤولية عملية التصنيف بمجرد تحديد جميع البيانات، غالباً ما يكون ممثل بيانات الأعمال – أحد منسوبي مكتب الجهة – هو الشخص الذي يفهم طبيعة البيانات وقيمتها داخل الجهة، وهو الشخص الذي يجب أن يتحمل المسؤولية حيال إجراء التصنيف الأولي، ونظراً إلى وجود أكثر من مسؤول بيانات داخل الجهة، فقد يوجد أكثر من شخص مسؤول عن تصنيف البيانات.

الخطوة 3 - إجراء عملية تقييم الأثر

يجب على ممثل بيانات الأعمال اتباع الخطوات اللازمة لعملية تقييم الأثر المحتمل الذي يترتب على:

- الإفصاح 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

تبدأ عملية تقييم الأثر بتطبيق مبدأ "الأصل في البيانات الإتاحة" (في المجال التنموي) ما لم تقتضِ طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية؛ السرية للغاية (في المجال السياسي والأمني) ما لم تقتضِ طبيعتها أو حساسيتها مستويات أدنى من التصنيف.

الخطوة 3أ - تحديد فئة الأثر:

يتمثل العنصر الأول من عملية تقييم الأثر في تحديد الفئة الرئيسة والفرعية للأثر المحتمل في أي من الفئات الرئيسة التالية:

- المصلحة الوطنية
- أنشطة الجهات
- صحة أو سلامة الأفراد
- الموارد البيئية

الخطوة -3ب - تحديد مستوى الأثر:

يُشير العنصر الثاني إلى أنه يتعين على ممثل بيانات الأعمال أن يحدد لكل أثر محتمل مستوى معين يعتمد تحديد المستوى على الآتي:

- مدة الأثر وصعوبة السيطرة على الضرر
- فترة تدارك وإصلاح الأضرار بعد وقوعها
- حجم الأثر على مستوى وطني، مناطقي، عدة جهات، جهة واحدة، عدة أفراد ... إلخ

تحدد هذه المعايير مستويات الأثر الأربعة:

- **عالي:** يؤدي الوصول إلى البيانات أو الإفصاح عنها إلى حدوث أضرارٍ جسيمة أو خطيرة للغاية على المدى الطويل لا يمكن تداركها أو إصلاحها.
- **متوسط:** يؤدي الوصول إلى البيانات أو الإفصاح عنها إلى حدوث أضرار جسيمة أو خطيرة يصعب السيطرة عليها.
- **منخفض:** يؤدي الوصول إلى البيانات أو الإفصاح عنها إلى أضرارٍ محدودة يمكن السيطرة عليها أو أضرار متقطعة على المدى القصير يمكن السيطرة عليها.
- **لا يوجد أثر:** لا يؤدي الوصول إلى البيانات أو الإفصاح عنها إلى أي ضرر على المدى الطويل أو القصير.

يجب أن تكون جميع الأضرار المحتملة والمحددة خلال عملية تقييم الأثر محددة وقائمة على أدلة، في محاولةٍ للحد من التقديرات الشخصية للمكلف بإجراء تصنيف البيانات.

يحدد ممثل بيانات الأعمال مستوى تصنيف البيانات بناءً على الآثار المحددة ومستوياتها:

- **عالٍ:** تُصنف البيانات باعتبارها "سرية للغاية".
- **متوسط:** تُصنف البيانات على أنها "سرية".
- **منخفض:** يلزم إجراء مزيدٍ من التقييمات (يرجى الاطلاع على الخطوة 4 و5).
- **لا يوجد أثر:** تُصنف البيانات على أنها بياناتٍ **"عامة"**.

ويوجد وصف مفصل للاعتبارات الرئيسة لكل فئة من فئات الأثر ومستواه في الجدول (2) **"فئات ومستويات تقييم أثر تصنيف البيانات".**

يجب الأخذ بعين الاعتبار الخطوتين 4 و5 عندما يكون مستوى الأثر المحدد منخفض.

يتم الانتقال إلى الخطوة 6 عندما تُصنف البيانات على أنها "سرية للغاية" أو "سرية" أو "عامة".

الخطوة 4 – تحديد الأنظمة ذات العلاقة (فقط إذا كان مستوى الأثر منخفضاً).

يجب إجراء تقييمات إضافية إذا كان مستوى الأثر المحدد "منخفض" وذلك بهدف زيادة مستوى تصنيف البيانات المصنفة على أنها بيانات "عامة" إلى الحد الأقصى.

يجب على ممثل بيانات الأعمال في هذا الصدد، دراسة ما إذا كان الإفصاح عن هذه البيانات يتعارض مع أنظمة المملكة العربية السعودية مثل نظام مكافحة الجرائم المعلوماتية ونظام التجارة االإلكترونية ... الخ وإذا كان الإفصاح عن البيانات مخالفاً للأنظمة، فيجب حينها تصنيف البيانات على أنها بيانات "مقيّدة"، بخلاف ذلك يتعين على ممثل بيانات الأعمال مواصلة تنفيذ الخطوة 5.

الخطوة 5 - الموازنة بين مزايا الإفصاح عن البيانات والآثار السلبية (فقط إذا كانت الإجابة على الخطوة 4 "لا").

بعد التأكد من مستوى الأثر المنخفض وضمان أن الإفصاح لن يكون انتهاكاً لأي نظام نافذ، يجب أيضاً تقييم المزايا المحتملة للإفصاح عن مثل هذا البيانات والتأكد مما إذا كانت هذه المزايا ستفوق الآثار السلبية أم لا، وتشمل المزايا المحتملة استخدام البيانات لتطوير خدمات جديدة ذات قيمة مضافة، أو زيادة شفافية العمليات الحكومية أو زيادة مشاركة الأفراد مع الحكومة.

- إذا كانت المزايا أكبر من الآثار السلبية، تصنف البيانات على أنها **"عامة"**.
- إذا كانت المزايا أقل من الآثار السلبية، تصنف البيانات على أنها **"مقيّدة"**.

الخطوة 6 - مراجعة مستوى التصنيف

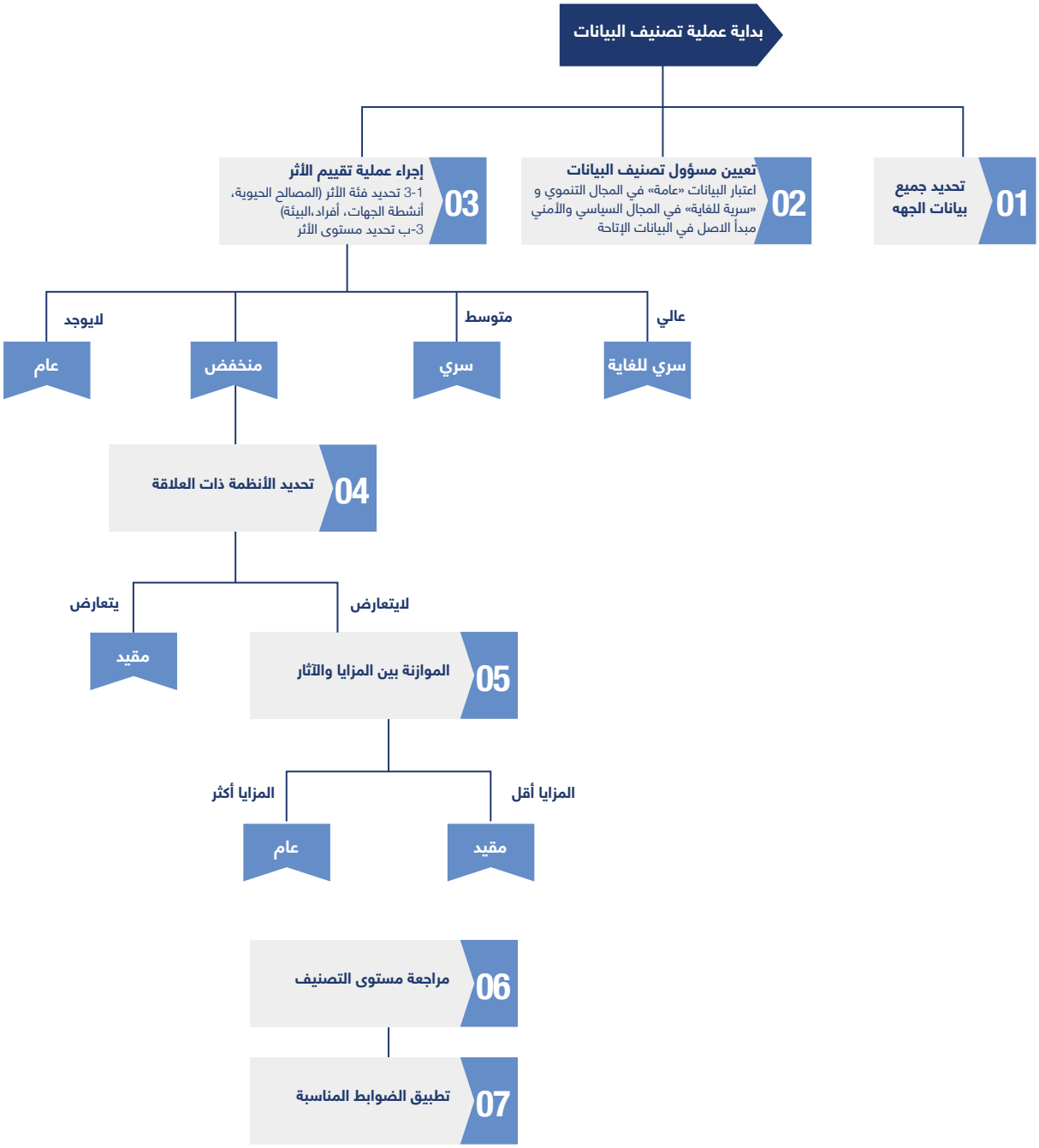
يجب أن يفحص مراجع تصنيف البيانات – أحد منسوبي مكتب الجهة – جميع البيانات المصنفة لضمان أن يكون مستوى التصنيف المحدد من جانب ممثل بيانات الأعمال هو الأنسب، وتتم مراجعته خلال شهر واحد من التصنيف الأولي.

الخطوة 7 - تطبيق الضوابط المناسبة

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

يتم الانتهاء من عملية التصنيف عند تصنيف جميع البيانات التي تملكها الجهة والتحقق من مستويات التصنيف وتطبيق الضوابط ذات الصلة.

بعد تصنيف البيانات على نحوٍ صحيح، يمكن للجهات مشاركتها مع جهات أخرى، أو إتاحتها ونشرها بصفتها بيانات مفتوحة عند تصنيفها بيانات "عامة".



الشكل (2) يوضح الخطوات اللازمة لإجراء تصنيف البيانات.

4.1.6.الأدوار والمسؤوليات داخل الجهة

على جميع الجهات تكليف أشخاص يتولون مسؤولية أداء الالتزامات المسندة لكل دورٍ من الأدوار الوظيفية المرتبطة بعملية تصنيف البيانات وشروط حمايتها على النحو المنصوص عليه أدناه.

ممثل بيانات الأعمال: الشخص المسؤول عن البيانات التي تجمعها الجهة أو تحتفظ بها، وعادةً ما يكون في مستوى إداري عالٍ، ويكون ممثل بيانات الأعمال مسؤول عن:

- **تصنيف البيانات:** تصنيف البيانات التي تجمعها الجهة أو الجهات التابعة لها.
- **تجميع البيانات:** التأكد من تصنيف البيانات المجمعة من مصادرٍ متعددة على أعلى مستويات التصنيف المستخدمة في تصنيف أي بيانات بشكل فردي.
- **تنسيق تصنيف البيانات:** التأكد من أن البيانات المتبادلة بين الإدارات أو الجهات مصنفة ومحمية بصورة متسقة.
- **الامتثال لتصنيف البيانات (بالتنسيق مع مختصي بيانات الأعمال) :** التأكد من أن البيانات محمية وفقاً للضوابط المحددة.

مراجع تصنيف البيانات: الشخص المسؤول عن مراجعة واعتماد مستويات تصنيف البيانات التي يحددها ممثل بيانات الأعمال، وعادة ما يكون في مستوى إداري عالٍ.

مختص بيانات الأعمال: عادةً ما يكون مختص بيانات الأعمال من أعضاء إدارات تقنية المعلومات أو أمن المعلومات أو كليهما، ويتحمل مسؤولية حماية البيانات عن طريق تطبيق الضوابط المعتمدة المحددة في قسم "ضوابط تصنيف البيانات" بالإضافة إلى ذلك، الحفاظ على الأنظمة وقواعد البيانات والخوادم التي تخزن البيانات ودعمها، وتتألف مسؤوليات مختص بيانات الأعمال من:

التحكم في الوصول: التأكد من تطبيق ضوابط التحكم في الوصول ورصدها ومراجعتها وفقًا لمستويات تصنيف البيانات التي يحددها ممثل بيانات الأعمال.

- **تقارير المراجعة:** إرسال تقرير سنوي إلى مسؤولي البيانات يتناول توافر البيانات المصنفة وسلامتها وسريتها.
- **النسخ الاحتياطي للبيانات:** إجراء نسخ احتياطية منتظمة للبيانات.
- **التحقق من صحة البيانات:** التحقق من صحة البيانات بشكل دوري.
- **استعادة البيانات:** استعادة البيانات من وسائط النسخ الاحتياطي.
- **نشاط المراقبة :** مراقبة الأنشطة التي تتم على البيانات وتسجيلها، بما في ذلك البيانات المتعلقة بالشخص الذي يصل إلى هذه البيانات.
- **الامتثال لتصنيف البيانات (بالاشتراك مع مسؤولي البيانات):** التأكد من تصنيف بيانات الجهة وحمايتها بعد العملية الموضحة في هذه السياسة ووفقاً للضوابط المحددة.

مستخدم البيانات: الموظف الذي يتعامل مع البيانات أو يصل إليها أو يستخدمها أو يحدّثها بغرض أداء مهمة يخولها له ممثل بيانات الأعمال، ويستغل المستخدمون البيانات بطريقة تتوافق مع الغرض المحدد، وكذلك الامتثال لهذه السياسة وجميع السياسات المتعلقة باستخدام البيانات في المملكة العربية السعودية، ويُكلف المسؤول الأول بالجهة من يراه من ذوي الاختصاص لأداء هذه الأدوار.

سياسة حماية البيانات الشخصية

4.2. سياسة حماية البيانات الشخصية

4.2.1. النطاق

تنطبق أحكام هذه السياسة على جميع الجهات في المملكة، التي تقوم كلياً أو جزئياً بمعالجة البيانات الشخصية، وكذلك الجهات الخارجية التي تقوم بمعالجة البيانات الشخصية المتعلقة بالأفراد المقيمين في المملكة والتي تتم عبر شبكة الإنترنت أو أي وسيلة أخرى.

يستثنى من نطاق تطبيق هذه السياسة، جمع البيانات الشخصية من غير صاحبها مباشرة – دون علمه – أو معالجتها لغير الغرض الذي جُمعت من أجله أو الإفصاح عنها دون موافقته أو نقلها إلى خارج المملكة في الأحوال التالية:

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

4.2.2. المبادئ الرئيسة لحماية البيانات الشخصية

المبدأ الأول: المسؤولية

أن يتم تحديد وتوثيق سياسات وإجراءات الخصوصية الخاصة بجهة التحكم واعتمادها من قبل المسؤول الأول بالجهة (أو من يفوضه)، ونشرها إلى جميع الأطراف المعنية بتطبيقها.

المبدأ الثاني: الشفافية

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

المبدأ الثالث: الاختيار والموافقة

أن يتم تحديد جميع الخيارات الممكنة لصاحب البيانات الشخصية والحصول على موافقته (الضمنية أو الصريحة) فيما يتعلق بجمع بياناته واستخدامها أو الإفصاح عنها.

المبدأ الرابع: الحد من جمع البيانات

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

المبدأ الخامس: الحد من استخدام البيانات والاحتفاظ بها والتخلص منها

أن يتم تقييد معالجة البيانات الشخصية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدّم صاحب البيانات موافقته الضمنية أو الصريحة، والاحتفاظ بها طالما كان ذلك ضرورياً لتحقيق الأغراض المحددة أو لما تقتضيه الأنظمة واللوائح والسياسات المعمول بها في المملكة وإتلافها بطريقة آمنة تمنع التسرب، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو الوصول غير المصرّح به نظاماً.

المبدأ السادس: الوصول إلى البيانات

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

المبدأ السابع: الحد من الإفصاح عن البيانات

أن يتم تقييد الإفصاح عن البيانات الشخصية للأطراف الخارجية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدّم صاحب البيانات موافقته الضمنية أو الصريحة.

المبدأ الثامن: أمن البيانات

أن تتم حماية البيانات الشخصية من التسرب، أو التلف، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو التعديل أو الوصول غير المصرّح به – وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.

المبدأ التاسع: جودة البيانات

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

المبدأ العاشر: المراقبة والامتثال

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

4.2.3.حقوق صاحب البيانات

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

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

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

4.2.4.التزامات جهة التحكم

1. أن تكون جهة التحكم مسؤولة عن إعداد وتطبيق السياسات والإجراءات المتعلقة بحماية البيانات الشخصية، ويكون المسؤول الأول بالجهة – أو من يفوضه – مسؤولاً عن الموافقة عليها واعتمادها.
2. أن تقوم جهة التحكم بإنشاء وحدة لحوكمة البيانات تكون (مرتبطة بمكاتب إدارة البيانات في الجهات الحكومية التي تم تأسيسها بموجب الأمر السامي الكريم رقم 59766 وتاريخ20/11/1439هـ) أو مستقلة (في جهات القطاع الخاص) وتسند إليهامسؤولية تطوير وتوثيق ومراقبة تنفيذ السياسات والإجراءات المعتمدة من الإدارة العليا بالجهة، على أن تتضمن مهام ومسؤوليات الوحدة وضع المعايير المناسبة لتحديد مستويات حساسية البيانات الشخصية.
3. أن تقوم جهة التحكم بتقييم المخاطر والآثار المحتملة لأنشطة معالجة البيانات الشخصية وعرض نتائج التقييم على المسؤول الأول بالجهة – أو من يفوضه – لتحديد مستوى قبول المخاطر وإقرارها.
4. أن تقوم جهة التحكم بمراجعة وتحديث العقود واتفاقيات مستوى الخدمة والتشغيل بما يتوافق مع سياسات وإجراءات الخصوصية المعتمدة من الإدارة العليا للجهة.
5. أن تقوم جهة التحكم بإعداد وتوثيق الإجراءات اللازمة لإدارة ومعالجة انتهاكات الخصوصية وتحديد المهام والمسؤوليات المتعلقة بفريق العمل المختص، والحالات التي يتم بها إشعار الجهة التنظيمية والمكتب حسب التسلسل الإداري - بناءً على قياس شدة الأثر.
6. أن تقوم جهة التحكم بإعداد برامج توعوية لتعزيز ثقافة الخصوصية ورفع مستوى الوعي وفقاً لسياسات وإجراءات الخصوصية المعتمدة من الإدارة العليا للجهة.

7. أن يتم إشعار صاحب البيانات - بطريقة ملائمة وقت جمع البيانات - بالغرض والأساس النظامي/ الاحتياج الفعلي والوسائل والطرق المستخدمة لجمع ومعالجة ومشاركة البيانات الشخصية وكذلك التدابير الأمنية لضمان حماية الخصوصية حسب الأنظمة واللوائح والسياسات المعمول بها في المملكة.
8. أن يتم إشعار صاحب البيانات عن المصادر الأخرى التي يتم استخدامها في حال تم جمع بيانات إضافية بطريقة غير مباشرة (من جهات أخرى).
9. أن يتم تزويد صاحب البيانات بالخيارات المتاحة فيما يتعلق بمعالجة البيانات الشخصية والآلية المستخدمة لممارسة هذه الخيارات، ومنها على سبيل المثال (Preferences, Opt-in and Opt-out).
10. أن يتم أخذ موافقة صاحب البيانات على معالجة البيانات الشخصية بعد تحديد نوع الموافقة (صريحة أو ضمنية) بناءً على طبيعة البيانات وطرق جمعها.
11. أن يكون الغرض من جمع البيانات متوافقاً مع الأنظمة واللوائح والسياسات المعمول بها في المملكة وذا علاقة مباشرة بنشاط الجهة.
12. أن يكون محتوى البيانات مقتصراً على الحد الأدنى من البيانات اللازمة لتحقيق الغرض من جمعها.
13. أن يتم تقييد جمع البيانات على المحتوى المعد سلفاً (الموضح في القاعدة 12) ويكون بطريقة عادلة (مباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التضليل).
14. أن يقتصر استخدام البيانات على الغرض التي جُمعت من أجله.
15. أن تقوم جهة التحكم بإعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات وفقاً للأغراض المحددة والأنظمة والتشريعات ذات العلاقة.
16. أن تقوم جهة التحكم بتخزين البيانات الشخصية ومعالجتها داخل الحدود الجغرافية للمملكة لضمان المحافظة على السيادة الوطنية الرقمية لهذه البيانات، ولا تجوز معالجتها خارج المملكة إلا بعد حصول جهة التحكم على موافقة كتابية من الجهة التنظيمية، بعد تنسيق الجهة التنظيمية مع المكتب.
17. أن تقوم جهة التحكم بإعداد وتوثيق سياسة وإجراءات التخلص من البيانات لإتلاف البيانات بطريقة آمنة تمنع فقدانها أو إساءة استخدامها أو الوصول غير المصرح به إليها – وتشمل البيانات التشغيلية، المؤرشفة، والنسخ الاحتياطية – وذلك وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني.

18. أن تقوم جهة التحكم بتضمين أحكام سياستي الاحتفاظ والتخلص من البيانات في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.

19. أن تقوم جهة التحكم بتحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية وذلك لمراجعتها وتحديثها.

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

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

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

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

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

25. أن يتم استخدام الضوابط الإدارية والتدابير التقنية المعتمدة في سياسات الجهة لأمن المعلومات لضمان حماية البيانات الشخصية ومنها على سبيل المثال لا الحصر:

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

26. أن تكون جهة التحكم مسؤولة عن مراقبة الامتثال لسياسات وإجراءات الخصوصية بشكل دوري ويتم عرضها على المسؤول الأول للجهة – أو من يفوضه – كما يتم تحديد وتوثيق الإجراءات التصحيحية التي سيتم اتخاذها في حال عدم الامتثال وإشعار الجهة التنظيمية والمكتب حسب التسلسل التنظيمي.

4.2.5. أحكام عامة

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

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

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

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

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

سادساً: يمارس المكتب أدوار ومهام الجهات التنظيمية على جهات التحكم غير الخاضعة لجهات تنظيمية.

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

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

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

سياسة مشاركة البيانات

4.3. سياسة مشاركة البيانات

4.3.1. النطاق

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

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

4.3.2.المبادئ الرئيسة لمشاركة البيانات

المبدأ الأول: تعزيز ثقافة المشاركة

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

المبدأ الثاني: مشروعية الغرض

أن تُشارك البيانات لأغراض مشروعة مبنية على أساس نظامي أو احتياج عملي مسوغ يهدف إلى تحقيق مصلحة عامة دون إلحاق أي ضرر بالمصالح الوطنية، أو أنشطة الجهات أو خصوصية الأفراد أو سلامة البيئة – ويستثنى من ذلك البيانات والجهات المستثناة بأوامر سامية.

المبدأ الثالث: الوصول المصرّح به

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

المبدأ الرابع: الشفافية

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

المبدأ الخامس: المسؤولية المشتركة

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

المبدأ السادس: أمن البيانات

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

المبدأ السابع: الاستخدام الأخلاقي

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

4.3.3. الخطوات اللازمة لإجراء عملية مشاركة البيانات

تـم تحديـد الخطـوات الأساسـية لعمليـة مشـاركة البيانـات لمسـاعدة الجهـات علـى توحيـد ممارسـات المشـاركة وضمـان اسـتيفاء جميـع الضوابـط والمتطلبـات اللازمـة – والتـي قـد لا تتجـاوز 3 أشـهر. الشكل (٣) أدناه يوضح الخطوات اللازمة لمشاركة البيانات

1. يقـوم مقـدّم الطلـب - سـواء أكان جهـة حكوميـة أو خاصـة أو فـرداً- بإرسـال طلـب مشـاركة بيانـات إلـى مكتـب الجهـة المطلـوب منهـا مشـاركة البيانـات، علـى أن يُرسـل الطلـب عـن طريـق مكتـب الجهـة فـي حـال كان مقـدم الطلـب جهـة حكوميـة.
2. يقـوم مكتـب الجهـة المطلـوب منهـا مشـاركة البيانـات بإحالـة الطلـب إلـى ممثـل بيانـات الأعمـال المختـص والـذي بـدوره يقـوم بتوجيـه هـذا الطلـب إلـى أحـد مختصـي بيانـات الأعمـال لتقييـم هـذا الطلـب ومعالجتـه.
3. يقوم مختص بيانات الأعمال بالتحقق من مستوى تصنيف البيانات المطلوبة:

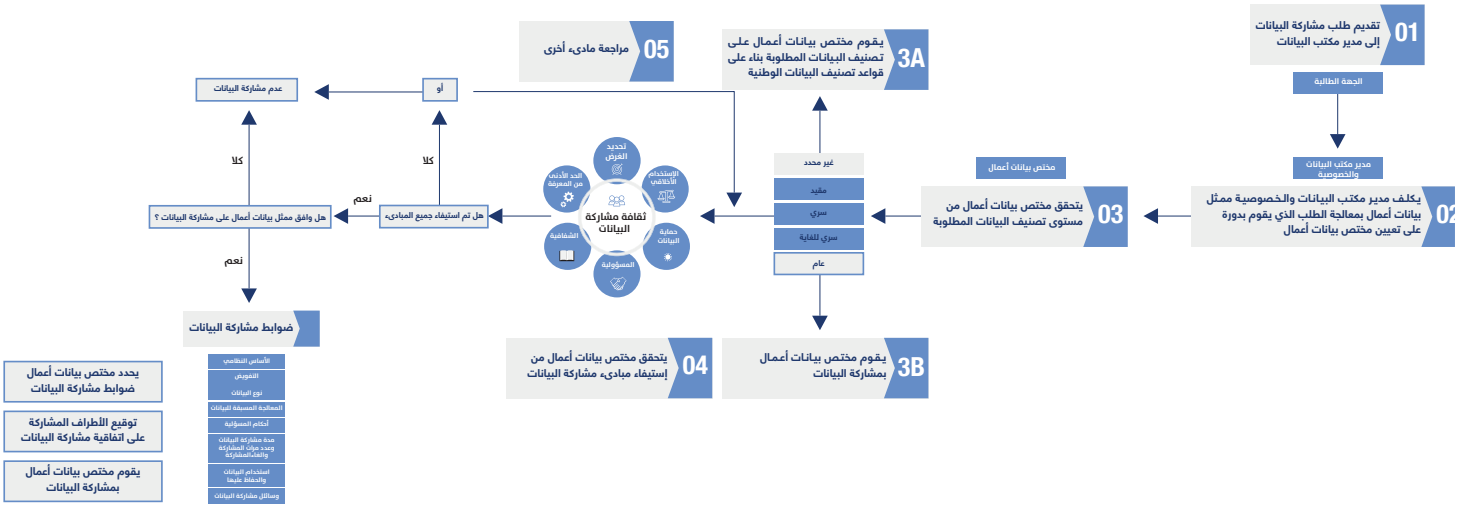
أ. فـي حالـة عـدم تحديـد مسـتوى التصنيـف، يجـب علـى مكتـب الجهـة – المطلـوب منهـا مشـاركة البيانـات – تصنيـف البيانـات المطلوبـة وفقـاً لسياسـة تصنيـف البيانـات.

ب. فـي حالـة تحديـد مسـتوى التصنيـف علـى أنـه "عـام"، يمكـن لمختـص بيانـات الأعمـال مشـاركة البيانـات المطلوبـة دون تقييـم الطلـب وفقـاً للمبـادئ الرئيسـية لمشـاركة البيانـات.

ت. فـي حالـة تحديـد مسـتوى التصنيـف علـى أنـه "مقيّـد" أو "سـري" أو "سـري للغايـة"، يتعيـن علـى مختـص بيانـات الأعمـال تقييـم الطلـب وفقـاً للمبـادئ الرئيسـية لمشـاركة البيانـات.

4. يجـب علـى مختـص بيانـات الأعمـال فـي مكتـب الجهـة المطلـوب منهـا مشـاركة البيانـات اسـتكمال عمليـة المشـاركة إذا تـم اسـتيفاء جميـع مبـادئ مشـاركة البيانـات بالكامـل.
5. لا يجـوز لمختـص بيانـات الأعمـال فـي مكتـب الجهـة المطلـوب منهـا مشـاركة البيانـات الاسـتمرار فـي مشـاركة البيانـات فـي حالـة عـدم اسـتيفاء مبـدأ واحـد أو أكثـر مـن مبـادئ مشـاركة البيانـات. كمـا يجـب علـى مختـص بيانـات الأعمـال فـي مكتـب الجهـة أن يـرد الطلـب إلـى مقـدم الطلـب مـع الملاحظـات وإتاحـة الفرصـة لتلبيـة جميـع مبـادئ مشـاركة البيانـات غيـر المتوافقـة.
6. عنـد اسـتيفاء جميـع مبـادئ مشـاركة البيانـات، يقـوم مختـص بيانـات الأعمـال بالحصـول علـى موافقـة ممثـل بيانـات الأعمـال علـى اسـتكمال عمليـة مشـاركة البيانـات.
7. يقـوم مختـص بيانـات الأعمـال فـي مكتـب الجهـة المطلـوب منهـا مشـاركة البيانـات بتحديـد الضوابـط المناسـبة لضمـان الالتـزام بمبـادئ مشـاركة البيانـات وتحقيـق الأهـداف المحـددة لـكل منهـا، كمـا يجـب أن يتـم الاتفـاق بيـن مختـص بيانـات الأعمـال فـي مكتـب الجهـة ومقـدم الطلـب والأطـراف الأخـرى المشـاركة فـي عمليـة المشـاركة علـى تطبيـق هـذه الضوابـط.

8. بعد الاتفاق على ضوابط مشاركة البيانات والالتزام بتطبيقها، ينبغي لمختص بيانات الأعمال توضيحها بالتفصيل في الاتفاقية ويجب على جميع الأطراف المُشارِكة في عملية المشاركة التوقيع على اتفاقية مشاركة البيانات.
9. يمكن لمكتب الجهة مشاركة البيانات المطلوبة مع الجهة الطالبة بعد توقيع اتفاقية مشاركة البيانات.



4.3.4. الإطار الزمني لعملية مشاركة البيانات

تقوم الجهة الحكومية - المطلوب منها مشاركة البيانات - بتقييم الطلب خلال فترة زمنية لا تتجاوز (30) يوماً من تاريخ استلام الطلب، وإشعار مقدم الطلب بقرار المشاركة على أن يكون القرار مكتوباً ومسبّباً (الخطوات من 2 إلى 4 من عملية مشاركة البيانات الموضحة أعلاه).

وفي حال عدم الموافقة على طلب المشاركة، فيحق لمقدم الطلب استكمال المتطلبات لاستيفاء جميع المبادئ وطلب الاستئناف من مختص بيانات الأعمال لإعادة تقييم الطلب وإصدار قرار المشاركة خلال فترة زمنية لا تتجاوز (14) يوماً من تاريخ استلامه (الخطوة 5 من عملية مشاركة البيانات).

بعد الحصول على موافقة ممثل بيانات الأعمال على الاستمرار في عملية المشاركة (الخطوة 6 من عملية مشاركة البيانات)، يقوم مختص بيانات الأعمال بتطوير وتطبيق الضوابط المناسبة لمشاركة البيانات وإعداد اتفاقية مشاركة بيانات خلال فترة زمنية لا تتجاوز (60) يوماً من تاريخ موافقة ممثل بيانات الأعمال (الخطوة 7 من عملية مشاركة البيانات).

بعد توقيع اتفاقية مشاركة البيانات (الخطوة 8 من عملية مشاركة البيانات)، يقوم مختص بيانات الأعمال بمشاركة البيانات مع مقدم الطلب خلال (7) أيام من تاريخ توقيع الاتفاقية (الخطوة 9 من عملية مشاركة البيانات).

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

التفويض:

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

- أن تُحدد الجهات والأشخاص 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 الجهة لضمان طلب البيانات من مصدرها الصحيح.
- أن تُحدد الحد الأنى من البيانات المطلوبة لتحقيق الأغراض المحددة.
- أن تُحدد البيانات المطلوبة وصيغتها والمتطلبات المتعلقة بتعديلها أو تغييرها (مثل صيغة البيانات، دقة البيانات، مستوى التفاصيل، هيكلة البيانات، نوع البيانات خام أو بيانات مُعالجة).

المعالجة المسبقة للبيانات:

- (المبادئ ذات العلاقة: المبدأ السادس: أمن البيانات)
- أن تُحدد ما إذا كان هناك حاجة لمعالجة البيانات قبل مشاركتها، وفي حال الحاجة لذلك يتم الاتفاق على أساليب المعالجة المطلوبة - على سبيل المثال، الحجب وإخفاء الهوية والتجميع (على ألا تتم معالجة البيانات بشكل يغير المحتوى).
- أن تُقيّم جودة البيانات المطلوبة وصحتها وسلامتها وتحديد ما إذا كانت تتطلب إجراء تحسين قبل مشاركتها، وفي حال الحاجة لذلك يجب على مكتب الجهة تدقيق البيانات قبل مشاركتها.

وسائل مشاركة البيانات:

(المبادئ ذات العلاقة: المبدأ السادس: أمن البيانات)

- الالتزام بضوابط حماية البيانات التي تصدرها الهيئة الوطنية للأمن السيبراني.
- أن يتم تحديد وسائل مشاركة البيانات المادية والرقمية.
- أن يتم التحقق من أمن وموثوقية وسائل المشاركة للتقليل من المخاطر المحتملة، كما يمكن الاستفادة من وسائل المشاركة الآمنة المعتمدة بين الجهات.
- أن يتم تحديد آلية مشاركة البيانات، وما إذا كان مختص بيانات الأعمال سيقوم بنقل البيانات مباشرةً إلى مقدم الطلب أو سيتم الاستعانة بمقدم خدمة لإتمام عملية المشاركة.
- أن يتم تحديد ما إذا كان سيتم استخدام وسائط المشاركة الموجودة (على سبيل المثال، قناة التكامل الحكومية، شبكة مركز المعلومات الوطني) أو سيتم استخدام وسائط مختلفة (شبكة الإنترنت اللاسلكية، وإمكانية الوصول عن بعد، والشبكة الافتراضية الخاصة، وواجهة برمجة التطبيقات).
- أن يتم الاتفاق على آلية إتلاف الوسائط المادية المستخدمة في مشاركة البيانات.

استخدام البيانات والحفاظ عليها:

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

- أن تُحدد متطلبات حماية البيانات عند مشاركتها، وتطبيق الضوابط المحددة لحماية البيانات بعد مشاركتها.
- أن تُفرض قيود مناسبة على الاستخدام أو المعالجة المسموح بها للبيانات (إن وُجدت)، مثل قيود خاصة بالمعالجة، أو قيود مكانية أو زمانية، أو حقوق حصرية أو تجارية.
- أن يتم تحديد حقوق جميع الأطراف المشاركة في عملية المشاركة بإجراء عمليات التدقيق والمراجعة.
- أن يتم الاتفاق على إجراءات تسوية النزاعات والتحكيم.
- أن تُحدد ما إذا كان هناك طرف ثالث للاستفادة من البيانات بعد مشاركتها والاتفاق على الآلية المنظمة لذلك.

مدة مشاركة البيانات وعدد مرات المشاركة وإلغاء المشاركة:

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

- أن تُحدد مدة مشاركة البيانات والموعد النهائي للوصول إلى البيانات أو تخزينها.
- أن تُحدد عدد مرات مشاركة البيانات، والمتطلبات اللازمة للمراجعة، وإجراء التعديلات، والإجراءات التي سيتم اتخاذها عند انتهاء الاتفاقية (مثل إخفاء هوية أصحاب البيانات أو إلغاء الوصول إلى البيانات أو إتلافها).
- أن تُحدد الأطراف الذين يحق لهم إنهاء مشاركة البيانات قبل التاريخ المتفق عليه، المستند النظامي، وفترة الإشعار المسموح بها.

أحكام المسؤولية:

(المبادئ ذات العلاقة: المبدأ الخامس: المسؤولية المشتركة)

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

4.3.6. القواعد العامة لمشاركة البيانات

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

1. يجب على جميع الجهات إعطاء الأولوية لوسائط المشاركة المعتمدة والآمنة لتبادل البيانات، ومنها على سبيل المثال قناة التكامل الحكومية، وشبكة مركز المعلومات الوطني.
2. يتولى مختص بيانات الأعمال في مكتب الجهة المطلوب منها المشاركة مسؤولية مشاركة البيانات بعد استيفاء جميع مبادئ مشاركة البيانات، بالإضافة إلى تحديد الضوابط المناسبة للمشاركة.
3. يجب على كل جهة تعيين أو تفويض الشخص المناسب – حسب المؤهلات والتدريب المطلوب - للتعامل مع البيانات بطريقة صحيحة، على أن يكون مصرح له طلب البيانات المشتركة وتلقيها والوصول إليها وتخزينها وإتلافها.
4. يجب إخفاء هوية أصحاب البيانات الشخصية، إلا إذا كان ذلك ضرورياً لغرض المشاركة مع تحديد الضوابط اللازمة للمحافظة على خصوصية أصحاب البيانات وفقاً لسياسة خصوصية البيانات الشخصية.
5. يجب إرفاق البيانات الوصفية (metadata) عند مشاركة البيانات في الحالات التي تتطلب ذلك.
6. تكون الجهات المشاركة في مشاركة البيانات مسؤولة عن حماية البيانات واستخدامها وفقاً للأغراض المحددة، ويحق لمكتب الجهة مراجعة مدى الالتزام بشكل دوري أو عشوائي بما يتوافق مع الضوابط المحددة في اتفاقية مشاركة البيانات.
7. يقوم المكتب بإعداد الدليل الإرشادي لمشاركة البيانات والمتضمن نموذج طلب مشاركة البيانات ونموذج اتفاقية قياسية لمشاركة البيانات.
8. تقوم الجهات التنظيمية – بعد التنسيق مع المكتب – بإعداد الآليات والإجراءات والضوابط المتعلقة بتسوية النزاع وفقاً لإطار زمني محدد.
9. في حال وجود نزاع بين الأطراف المشاركة في عملية مشاركة البيانات، يحق للجهات التابعة لنفس الجهة التنظيمية إشعار الجهة التنظيمية والمطالبة بتسوية النزاع بين الأطراف المشاركة، وفي حال لم يتم حل النزاع، يتم إشعار المكتب بذلك، ويتولى المكتب تسوية النزاع إذا كانت الجهتان غير خاضعتين لنفس الجهة التنظيمية.
10. في حال وجود جانب من جوانب مشاركة البيانات لا تشملها هذه السياسة، يحق لمكتب الجهة وضع قواعد إضافية لا تتعارض مع مبادئ مشاركة البيانات مع تقديم مسوغ كافٍ وإشعار المكتب بذلك.

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

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

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

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

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

سياسة حرية المعلومات

4.4. سياسة حرية المعلومات

4.4.1.النطاق

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

لا تنطبق أحكام هذه السياسة على المعلومات المحمية:

1. المعلومات التي يؤدي إفشاؤها إلى الإضرار بالأمن الوطني للدولة أو سياساتها أو مصالحها أو حقوقها.
2. المعلومات العسكرية والأمنية.
3. المعلومات والوثائق التي يتم الحصول عليها بمقتضى اتفاق مع دولة أخرى وتصنف على أنها محمية.
4. التحريات والتحقيقات وأعمال الضبط وعمليات التفتيش والمراقبة المتعلقة بجريمة أو مخالفة أو تهديد.
5. المعلومات التي تتضمن توصيات أو اقتراحات أو استشارات من أجل إصدار تشريع أو قرار حكومي لم يصدر بعد.
6. المعلومات ذات الطبيعة التجارية أو الصناعية أو المالية أو الاقتصادية التي يؤدي الإفصاح عنها إلى تحقيق ربح أو تلافي خسارة بطريقة غير مشروعة.
7. الأبحاث العلمية أو التقنية، أو الحقوق المشتملة على حق من حقوق الملكية الفكرية التي يؤدي الكشف عنها إلى المساس بحق معنوي.
8. المعلومات المتعلقة بالمنافسات والعطاءات والمزايدات التي يؤدي الإفصاح عنها إلى الإخلال بعدالة المنافسة.
9. المعلومات التي تكون سرية أو شخصية بموجب نظام آخر، أو تتطلب إجراءات نظامية معينة للوصول إليها أو الحصول عليها.

4.4.2.المبادئ الرئيسة لحرية المعلومات

المبدأ الأول: الشفافية

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

المبدأ الثاني: الضرورة والتناسب

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

المبدأ الثالث: الأصل في المعلومات العامة الإفصاح

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

المبدأ الرابع: المساواة

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

4.4.3.حقوق الأفراد بما يتعلق بالاطلاع على المعلومات العامة أو الحصول عليها

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

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

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

4.4.4.التزامات الجهات العامة

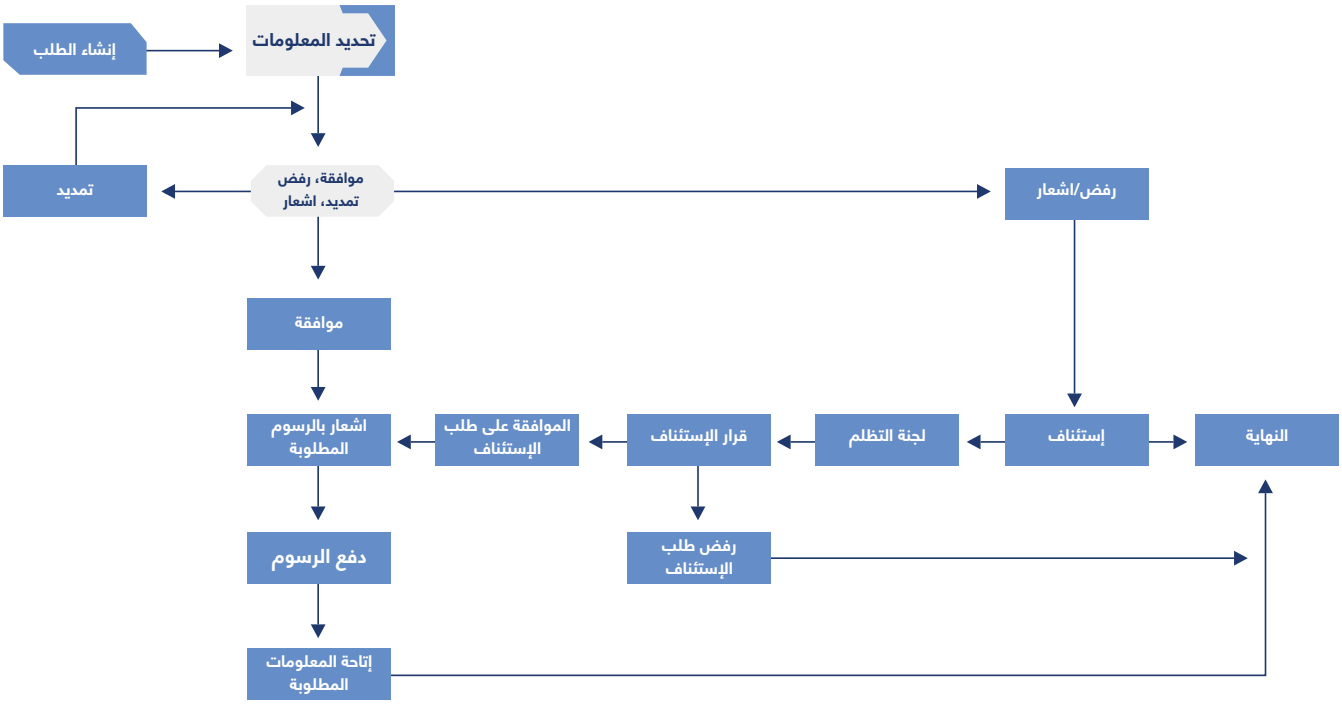
1. أن تكون الجهة العامة مسؤولة عن إعداد وتطبيق السياسات والإجراءات المتعلقة بممارسة حق الوصول إلى المعلومات العامة أو الحصول عليها، ويكون المسؤول الأول بالجهة مسؤولاً عن الموافقة عليها واعتمادها.
2. أن تقوم الجهة العامة بإنشاء وحدة إدارية تكون مرتبطة بمكاتب إدارة البيانات في الجهات الحكومية التي تم تأسيسها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

3. أن تقوم الجهة العامة بتحديد وتوفير الوسائل الممكنة (نماذج طلب المعلومات العامة) – سواء أكانت نماذج ورقية أو إلكترونية – والتي من خلالها يمكن للفرد طلب الاطلاع على المعلومات العامة أو الحصول عليها.
4. أن تقوم الجهة العامة بالتحقق من هوية الأفراد قبل منحهم حق الاطلاع على المعلومات العامة أو الحصول عليها وفقاً للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات العلاقة.
5. أن تقوم الجهة بوضع المعايير اللازمة لتحديد الرسوم المترتبة على معالجة طلبات الاطلاع على المعلومات العامة أو الحصول عليها بناءً على طبيعة البيانات وحجمها والجهد المبذول والوقت المستغرق - وفقاً لوثيقة سياسة تحقيق الدخل من البيانات . أن تقوم الجهة العامة 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.
6. أن تقوم الجهة العامة بإعداد وتوثيق سياسات وإجراءات الاحتفاظ بسجلات الطلبات والتخلص منها وفقاً للأنظمة والتشريعات ذات العلاقة بأعمال وأنشطة الجهة.
7. أن تقوم الجهة العامة بإعداد وتوثيق الإجراءات اللازمة لإدارة ومعالجة وتوثيق طلبات التمديد، والطلبات المرفوضة وتحديد المهام والمسؤوليات المتعلقة بفريق العمل المختص، والحالات التي يتم بها إشعار الجهة التنظيمية والمكتب حسب التسلسل الإداري وفقاً للفترة الزمنية المحددة لمعالجة الطلبات.
8. أن تقوم الجهة العامة بإشعار الفرد - بطريقة ملائمة – في حال تم رفض الطلب كلياً أو جزئياً، مع إيضاح أسباب الرفض والحق في التظلّم وكيفية ممارسة هذا الحق خلال مدة لا تتجاوز (15) يوماً من اتخاذ القرار.
9. أن تقوم الجهة العامة بإعداد برامج توعوية لتعزيز ثقافة الشفافية ورفع مستوى الوعي وفقاً لسياسات وإجراءات حرية المعلومات المعتمدة من الإدارة العليا للجهة.
10. أن تكون الجهة العامة مسؤولة عن مراقبة الامتثال لسياسات وإجراءات حرية المعلومات بشكل دوري ويتم عرضها على المسؤول الأول بالجهة أو من يفوضه، كما يتم تحديد وتوثيق الإجراءات التصحيحية التي سيتم اتخاذها في حال عدم الامتثال وإشعار الجهة التنظيمية والمكتب حسب التسلسل الإداري.

4.4.5.الخطوات الرئيسة للاطلاع على المعلومات أو الحصول عليها

المتطلبات الرئيسية لطلبات الوصول إلى المعلومات العامة أو الحصول عليها:

1. يجب أن يكون الطلب خطياً أو إلكترونياً
2. يجب تعبئة "نموذج طلب معلومات عامة" المعتمد من قبل الجهة العامة
3. يجب أن يكون الطلب لأغراض الوصول إلى المعلومات العامة أو الحصول عليها
4. يجب أن يتضمن نموذج الطلب تفاصيل حول كيفية إرسال القرار النهائي والإشعارات إلى الفرد (العنوان الوطني أو البريد الإلكتروني أو موقع الجهة... الخ)
5. يجب إرسال نموذج الطلب مباشرة إلى الجهة العامة



الشكل 2 الخطوات الرئيسة لطلب الاطلاع على المعلومات العامة أو الحصول عليها

الخطوات الرئيسة لطلب الاطلاع أو الحصول على المعلومات العامة:

أولاً: يتم تقديم الطلبات عن طريق ملء "نموذج طلب معلومات عامة" – إلكتروني أو ورقي – وتقديمه للجهة العامة التي لديها المعلومات.

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

1. **الموافقة:** في حال تمت موافقة الجهة العامة على طلب الوصول إلى المعلومات أو الحصول عليها كليًا أو جزئيًا، فيجب إشعار الفرد خطياً أو إلكترونياً بالرسوم المطبقة، ويجب على الجهة العامة إتاحة هذه المعلومات للفرد خلال فترة زمنية لا تتجاوز (10) أيام عمل من استلام المبلغ.
2. **الرفض:** في حال تم رفض طلب الوصول إلى المعلومات أو الحصول عليها، فيجب أن يكون الرفض خطياً أو إلكترونياً على أن يتضمن المعلومات التالية:
   - تحديد ما إذا كان رفض الطلب كليًا أو جزئيًا
   - أسباب الرفض، إن أمكن
   - الحق في التظلّم على هذا الرفض وكيفية ممارسة هذا الحق.
3. **التمديد:** في حال عدم إمكانية معالجة طلب الوصول إلى المعلومات في الوقت المحدد، ينبغي للجهة العامة تمديد الفترة التي سيتم الرد فيها بمدة معقولة حسب حجم وطبيعة المعلومات المطلوبة – على سبيل المثال لا تتجاوز (30) يوماً إضافيةً – وتزويد الفرد بالمعلومات التالية:
   - إشعار التمديد والتاريخ المتوقع فيه إكمال الطلب
   - أسباب التأخير
   - الحق في التظلّم على هذا التمديد وكيفية ممارسة هذا الحق.
4. **الإشعار:** في حال كانت المعلومات المطلوبة متاحة على موقع الجهة، أو ليست من اختصاصها، فيجب إشعار الفرد بذلك خطياً أو إلكترونياً على أن يتضمن المعلومات التالية:
   - نوع الإشعار، على سبيل المثال، البيانات المطلوبة متاحة على موقع الجهة، أو ليست من اختصاصها.
   - الحق في التظلّم على هذا الإشعار وكيفية ممارسة هذا الحق.

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

4.4.6.أحكام عامة

أولاً: تتولى الجهات العامة مواءمة هذه السياسة مع وثائقها التنظيمية – السياسات والإجراءات – وتعميمها على جميع الجهات التابعة لها أو المرتبطة بها بما يحقق التكامل ويضمن تحقيق الهدف المنشود من إعدادها.

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

ثالثاً: يجب على الجهات العامة الامتثال لهذه السياسة وتوثيق الامتثال بشكل دوري وفقاً للآليات والإجراءات التي تحددها هذه الجهات بعد التنسيق مع المكتب.

رابعاً: تقوم الجهات التنظيمية – بعد التنسيق مع المكتب – بإعداد الآليات والإجراءات والضوابط المتعلقة بمعالجة الشكاوى وفقاً لإطار زمني محدد وحسب التسلسل التنظيمي.

خامساً: يجب على الجهات العامة إشعار المكتب في حال تم رفض طلب الاطلاع أو الحصول على المعلومات العامة أو تمديد الفترة المحددة لتقديم هذه المعلومات وهي ضمن النطاق.

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

سابعاً: يحق للجهات العامة وضع قواعد إضافية لمعالجة الطلبات المتعلقة بأنواع محددة من المعلومات العامة وفقاً لطبيعتها وحساسيتها بعد التنسيق مع المكتب.

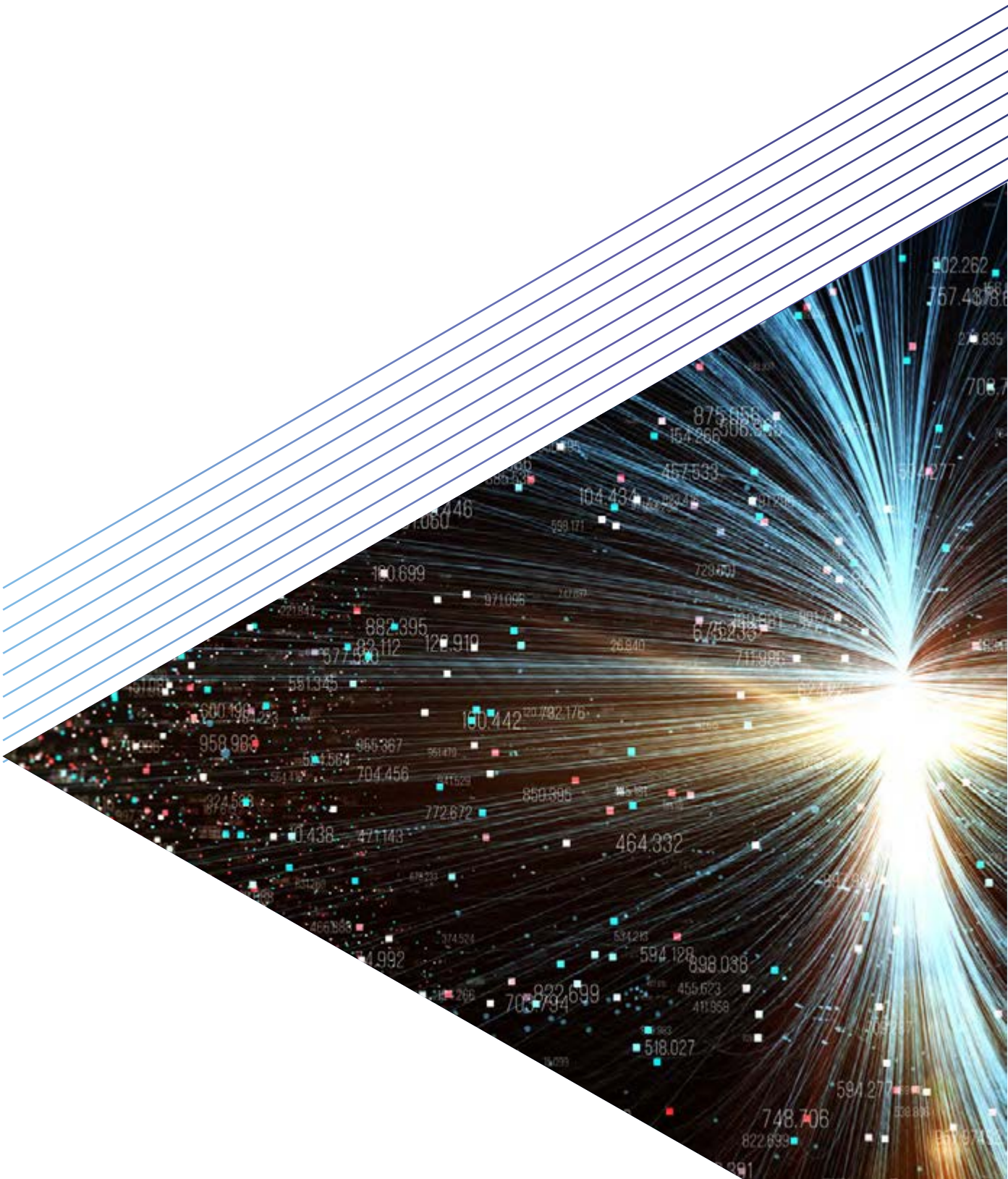
ثامناً: يجب على الجهات العامة إعداد نماذج للاطلاع أو الحصول على المعلومات العامة – سواء أكانت ورقية أو إلكترونية – يحدد فيها المعلومات اللازمة والوسائل الممكنة لتقديم المعلومات المطلوبة.

4.4.7.حرية المعلومات والبيانات المفتوحة

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

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

سياسة البيانات المفتوحة



4.5. سياسة البيانات المفتوحة

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

4.5.1.النطاق

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

4.5.2. المبادئ الرئيسة للبيانات المفتوحة

المبدأ الأول: الأصل في البيانات الإتاحة

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

المبدأ الثاني: الصيغة المفتوحة وإمكانية القراءة آلياً

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 (Data Sets) المفتوحة بصفة منتظمة وإتاحتها للجميع حال توافرها. كما يتم نشر البيانات المجمعة من قبل الجهات العامة في أسرع وقت ممكن بمجرد جمعها، كلما أمكن ذلك، وتُعطى الأولوية 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 الأطراف المعنية على تمكين الجيل القادم من المبتكرين في مجال البيانات المفتوحة وإشراك الأفراد والمؤسسات والجميع بوجه عام في إطلاق قدرات البيانات المفتوحة.

4.5.3. تقييم قيمة البيانات العامة لتحديد مجموعات البيانات المفتوحة

عملية تقييم قيمة البيانات (Data Valuation) لتمكين نشر أكبر قدر ممكن من البيانات المفتوحة تمر بعدة مراحل رئيسة، على النحو التالي:

الخطوة الأولى: تحديد البيانات والمعلومات العامة

لتقييم قيمة البيانات، يجب على الجهة العامة أن تقوم 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 الأخذ بعين الاعتبار مجال البيانات أو القطاع عند تحليل حالات الاستخدام المحتملة، على سبيل المثال، يمكن الاستفادة من البيانات الجيومكانية لخدمة القطاع الصحي. بالإضافة إلى ذلك، يمكن الأخذ بعين الاعتبار مصادر البيانات: بيانات تم جمعها عن طريق المستخدمين بشكل مباشر، بيانات تم جمعها آلياً عن طريق سجلات الأحداث مثل التعاملات الإلكترونية، بيانات مجمّعة أو بيانات تم تطويرها من بيانات أخرى ... إلخ.

الخطوة الثانية: تقييم الفائدة من البيانات

بعد تحديد مجموعات البيانات في الخطوة السابقة، يتم دراسة العوامل الرئيسة المتعلقة بفائدة البيانات (Usefulness) والتي تلعب دوراً 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 الأشخاص ذوي المصلحة المحتملين في سلسلة القيمة بأكملها (Chain Value) على سبيل المثال، يمكن نشر أنماط سلوك المستهلكين لمصنّعي المنتجات وليس فقط لمحلات التجزئة، وبذلك يمكن للجهات معرفة الدوافع الرئيسة لذوي المصلحة، ومنها تحقيق الإيرادات من خلال تطوير منتجات البيانات أو تطوير الخدمات للصالح العام كالتي تساهم في تحسين جودة الحياة.

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

4.5.4.القواعد العامة للبيانات المفتوحة

تحدد سياسة البيانات المفتوحة القواعد العامة والالتزامات التي يجب على الجهات العامة 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 الجهة العامة:

1. تعيين مسؤول البيانات المفتوحة والمعلومات في مكتب الجهة وتتمثل مسؤوليته الأساسية في دعم التخطيط والتنفيذ وإعداد التقارير بشأن أجندة البيانات المفتوحة لدى الجهة وبما يتماشى مع هذه السياسة.

2. وضع خطة للبيانات المفتوحة، تتضمن ما يلي:
- الأهداف الاستراتيجية للبيانات المفتوحة على مستوى الجهة.
- تحديد مجموعات البيانات الخاصة بالجهة المطلوب نشرها على المنصة الوطنية للبيانات المفتوحة وترتيب تلك المجموعات بحسب الأولوية.
- مؤشرات الأداء الرئيسية والأهداف المتعلقة بالبيانات المفتوحة بالنسبة للجهة.
- منهجية ومعايير تحديد الأولوية.
- احتياجات التدريب ذات الصلة بالبيانات المفتوحة.
- الجداول الزمنية لنشر وتحديث البيانات المفتوحة.

3. تطوير وتوثيق العمليات المطلوبة في جميع مراحل دورة حياة البيانات المفتوحة، ويشمل ذلك، على سبيل المثال لا الحصر، ما يلي:
- عمليات تحديد مجموعات البيانات العامة التي سيتم نشرها من جانب الجهة العامة.
- عمليات التحقق من التزام البيانات المفتوحة بالمتطلبات المتعلقة بأمن المعلومات وخصوصية البيانات الشخصية وجودة البيانات ومراجعة ذلك بشكل منتظم والتعامل 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 الجهة وتحسين التأثير العام للبيانات المفتوحة على الصعيد الوطني.

4. ضمان مراجعة خطة البيانات المفتوحة وتحديثها بصفة دورية.
5. تقديم تقرير سنوي للمكتب حول خطة البيانات المفتوحة ومستوى التقدم في تحقيق أهداف البيانات المفتوحة المحددة في الخطة.
6. تنظيم دورة تدريبية عن جميع ما يتعلق بالبيانات المفتوحة بدعم من المكتب أو بالتنسيق معه.
7. إطلاق حملات توعية لضمان معرفة المستخدمين المحتملين بتوافر البيانات المفتوحة المنشورة من جانب الجهة وطبيعتها وجودتها.

تحديد البيانات المفتوحة

يجب على الجهات العامة:

1. تحديد جميع البيانات المصنفة على أنها بيانات عامة بصفة منتظمة وتقييم مدى أولوية كل مجموعة من مجموعات البيانات المحددة لنشرها كبيانات مفتوحة.
2. 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.
3. تسجيل البيانات الوصفية (Metadata) لمجموعات البيانات المفتوحة المحددة ونشرها.

4. دراسة ما إذا كان الجمع بين عدة مجموعات من البيانات المفتوحة سيؤدي إلى رفع مستوى تصنيف البيانات إلى بيانات محمية وفقاً لما يصدر من المكتب من أدلة إرشادية في هذا الخصوص.

نشر البيانات المفتوحة

يجب على الجهات العامة:

1. نشر مجموعات البيانات المفتوحة الخاصة بها على المنصة الوطنية للبيانات المفتوحة.
2. التأكد من نشر البيانات بصيغ معيارية موحدة وهيكلة مقروءة آلياً وغير مسجلة الملكية، تشمل على سبيل المثال لا الحصر: (CSV)، و(JSON)، و(XML)، و(RDF). ويجب أن تكون ملفات مجموعات البيانات مصحوبة بالوثائق ذات الصلة بالصيغة والتعليمات المتعلقة بكيفية استخدامها.
3. توفير البيانات بعدة صيغ كلما أمكن.

تحديث البيانات المفتوحة

يجب على الجهات العامة:

1. ضمان تحديث جميع مجموعات البيانات المفتوحة المنشورة بصفة منتظمة بحسب الآلية المحددة في البيانات الوصفية.
2. المراجعة المستمرة لمجموعات البيانات المنشورة لضمان استيفائها للمتطلبات التنظيمية المحددة.
3. ضمان تحديث البيانات الوصفية وخاصة تحديثها كلما تغيرت عناصر البيانات في مجموعات البيانات المفتوحة المنشورة.
4. الحفاظ على إمكانية تتبع البيانات من خلال توثيق مصادر البيانات والحفاظ على سجل إصدارات مجموعة البيانات.
5. نشر مجموعات البيانات المفتوحة مع تحديد القيود المتعلقة بالجودة وتوثيقها في البيانات الوصفية.

متابعة أداء البيانات المفتوحة

يجب على الجهات العامة:

1. تحليل حجم الطلب على البيانات المفتوحة ومعدل استخدامها لفهم حجم الطلب العام وإعادة ترتيب مجموعات البيانات بحسب الأولوية وفقاً لذلك.
2. جمع طلبات المستخدمين المقدمة بصورة مباشرة أو من خلال المنصة الوطنية للبيانات المفتوحة لنشر مجموعات بيانات إضافية وتحليل تلك الطلبات والرد عليها في حينها.

4.5.5. الأدوار والمسؤوليات

تحدد سياسة البيانات المفتوحة الأدوار والمسؤوليات التالية على المستوى الوطني وعلى مستوى الجهة.

على المستوى الوطني

1. المكتب

يقوم المكتب – بصفته الجهة المسؤولة عن الإشراف على مبادرات البيانات المفتوحة في المملكة – بتنسيق جميع المبادرات والمهام المتعلقة بالبيانات المفتوحة على المستوى الوطني. ويحدد المكتب الاتجاه الاستراتيجي للبيانات المفتوحة في المملكة كما يطور اللوائح والمعايير والإجراءات الوطنية التي تضمن إدارة ونشر البيانات المفتوحة بفعالية على مستوى المملكة وتحقيق الأهداف المنشودة.

تتضمن مسؤوليات المكتب ما يلي:

- **إعداد ومراجعة سياسة البيانات المفتوحة** - إعداد سياسة البيانات المفتوحة (هذه السياسة) وتحديثها، كما يجب مراجعة هذه السياسة بشكل دوري والأخذ بعين الاعتبار التغييرات المحتملة المؤثرة على دورة حياة البيانات المفتوحة.
- **تطوير خطة لتبني سياسة البيانات المفتوحة** - تقديم التوجيهات المستمرة إلى الجهات العامة لتمكين اعتماد وتنفيذ هذه السياسة.
- **الاستشارات المتعلقة بالبيانات المفتوحة** - دعم الجهات العامة للامتثال لهذه السياسة والإجابة عن أي استفسارات تتعلق بتحديد وتحديث ونشر البيانات المفتوحة.
- **قياس مدى الامتثال لمتطلبات البيانات المفتوحة:** قياس مدى امتثال الجهات العامة بشكل دوري وبناءً على آلية الامتثال المحددة (يرجى الرجوع إلى قسم "الامتثال" لمزيد من التفاصيل) والتحقق من مبادرات وأنشطة البيانات المفتوحة عند الحاجة.
- **التثقيف والتوعية بالبيانات المفتوحة:** إطلاق مبادرات التواصل والتدريب ومتابعتها بهدف رفع مستوى الوعي بالبيانات المفتوحة واعتمادها على المستوى الوطني.
- **اعداد قائمة بالبيانات المفتوحة:** مراجعة مجموعات البيانات المفتوحة المتاحة على المستوى الوطني وإعداد قائمة بها تعكس مدى التقدم والإنجاز.
- **أداء البيانات المفتوحة:** تحليل استخدام البيانات المفتوحة وتأثيرها على المستوى الوطني وإيجاد فرص التحسين لإبلاغ الجهات المعنية بها.
- **إعداد ومراجعة ترخيص البيانات المفتوحة:** ترخيص يسمح للمستخدمين مشاركة البيانات المفتوحة وتعديلها واستخدامها.

2. مركز المعلومات الوطني

يعمل مركز المعلومات الوطني بصفته المشغِّل التقني للبوابة الوطنية للبيانات المفتوحة، ويشمل ذلك تصميم المنصة وإنشاءها وتشغيلها وصيانتها.

تتضمن مسؤوليات المركز ما يلي:

- **تطوير وإدارة المنصة الوطنية للبيانات المفتوحة وتشغيلها:** تصميم المنصة وإنشاؤها وصيانتها لضمان تمكين الجهات المُطبقة من نشر مجموعات بياناتها المفتوحة وإدارتها وتحديثها.
- **منح التفويض بالمشاركة على المنصة وإعداد الأدلة الإرشادية:** منح التفويض للجهات العامة وضمان إمكانية وصولها إلى المنصة الوطنية للبيانات المفتوحة. هذا إلى جانب إعداد التوجيهات التشغيلية والتقنية لنشر البيانات المفتوحة على المنصة وتحديثها.
- **تسجيل إحصائيات استخدام المنصة:** تسجيل توجهات وإحصائيات استخدام البيانات المفتوحة المنشورة وتقديمها إلى المكتب والجهات العامة.

على مستوى الجهة

تتمثل المسؤولية الأساسية لجميع الجهات العامة في ضمان نشر بياناتها المفتوحة وفقاً لسياسة البيانات المفتوحة. وبالتالي، يجب على الجهات تعيين من يتولون مسؤولية تنفيذ الأنشطة المتعلقة بالبيانات المفتوحة على النحو المنصوص عليه أدناه.

يتحمل مدير مكتب الجهة ومسؤول البيانات المفتوحة والمعلومات المسؤولية الأساسية المتعلقة بأنشطة البيانات المفتوحة لدى الجهة.

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

- **اعتماد خطة البيانات المفتوحة:** الموافقة على تنفيذ خطة البيانات المفتوحة لدى الجهة والإشراف عليها.
- **تخصيص الأدوار المتعلقة بالبيانات المفتوحة:** تخصيص الأدوار المختلفة المتعلقة بالبيانات المفتوحة.
- **اعتماد التقرير السنوي للبيانات المفتوحة:** اعتماد التقرير السنوي للبيانات المفتوحة الذي يُعده مدير مكتب الجهة.

مدير مكتب الجهة: يعتبر المدير الاستراتيجي للعمليات المتعلقة بالبيانات المفتوحة في جهته، وتتضمن مسؤولياته ما يلي:

- **التخطيط الاستراتيجي للبيانات المفتوحة:** الإشراف على وضع خطة البيانات المفتوحة وتقديمها إلى رئيس الجهة. 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 لا الحصر، تصنيف البيانات وحماية خصوصية البيانات الشخصية وحرية المعلومات.
- **التنسيق مع المكتب:** يعد مدير مكتب الجهة المنسق الأول بين الجهة والمكتب فيما يتعلق بالبيانات المفتوحة. ويتولى حل المشاكل المتعلقة بالبيانات المفتوحة بالنسبة للجهة وتصعيدها إلى المكتب إذا لزم الأمر.

مسؤول البيانات المفتوحة والمعلومات: هو المدير التشغيلي للبيانات المفتوحة داخل الجهة. 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 الجهة ورئيس الجهة.
- **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 بالجهة 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 الجهة.
- **التنسيق مع المكتب (بشكل ثانوي):** يقوم مسؤول البيانات المفتوحة والمعلومات بالتنسيق مع المكتب عند الحاجة كمستوى ثانٍ.

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.

4.5.6.الامتثال

يقوم المكتب – بصفته الجهة التنظيمية للبيانات الوطنية – بمراقبة الامتثال لسياسة البيانات المفتوحة بدعم من الجهات التنظيمية.

شروط الامتثال

1. يجب على جميع الجهات العامة الالتزام بسياسة البيانات المفتوحة وتقديم تقرير سنوي إلى المكتب يشمل، على سبيل المثال لا الحصر، ما يلي:
   - التقدم ومستوى الإنجاز الذي حققته الجهة في خطتها المحددة
   - الأهداف ومؤشرات الأداء الرئيسة المحددة في خطة البيانات المفتوحة
   - عدد مجموعات البيانات المفتوحة المحددة
   - عدد مجموعات البيانات المفتوحة المنشورة
2. تقوم الجهات التنظيمية – بعد التنسيق مع المكتب – بإعداد الآليات والإجراءات والضوابط المتعلقة بتسوية النزاعات المتعلقة بالبيانات المفتوحة وفقاً لإطار زمني محدد وحسب التسلسل التنظيمي.

3. يقـوم المكتـب بمراجعـة التقاريـر السـنوية التـي تـم إعدادهـا مـن قبـل الجهـات العامـة حـول الامتثـال العـام بسياسـة البيانـات المفتوحـة ومشـاركتها مـع الجهـات ذات العلاقـة.
4. يقـوم المكتـب بإجـراء عمليـات التدقيـق بشـكل دوري أو عشـوائي للتحقـق مـن امتثـال الجهـة العامـة ومراجعـة القـرارت المتعلقـة بنشـر البيانـات أو رفـض نشـرها واتخـاذ مايلـزم مـن إجـراءات بهـذا الخصـوص.

التعامل مع حالات عدم الامتثال

عنـد مراجعـة حـالات عـدم الامتثـال، يجـب علـى المكتـب اتبـاع منهجيـة تدريجيـة لتحليـل سـبب عـدم الامتثـال ومـدى الآثـار والمخاطـر المترتبـة علـى ذلـك، والتعامـل مـع هـذه الحـالات وفقـاً للمسـتويات التاليـة:

- **التوعيـة** - يقـوم المكتـب باسـتخدام التوعيـة عنـد التعامـل مـع حـالات عـدم الامتثـال العرضيـة أو غيـر المقصـودة ذات الآثـار السـلبية المحـدودة جـداً.
- **التعـاون** - يقـوم المكتـب بالتعـاون مـع الجهـة العامـة لمنـع أو ردع أو معالجـة حـالات عـدم الامتثـال ذات الآثـار السـلبية المحـدودة الناجمـة عـن الإهمـال وعـدم الامتثـال بأحـكام وقواعـد هـذه السياسـة.
- **التدخـل المباشـر** – يقـوم المكتـب بالتحقيـق فـي حـالات عـدم الامتثـال المسـتمرة والمتكـررة أو المتعمـدة أو ذات الآثـار السـلبية الشـديدة واتخـاذ القـرارات التـي تتناسـب مـع حجـم وطبيعـة الآثـار السـلبية.

سياسة حماية البيانات الشخصية للأطفال ومن في حكمهم

4.6. سياسة حماية البيانات الشخصية للأطفال ومن في حكمهم

تتضمن الحقوق والقواعد العامة التي يجب على الجهات المشمولة بنطاق تطبيق هذه السياسة مراعاتها والالتزام 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.

4.6.1. النطاق

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.

4.6.2.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 المكتب، 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.

4.6.3.القواعد العامة

دون إخلال بالقواعد العامة المنصوص عليها في سياسة حماية البيانات الشخصية، تلتزم جهة التحكم بالقواعد الإضافية التالية التي تضمن المحافظة على خصوصية الأطفال ومن في حكمهم وحماية حقوقهم:

1. أن تكون جهة التحكم مسؤولة عن إعداد وتطبيق السياسات والإجراءات المتعلقة بحماية البيانات الشخصية للأطفال ومن في حكمهم، ويكون المسؤول الأول بالجهة – أو من يفوضه – مسؤولاً عن الموافقة عليها واعتمادها.
2. تلتزم جهة التحكم بتقييم الآثار السلبية والمخاطر المحتملة المترتبة على جميع أنشطة معالجة البيانات الشخصية للأطفال ومن في حكمهم، مع الأخذ بعين الاعتبار مصالحهم وحقوقهم وجميع ما يتعلق بأحوال أسرهم، وعرض نتائج التقييم على المسؤول الأول بالجهة – أو من يفوضه – لتحديد مستوى قبول المخاطر وإقرارها.

3. تلتزم جهة التحكم بمراجعة وتحديث العقود واتفاقيات مستوى الخدمة والتشغيل بما يتوافق مع السياسات والإجراءات المتعلقة بحماية البيانات الشخصية للأطفال ومن في حكمهم المعتمدة من الإدارة العليا للجهة.
4. تلتزم جهة التحكم بإعداد وتوثيق الإجراءات 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 بناءً على قياس شدة الأثر.
5. تلتزم جهة التحكم بإعداد برامج توعوية لتعزيز ثقافة الخصوصية ورفع مستوى الوعي فيما يتعلق بجمع ومعالجة البيانات الشخصية للأطفال ومن في حكمهم.
6. تلتزم جهة التحكم بإعداد وتطوير إشعار الخصوصية بشكل واضح ودقيق وبلغة تناسب هذه الفئة ونشره على الموقع الإلكتروني أو التطبيق الخاص (حسب الدليل الإرشادي لتطوير إشعار الخصوصية الصادر من المكتب) وإشعار الولي – بطريقة تناسب وقت جمع البيانات – بالغرض والأساس النظامي أو الاحتياج الفعلي والوسائل والطرق المستخدمة لجمع ومعالجة ومشاركة البيانات الشخصية للأطفال ومن في حكمهم وكذلك كيفية ممارسة الحقوق، والتدابير الأمنية لحماية خصوصيتهم، وأي تغييرات جوهرية تطرأ عليه.
7. تلتزم جهة التحكم بإشعار الولي عن المصادر الأخرى التي يتم استخدامها في حال تم جمع بيانات إضافية بطريقة غير مباشرة (من جهات أخرى).
8. تلتزم جهة التحكم 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.
9. تلتزم جهة التحكم بتبنّي 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.
10. تلتزم جهة التحكم 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.
11. أن يكون الغرض من جمع البيانات الشخصية للأطفال ومن في حكمهم متوافقاً مع الأنظمة ذات الصلة وذو علاقة مباشرة بنشاط جهة التحكم.
12. أن يكون محتوى البيانات مقتصراً على الحد الأدنى من البيانات اللازمة لتحقيق الغرض من جمعها.

13. أن يتم تقييد جمع البيانات الشخصية للأطفال ومن في حكمهم على المحتوى المعد سلفاً (الموضح في القاعدة 12) ويكون بطريقة عادلة (مباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التضليل).
14. أن يقتصر استخدام البيانات على الغرض التي جُمعت من أجله والذي تمت الموافقة عليه من قبل الولي.
15. تلتزم جهة التحكم بإعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات الشخصية للأطفال ومن في حكمهم وفقاً للأغراض المحددة والأنظمة والتشريعات ذات العلاقة.
16. تلتزم جهة التحكم 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 إلا بعد حصول جهة التحكم على موافقة كتابية من الجهة التنظيمية (وفقاً للقواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة)، بعد تنسيق الجهة التنظيمية مع المكتب متى ما استدعى الأمر ذلك.
17. تلتزم جهة التحكم 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.
18. تلتزم جهة التحكم بتضمين أحكام سياستي الاحتفاظ والتخلص من البيانات في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.
19. تلتزم جهة التحكم بتحديد وتوفير الوسائل التي من خلالها يمكن للولي الوصول إلى البيانات الشخصية للطفل ومن في حكمه وذلك لمراجعتها وتحديثها.
20. تلتزم جهة التحكم 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.
21. يحظر مشاركة البيانات الشخصية للأطفال ومن في حكمهم مع جهات أخرى إلاّ وفقاً 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.
22. تلتزم جهة التحكم بإشعار الولي وأخذ الموافقة منه في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الأغراض المحددة.
23. تلتزم جهة التحكم 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.

24. تلتزم جهة التحكم بأخذ موافقة المكتب – بعد التنسيق مع الجهة التنظيمية – قبل مشاركة البيانات الشخصية للأطفال ومن في حكمهم مع جهات أخرى خارج المملكة.
25. يحظر على جهة التحكم جمع بيانات شخصية من الطفل أو من في حكمه تتعلق بأحد أفراد أسرته في أي حال من الأحوال، ماعدا البيانات الشخصية للولي.
26. تلتزم جهة التحكم 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.
27. تلتزم جهة التحكم 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.
28. تلتزم جهة التحكم 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.
29. تلتزم جهة التحكم بعدم اتخاذ قرارات آلية بناء على معالجة البيانات الشخصية للأطفال ومن في حكمه واستخدامها لأغراض متعددة لها تأثير كبير عليهم، ومنها على سبيل المثال التسويق المباشر.
30. تلتزم جهة التحكم باستخدام الضوابط الإدارية والتدابير التقنية والضمانات القانونية الكافية لحماية البيانات الشخصية للأطفال ومن في حكمهم.
31. تلتزم جهة التحكم بمراقبة الامتثال للسياسات والإجراءات المتعلقة بحماية البيانات الشخصية للأطفال ومن في حكمهم بشكل دوري ويتم عرضها على المسؤول الأول للجهة – أو من يفوضه – كما يتم تحديد وتوثيق الإجراءات التصحيحية التي سيتم اتخاذها في حال عدم الامتثال وإشعار الجهة التنظيمية والمكتب حسب التسلسل التنظيمي.

4.6.4. الاستثناءات

1. لا يشترط الحصول على موافقة الولي في حال كانت الخدمة المقدمة للطفل أو من في حكمه هي خدمة وقائية أو استشارية وفقاً لمهام واختصاصات جهة التحكم (الجهات ذات العلاقة بحماية الطفل)، على أن تلتزم الجهة بجمع الحد الأدنى من البيانات اللازمة لتحقيق الغرض، وإتلافها فور الانتهاء من تقديم الخدمة.
2. لا يشترط الحصول على موافقة الولي في حال الإفصاح عن بياناته الشخصية لطرف ثالث من أجل تنفيذ التزام مشروع على جهة التحكم أو لتنفيذ نظام آخر أو لتنفيذ اتفاقية تكون المملكة طرفاً فيه أو كانت الجهة التي سيتم الإفصاح لها جهة قضائية أو أمنية.

3. 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 مرّة أخرى أو لأي غرض آخر، ولا يتم الإفصاح عنها، وتقوم جهة التحكم بحذفها من سجلاتها فور الاستجابة لطلب الطفل.
4. 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.
5. 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 جهة التحكم تزويد الولي بإشعار بذلك.

4.6.5. أحكام عامة

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

ثانياً: تلتزم الجهة التنظيمية بمراقبة وتوثيق الامتثال لهذه السياسة بشكل دوري.

ثالثاً: تلتزم جهة التحكم بالامتثال لهذه السياسة وتوثيق الامتثال وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية.

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

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

سادساً: يمارس المكتب أدوار ومهام الجهات التنظيمية على جهة التحكم غير الخاضعة لجهات تنظيمية.

سابعاً: يحق للجهة التنظيمية وضع قواعد إضافية لمعالجة أنواع محددة من البيانات الشخصية للأطفال ومن في حكمهم وفقاً لطبيعة وحساسية هذه البيانات بعد التنسيق مع المكتب.

ثامناً: تلتزم الجهة التنظيمية – بعد التنسيق مع المكتب – بإعداد الآليات والإجراءات التي تنظم عملية معالجة الشكاوى والاعتراضات وفقاً لإطار زمني محدد وحسب التسلسل التنظيمي للجهات.

4.6.6. الأحكام الخاصة المتعلقة بالولي الشرعي

1. يجوز لجهة التحكم أن تحصل على البيانات الشخصية للولي من الطفل ومن في حكمه مباشرة، على أن تلتزم بالحصول على الحد الأدنى من البيانات اللازمة – الاسم وطريقة التواصل مع الولي – فقط من أجل إشعار الولي والحصول على موافقته.
2. تلتزم جهة التحكم باستخدام الوسائل المناسبة للتحقق من هوية الولي قبل أخذ موافقته ومنحه الوصول إلى بيانات الطفل الشخصية ومن في حكمه وفقاً للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.
3. في حال تم طلب موافقة الولي ولم يقدم موافقته خلال (10) أيام من تاريخ التواصل معه، تلتزم جهة التحكم بإتلاف بيانات الطفل الشخصية ومن في حكمه وبيانات الولي التي جُمعت.
4. تلتزم جهة التحكم بعدم استخدام البيانات الشخصية للولي لغير الغرض الذي جُمعت من أجله في حدود الموافقة على جمع ومعالجة البيانات الشخصية للطفل ومن في حكمه.
5. تلتزم جهة التحكم بإشعار الولي بالطلبات المقدمة من الطفل ومن في حكمه فيما يتعلق بالبيانات الشخصية له وأخذ موافقته عليها.

القواعد العامة لنقل البيانات الشخصية خارج الجدود الجغرافية للمملكة

4.7. 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 جهات التحكم والمعالجة حيال عمليات نقل البيانات الشخصية خارج الحدود الجغرافية، وتوفير الوسائل المناسبة التي تمكّن أصحاب البيانات من ممارسة حقوقهم، وتحديد أدوار ومسؤوليات هذه الجهات بالإضافة إلى الجهات التنظيمية والجهات الإشرافية على تطبيق أحكام هذه السياسات.

4.7.1. النطاق

تنطبق أحكام هذه الوثيقة على جميع الجهات العامة والخاصة وكذلك الجهات غير الربحية في المملكة – المشمولة بنطاق تطبيق سياسة حماية البيانات الشخصية – والتي تقوم بنقل البيانات الشخصية إلى جهات أخرى خارج الحدود الجغرافية للمملكة بغرض معالجتها، ويستثنى من ذلك نقل البيانات الشخصية من وإلى الأفراد مباشرة.

4.7.2. حقوق أصحاب البيانات

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

- **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 وبعد.
- **ثانياً:** الحق في الرجوع عن موافقته على معالجة بياناته الشخصية خارج الحدود – في أي وقت – ما لم يكن الغرض من نقل البيانات تحقيقاً للمصلحة العامة، أو حمايةً للمصالح الحيوية للأفراد، أو تنفيذاً لمتطلبات نظامية.
- **ثالثاً:** الحق في الوصول إلى بياناته الشخصية لدى جهة التحكم/جهة المعالجة الخارجية، وذلك للاطلاع عليها، وطلب تصحيحها، أو إتمامها، أو تحديثها، وطلب إتلاف ما انتهت الحاجة إليه منها، والحصول على نسخة منها بصيغة واضحة.

4.7.3. التزامات الجهات

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

1. إذا كانت جهة المعالجة الخارجية المسند إليها أنشطة معالجة البيانات الشخصية في دولة ضمن قائمة الاعتماد، فتقوم جهة التحكم/جهة المعالجة الداخلية بأخذ موافقة كتابية من الجهة التنظيمية على نقل البيانات، وعلى الجهة التنظيمية التنسيق مع المكتب.
2. إذا كانت جهة المعالجة الخارجية في دولة ليست ضمن قائمة الاعتماد، فإن نقل البيانات الشخصية خارج الحدود الجغرافية للمملكة يتطلب مستوى كافٍ من الحماية – لا يقل عن مستوى الحماية الذي كفلته سياسة حماية البيانات الشخصية الصادرة من المكتب – بعد إجراء تقييم مستوى الحماية التي توفرها جهة المعالجة الخارجية.
3. إذا لم يكن هناك مستوى كافٍ من الحماية، فتقوم الجهة بوضع ضمانات مناسبة لحماية حقوق أصحاب البيانات، ومنها على سبيل المثال، استخدام البنود القياسية، أو القواعد الملزمة.
4. إذا لم تتمكن الجهة من توفير الضمانات الكافية، فيمكن الاعتماد على أحد الاستثناءات النظامية التي تتطلب نقل البيانات والموضحة في البند (ثالثاً) أدناه.

في جميع الحالات الواردة في الفقرات (2) و (3) و(4) أعلاه، يجب على جهة التحكم 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 جهة التحكم/جهة المعالجة الخارجية ستوفر مستوى كافٍ من الحماية لحقوق أصحاب البيانات وعرض نتائج التقييم على (المسؤول الأول للجهة) 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 ملائماً في جميع الظروف:

أ- معايير التقييم العامة

-طبيعة وحساسية البيانات: يجب على الجهة 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 الجهة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار ما إذا كانت المعالجة ستتم بشكل مقيّد أو عرضي – لمرة واحدة فقط أو لفترة محدودة – أو ستتم بشكل متكرر ومنتظم، حيث إن البيانات الشخصية التي سيتم معالجتها بشكل منتظم وعلى المدى الطويل تتطلب مستوى عالٍ من الحماية.

- منشأ البيانات: يجب على الجهة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار الدولة التي جُمعت 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 الجهة 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 الجهة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار الإجراءات الإدارية والتدابير التقنية والضوابط المادية المعتمدة في سياسات الجهة لأمن المعلومات، كالتشفير والضوابط الأمنية والمعايير الدولية.

إذا أظهرت نتائج تقييم مستوى الحماية – بناءً على المعايير العامة – أنه بالظروف الخاصة للحالة تكون الآثار السلبية على حقوق أصحاب البيانات محدودة والمخاطر المحتملة منخفضة، فقد لا يكون تقييم مستوى الحماية – بناءً على المعايير القانونية – ضرورياً في هذه الحالة.

ب- معايير التقييم القانونية:

يجب أن تقوم 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 كافٍ، فيجب عليها توفير الضمانات المناسبة لحماية البيانات الشخصية، ومنها:

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

- القواعد المشتركة الملزمة: يجب على جهة التحكم وجهة المعالجة – كل على حدة – 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 والإشعار عنها على أن تتم الموافقة عليها من قبل المكتب، ويتم تضمين هذه القواعد المشتركة بصفتها ملحقاً لاتفاقيات مستوى الخدمة أو العقود المبرمة بين الجهتين. كما يجب على جهة التحكم أخذ موافقة الجهة التنظيمية عند وجود أي التزام قانوني تخضع له هذه الجهة أو إحدى الجهات التابعة لها في دولة أخرى يرجّح أن يكون له أثر سلبي على الضمانات التي توفرها القواعد المشتركة الملزمة.

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

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

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

ثالثاً: الاستثناءات لحالات محددة

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

1. استنادًا على موافقة أصحاب البيانات.
2. تنفيذاً لالتزام تعاقدي ويكون صاحب البيانات طرفاً فيه.
3. تنفيذاً لمتطلبات قضائية.
4. تنفيذاً لأحكام نظام آخر أو اتفاقية دولية تكون المملكة طرفاً فيها.
5. للمحافظة على المصلحة العامة بما في ذلك حماية الصحة أو السلامة العامة.
6. لحماية المصالح الحيوية لأصحاب البيانات.

في جميع هذه الحالات الواردة في الفقرات (1)، (2)، (3)، (4)، (5)، يجب على جهة التحكم أو المعالجة الداخلية الحصول على موافقة كتابية من الجهة التنظيمية على نقل البيانات – كل حالة على حدة – وعلى الجهة التنظيمية التنسيق مع المكتب. أما ما يتعلق بالحالة الواردة في الفقرة (6) فيجب على جهة التحكم أو جهة المعالجة إشعار الجهة التنظيمية فقط، وعلى الجهة التنظيمية إشعار المكتب بذلك.

4.7.4. أحكام عامة

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

ثانياً: تقوم الجهات التنظيمية بمراقبة امتثال الجهات التابعة لها أو المرتبطة بها لهذه القواعد بشكل دوري.

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

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

خامساً: يمارس المكتب أدوار الجهات التنظيمية ومهامها على جهات التحكم غير الخاضعة لجهات تنظيمية.

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

سابعاً: يقوم المكتب بمراجعة معايير التقييم – العامة والقانونية – المتعلقة بحماية البيانات الشخصية عند نقلها خارج الحدود الجغرافية للمملكة واتخاذ القرارات المنظمة لها.

ثامناً: يقوم المكتب 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.

تاسعاً: يقوم المكتب بإعداد قائمة الاعتماد ومراجعتها ونشرها وتحديثها بشكل دوري وذلك بناءً على تقييم مستوى الحماية المناسب بحيث لا يقل عن مستوى الحماية الذي كفلته سياسة حماية البيانات الشخصية الصادرة من المكتب.

عاشراً: يقوم المكتب بإعداد البنود القياسية ومراجعتها لحماية البيانات الشخصية.


0,64 0,69 0,63 0,65
0,67 0,72 0,65 0,68 0,62
0,24 0,29 0,28 0,23 0,22 0,18
0,30 0,35 0,34 0,29 0,28 0,24
0,36 0,41 0,39 0,35 0,33 0,29

السياسات غير المعتمدة من قبل مجلس الإدارة

5.السياسات غير المعتمدة من قبل مجلس الإدارة

بالإضافة السياسات السبعة الخاصة بحوكمة البيانات الوطنية، عُمِل على سياستين إضافيتين ولكنها لم تعتمد من قبل مجلس الإدارة حتى الآن:

1. سياسة تحقيق الإيرادات من البيانات

تتضمن مجموعة من المبادئ والقواعد والالتزامات لمختلف الأطراف المشاركة في تسويق البيانات وذلك لتحقيق الإيرادات من البيانات ومنتجات البيانات.

2. القواعد العامة لحوكمة البيانات عند تطوير أو استخدام أنظمة الذكاء الاصطناعي

مساعدة الجهات على استخدام المعايير القياسية والأخلاقيات عند بناء وتطوير الحلول المبنية على تقنيات الذكاء الاصطناعي وتطويرها استخدامها بشكل مسؤول وضمان المحافظة على خصوصية أصحاب البيانات الشخصية وحماية حقوقهم المتعلقة بجمع بياناتهم ومعالجتها.

سياسة تحقيق الإيرادات من البيانات

5.1. سياسة تحقيق الإيرادات من البيانات

تسعى المملكة إلى الاستفادة من الكم الهائل من البيانات التي تجمعها أو تنتجها أو تتعامل معها الجهات في القطاعين العام والخاص، بالإضافة إلى الجهات غير الربحية، لتحسين كفاءة الأداء وزيادة الإنتاجية، وتسهيل تقديم الخدمات بأساليب إبداعية ومبتكرة، وتعزيز التنمية الاقتصادية، وتحسين جودة الحياة عن طريق إجراء التنبؤات الدقيقة واستشراف المستقبل ومساندة عملية اتخاذ القرار، وتمكين الريادة والابتكار وخلق فرص استثمارية نوعية في عدد من المجالات المختلفة.

5.1.1. النطاق

تنطبق أحكام هذه السياسة على أي تسويق للبيانات الحكومية أو المنتجات المبنية على هذه البيانات المعالجة جزئياً أو كلياً، ويستثنى من نطاق تطبيق هذه السياسة بيانات القطاع الخاص وكذلك أي نشاط متعلق بجمع أي منتج بيانات القطاع الخاص ومعالجتة وتطويره.

5.1.2. السياسات ذات العلاقة

تلتزم جميع الجهات المشمولة بنطاق تطبيق هذه السياسة بالامتثال للأنظمة واللوائح والسياسات ذات العلاقة، بما في ذلك سياسات حوكمة البيانات الوطنية الصادرة من المكتب والمعتمدة من مجلس إدارة الهيئة السعودية للبيانات والذكاء الاصطناعي، ومنها على وجه التحديد السياسات الموضّحة أدناه التي تحدد التزامات مزودي البيانات عند تحقيق الإيرادات من البيانات أو منتجات البيانات:

1. **سياسة تصنيف البيانات:** تهدف هذه السياسة إلى وضع إطار وطني موحّد لتصنيف البيانات –التي تنتجها أو تعالجها الجهات الحكومية– ينظّم حق الاطلاع على هذه البيانات وآلية التعامل معها.
2. **سياسة حماية البيانات الشخصية:** تهدف هذه السياسة إلى وضع الأحكام والقواعد العامة التي تنظّم جمع ومعالجة البيانات الشخصية.
3. **سياسة مشاركة البيانات:** تهدف هذه السياسة إلى تعزيز مبدأ مشاركة البيانات الرئيسة التي تنتجها الجهات الحكومية لتحقيق التكامل وتبني مبدأ المرّة الواحدة للحصول على البيانات من مصادرها الصحيحة والحد من ازدواجيتها وتعارضها وتعدد مصادرها.
4. **سياسة حرية المعلومات:** تهدف هذه السياسة إلى تنظيم حق الاطلاع أو الحصول على البيانات غير المصنّفة على إحدى درجات السرية التي تنتجها الجهات الحكومية بما يعزز منظومة النزاهة والشفافية.

5. **سياسة البيانات المفتوحة:** تهدف هذه السياسة إلى إتاحة مجموعة محددة من البيانات غير المصنّفة على إحدى درجات السرية التي تنتجها الجهات الحكومية للباحثين وروّاد الأعمال والمبتكرين والشركات الناشئة بما يضمن تهيئة بيئة مواتية لنمو الأعمال التجارية.
6. **ضوابط إدارة البيانات الوطنية ومعاييرها:** تهدف هذه الوثيقة إلى تحديد الحد الأدنى من المواصفات والضوابط المتعلقة بكل مجال من المجالات الرئيسية لإدارة البيانات لتعظيم الفائدة من البيانات الوطنية.

5.1.3. المبادئ الأساسية لتحقيق الإيرادات من البيانات

المبدأ الأول: البيانات أصول وطنية

تعتبر البيانات التي تنتجها الجهات الحكومية أحد الأصول الوطنية التي ينبغي أن تديرها هذه الجهات بما يحقق المصلحة العامة وفقاً لقرار مجلس الوزراء رقم (40) وتاريخ 1427/2/27هـ القاضي في الفقرة (1) تعد المعلومات والبيانات الحكومية ثروة وطنية، يجب على جميع الجهات الحكومية تنميتها، ولضمان المحافظة عليها بصفتها أصولاً وطنية، تحتفظ الجهة الحكومية بحقوق الملكية الفكرية الخاصة بالبيانات ولا يجوز استخدامها من قبل أي جهة أخرى إلّا بموجب اتفاقية مشاركة البيانات بين الجهات، أما ما يتعلق بمنتجات البيانات، فيحق لأي جهة طورت منتجاً مبنياً على البيانات أن تحتفظ بحقوق الملكية الفكرية المطوّرة حسب الأنظمة واللوائح ذات الصلة.

المبدأ الثاني: تنمية الإيرادات

تعتبر البيانات أصولاً قيّمة يمكن الاستفادة منها في رفع كفاء الإنفاق وتنمية الإيرادات المتعلقة بالبيانات لضمان استدامة الخدمات التي تقدمها الجهات الحكومية.

المبدأ الثالث: الخصوصية بالتصميم

الأخذ بعين الاعتبار متطلبات الخصوصية منذ المراحل الأولى لإجراءات تحقيق الإيرادات من البيانات ومنتجات البيانات بما يتوافق مع سياسة حماية البيانات الشخصية.

المبدأ الرابع: الأصل في البيانات الإتاحة

يجب الا يتعارض تسويق البيانات غير المعالجة أو منتجات البيانات مع سياسة البيانات المفتوحة والجهود المبذولة من قبل الجهات الحكومية لتعزيز مساهمتها في مبادرات البيانات المفتوحة واستراتيجياتها.

المبدأ الخامس: تعزيز ثقافة المشاركة

يجب الا يتعارض تسويق البيانات غير المعالجة أو منتجات البيانات مع سياسة مشاركة البيانات والجهود المبذولة لتحقيق التكامل بين الجهات الحكومية والحصول على البيانات من مصادرها الصحيحة.

المبدأ السادس: منع الممارسات الاحتكارية

تلعب الجهات الحكومية دوراً أساسياً في صناعة سوق البيانات وتشجّع على الابتكار في القطاع الخاص. وبالتالي يجب على الجهات الحكومية تقييد أي ميزة غير عادلة (بما في ذلك الاحتكار) وتعزيز الوصول المتساوي إلى البيانات، وإزالة الحواجز التي تعيق تطوير منتجات البيانات من قبل القطاع الخاص مما يؤدي إلى سوق عادلة وتنافسية للبيانات.

المبدأ السابع: الشفافية

يجب توثيق المعلومات المتعلقة بتحقيق الإيرادات من البيانات وإتاحتها عند الحاجة، وهذا يتضمن على سبيل المثال لا الحصر نموذج تحقيق الإيرادات، والبيانات المستخدمة، ونموذج التسعير المعتمد، وتحصيل الإيرادات.

المبدأ الثامن: استرداد التكاليف

تسعى الجهات الحكومية إلى تحقيق أقل قدر ممكن من الأرباح من البيانات أو منتجات البيانات، مع المحافظة على دورها بصفتها صانع سوق ومطور اقتصادي وفقاً للمبدأ السادس. كما يجب أن تعتمد الجهات الحكومية نموذج تسعير استرداد التكاليف ما لم يكن العائد من الاستثمار أو سعر السوق مبرراً.

5.1.4. إطار سياسة تحقيق الإيرادات – القواعد العامة

تماشياً مع نطاق تطبيق هذه السياسة، طُوّر إطار عمل لتنظيم تحقيق الإيرادات من البيانات غير المعالجة ومنتجات البيانات، ويمكن تحقيق الإيرادات بأحد الطرق التالية:

- مشاركة البيانات غير المعالجة بمقابل مالي.
- تقديم الرؤى أو التحليلات.
- تقديم منتج أو خدمات مثل: منصات التحليلات.

نماذج تحقيق الإيرادات

نموذج تحقيق الإيرادات (revenue model) هو الهيكل الذي ينص على كسب الإيرادات الخاصة بنموذج العمل (business model) ويشمل المنتج أو الخدمة ذات القيمة المضافة، والمستهلكين المستهدفين. وبناءً على ذلك، فهناك عدة نماذج شائعة، لكل نموذج منها استخدامات تتنوع حسب طبيعة المنتج أو الخدمة، ومنها على سبيل المثال لا الحصر: الإعلانات، والميزة التنافسية، والتراخيص، والعمولة، وغيرها من النماذج الأخرى.

نماذج التسعير

نموذج التسعير (Pricing Model) هو الآلية المستخدمة لتحديد الأسعار التقديرية للبيانات ومنتجات البيانات. وبناءً على ذلك فهناك عدد من النماذج تُستخدم حسب نموذج تحقيق الإيرادات وحسب المنتج أو الخدمة، ومنها على سبيل المثال:

1. **نموذج التسعير التجاري (تحقيق الأرباح):** تقدير سعر البيانات ومنتجات البيانات بناءً على سعر المنتجات أو الخدمات المماثلة في السوق.
2. **نموذج التكلفة الهامشية (Marginal Cost Model):** حساب تكاليف توفير البيانات لمستفيد آخر وعادةً ما يكون قريب من الصفر، أو مكافئاً لتقديمها بشكل مجاني.
3. **نموذج استرداد التكاليف (Cost Recovery):** حساب التكلفة الهامشية بالإضافة إلى تكاليف توفير البيانات أو تطوير منتجات البيانات.
4. **نموذج استرداد التكاليف بلس (Cost Recovery + ROI):** حساب تكاليف توفير البيانات أو منتجات البيانات بالإضافة إلى تحديد نسبة محددة كعائد على الاستثمار مما يسمح باسترداد التكاليف وإضافة هامش ربح على الخدمات ذات القيمة المضافة.

ولتحقيق الهدف المنشود من هذه السياسة، يعتبر النموذجان المشار إليهما في الفقرة (3) والفقرة (4) أعلاه هما نموذجا التسعير المعتمدان من المكتب عند قيام الجهات الحكومية بتحقيق الإيرادات من البيانات أو منتجات البيانات.

إطار تحقيق الإيرادات

يتضمن إطار تحقيق الإيرادات من البيانات ثلاثة مسارات رئيسة كل واحد من هذه المسارات يصف القواعد المتعلقة بتحقيق الإيرادات من البيانات ومنتجات البيانات، ولضمان تحقيق المنافسة العادلة ومنع الممارسات الاحتكارية، يجب على الجهات الحكومية الالتزام بالتالي:

- إتاحة أكبر قدر ممكن من البيانات المصنّفة (على مستوى: عام) ونشرها على أنها بيانات مفتوحة –مجاناً وبدون مقابل– وفقاً لسياسة البيانات المفتوحة المعدّة من قبل المكتب.
- تبادل البيانات التابعة لها وإتاحة البيانات المشتركة منها إلكترونياً مجاناً (دون مقابل) للجهات الحكومية الأخرى المستفيدة تنفيذاً للأمر السامي الكريم رقم 17850 وتاريخ 16/3/1441هـ.

المسار الأول: الجدول (1) أدناه يوضح التزامات الجهات الحكومية تجاه الجهات الحكومية (G2G).

	غير المعالجة	منتجات البيانات
البيانات المفتوحة	مجاناً	استرداد التكاليف
البيانات المصنّفة (مقيّد، عام)	مجاناً	استرداد التكاليف

الجدول 1 التزامات الجهات الحكومية تجاه الجهات الحكومية

القواعد العامة المعلقة بالمسار الأول

1. لا تفرض الجهات الحكومية رسوماً على البيانات غير المعالجة، سواءً عند إتاحة البيانات المفتوحة أو عند مشاركة البيانات المصنّفة (على مستوى: مقيّد أو عام) مع جهات حكومية أخرى لتنفيذ المهام والاختصاصات المنوطة بها. كما تضمن هذه القاعدة الالتزام بالأمر السامي الكريم رقم 17850 وتاريخ 1441/3/16هـ المشار إليه أعلاه.
2. يمكن للجهات الحكومية أن تحقق إيرادات من منتجات البيانات المطورة من البيانات المفتوحة أو البيانات المصنّفة (على مستوى: مقيّد أو عام)، على أن تُقدم هذه المنتجات عن طريق الجهة أو الجهات الخاصة ويكون التسعير وفقاً لنموذج استرداد التكاليف المنصوص عليه في هذه السياسة.
3. تلتزم الجهات الحكومية بأحكام سياسة مشاركة البيانات ومتطلبات حماية البيانات الشخصية عند تطوير منتجات البيانات، ومنها على سبيل المثال إجراء المعالجة المسبقة للبيانات الشخصية قبل مشاركتها مثل: التعتيم (Data Masking) أو المزج (Data Scrambling) أو التعمية (Data Anonymization).
4. يجب على الجهات الحكومية أن تقدم –وفقاً للمبدأ السادس– وصولاً متساوياً لأي بيانات أو منتج بيانات يُستخدم لتحقيق الإيرادات من قبل الجهات الخاصة وذلك لتحقيق المنافسة العادلة ومنع الممارسات الاحتكارية.

المسار الثاني: الجدول (2) أدناه يوضح التزامات الجهات الحكومية تجاه الجهات الخاصة أو الأفراد (G2B/G2I)

	البيانات غير المعالجة	منتجات البيانات
البيانات المفتوحة	مجاناً	استرداد التكاليف
البيانات المصنّفة (مقيّد، عام)	استرداد التكاليف	استرداد التكاليف (بلس)

الجدول 2 التزامات الجهات الحكومية تجاه الجهات الخاصة والأفراد

القواعد العامة المتعلقة بالمسار الثاني

1. لا تفرض الجهات الحكومية رسوماً على البيانات المفتوحة (غير المعالجة) التي تُتاح للعموم (الجهات الخاصة والأفراد).
2. يمكن للجهات الحكومية تحقيق إيرادات من منتجات البيانات المطورة من البيانات المفتوحة، على أن تُقدم هذه المنتجات عن طريق الجهة أو الجهات الخاصة ويكون التسعير وفقاً لنموذج استرداد التكاليف المنصوص عليه في هذه السياسة.
3. يمكن للجهات الحكومية تحقيق إيرادات من البيانات غير المعالجة المصنّفة (على مستوى: مقيّد أو عام)، على أن تُزود هذه البيانات عن طريق الجهة أو الجهات الخاصة ويكون التسعير وفقاً لنموذج استرداد التكاليف المنصوص عليه في هذه السياسة.
4. يمكن للجهات الحكومية تحقيق إيرادات من منتجات البيانات (البيانات المعالجة) المصنّفة (على مستوى: مقيّد أو عام)، على أن تُقدم هذه المنتجات عن طريق الجهة أو الجهات الخاصة ويكون التسعير وفقاً لنموذج استرداد التكاليف (بلس) المنصوص عليه في هذه السياسة.
5. تلتزم الجهات الحكومية بأحكام سياسة مشاركة البيانات ومتطلبات حماية البيانات الشخصية عند مشاركة البيانات غير المعالجة أو تطوير منتجات البيانات، ومنها على سبيل المثال إجراء المعالجة المسبقة للبيانات الشخصية قبل مشاركتها مع الجهات الخاصة أو الأفراد مثل التعتيم (Data Masking) أو المزج (Data Scrambling) أو التعمية (Data anonymization).
6. يجب على الجهات الحكومية أن تقدم –وفقاً للمبدأ السادس– وصولاً متساوياً لأي بيانات أو منتج بيانات يُستخدم لتحقيق الإيرادات من قبل الجهات الخاصة أو الأفراد وذلك لتحقيق المنافسة العادلة ومنع الممارسات الاحتكارية.

المسار الثالث: الجدول (3) يوضح التزامات الجهات الخاصة تجاه الجهات الحكومية والجهات الخاصة والأفراد(B2G/B2B/B2I) وفقاً للسياسات الصادرة من الجهات التنظيمية والمكتب والجهات الأخرى ذات العلاقة، ومنها على سبيل المثال الهيئة العامة للمنافسة.

	غير المعالجة	منتجات البيانات
البيانات المفتوحة	غير خاضعة لأحكام السياسة، ويمكن تنظيمها وفقاً للمبادئ التوجيهية المعتمدة من الجهات التنظيمية والجهات ذات العلاقة	غير خاضعة لأحكام السياسة، ويمكن تنظيمها وفقاً للمبادئ التوجيهية ونماذج التسعير التجاري الموصى بها من الجهات التنظيمية والجهات ذات العلاقة
البيانات الحكومية التي تعالجها الجهات الخاصة (مقيّد، عام)	استرداد التكاليف (B2G) استرداد التكاليف بلس (B2B/B2I)	استرداد التكاليف (بلس)
بيانات الجهات الخاصة	غير خاضعة لأحكام السياسة، ويمكن تحديدها وفقاً لنماذج التسعير التجاري الموصى بها من الجهات التنظيمية والجهات ذات العلاقة	غير خاضعة لأحكام السياسة، ويمكن تحديدها وفقاً لنماذج التسعير التجاري الموصى بها من الجهات التنظيمية والجهات ذات العلاقة

الجدول 3 التزامات الجهات الخاصة تجاه الجهات الحكومية والجهات الخاصة والأفراد

القواعد العامة المتعلقة بالمسار الثالث

1. يمكن للجهات الخاصة أن تحقق إيرادات من منتجات البيانات المطورة من البيانات المفتوحة، علماً أنه لا يخضع تسعير منتجات البيانات لأحكام هذه السياسة، وإنما يخضع لنماذج التسعير الموصى بها من الجهات التنظيمية والجهات ذات العلاقة، ومنها على سبيل المثال الهيئة العامة للمنافسة.
2. لا يجوز للجهات الخاصة –في حال تم منحها ترخيص لاستخدام البيانات من قبل جهة حكومية– إعادة استخدام البيانات الحكومية غير المعالجة لأغراض غير الأغراض المحددة في اتفاقيات مشاركة البيانات أو مشاركتها مع جهات أخرى سواء بمقابل مالي أو بدون مقابل. تنطبق هذه القاعدة على جميع الجهات الخاصة، بما في ذلك الاتفاقيات التجارية التي تحكم العلاقة بين الجهة الخاصة والجهة الحكومية.
3. يمكن للجهات الخاصة أن تحقق إيرادات من البيانات غير المعالجة التي يتم الحصول عليها من الجهات الحكومية المصنّفة (على مستوى: مقيّد أو عام) عند مشاركتها مع جهات حكومية أخرى، على أن يكون التسعير وفقاً لنموذج استرداد التكاليف المنصوص عليه في هذه السياسة.
4. يمكن للجهات الخاصة أن تحقق إيرادات من منتجات البيانات التي يتم الحصول عليها من الجهات الحكومية المصنّفة (على مستوى: مقيّد أو عام) عند تقديمها إلى جهات خاصة أخرى أو أفراد، على أن يكون التسعير وفقاً لنموذج استرداد التكاليف (بلس) المنصوص عليه في هذه السياسة.
5. يوصي مكتب البيانات بأن تقوم الجهات التنظيمية بالتنسيق مع الجهات ذات العلاقة بتحديد نماذج التسعير التي يمكن استخدامها من قبل الجهات الخاصة لمنع الممارسات الاحتكارية وتحقيق المنافسة العادلة.

5.1.5. نموذج التسعير (استرداد التكاليف)

معايير تسعير البيانات

لإجراء تسعير البيانات ومنتجات البيانات وفقاً لنماذج التسعير الموضحة في هذه السياسة، يتم الأخذ بعين الاعتبار العوامل التالية:

- ندرة البيانات (بيانات خام أو أولية، عدد الجهات المنشأة للبيانات، ...إلخ.
- تعدد مصادر البيانات (عدد مصادر البيانات التي عن طريقها يتم ربط أو جمع البيانات لتقديم الرؤى والتحليلات، ومدى حصرية هذه المصادر، وحجم الحقول، ...إلخ.
- عدد المشتركين/ العملاء للجهة (مدى تنوّع الشرائح، ...إلخ.
- قيمة البيانات (طبيعة ومحتوى البيانات "شخصية أو غير شخصية، معماه أو غير معماه، مجمّعة أو غير مجمّعة، ...إلخ" جودة البيانات، الاستخدامات الممكنة، المستفيدين المستهدفين، ...إلخ.
- نوع البيانات (بيانات مهيكلة، شبه مهيكلة، غير مهيكلة)
- حجم البيانات (الحجم بالجيجابايت، عدد السجلات، ...إلخ.
- سعر البيانات ومنتجات البيانات المماثلة في السوق.

آلية تسعير استرداد التكاليف

بناءً على المبادئ الأساسية والقواعد العامة الموضحة أعلاه، يجب على الجهات اتباع الإرشادات التالية لتقدير قيمة البيانات ومنتجات البيانات غير المعالجة:

1. يجب على الجهة أخذ العوامل التالية بعين الاعتبار عند تسعير استرداد التكاليف:

السعر = تكاليف جمع البيانات + تكاليف التطوير

- تكاليف جمع البيانات: التكاليف المتعلقة بجمع البيانات وتنقيتها وتهيئتها والاحتفاظ بها (الأجهزة، والبرامج والتطبيقات، والموارد البشرية، والاستضافة، ...إلخ.
- تكلفة التطوير: التكلفة المتعلقة بتحليل أو تمثيل او معالجة البيانات، بالإضافة إلى الأنشطة الأخرى المتعلقة تطوير منتج البيانات (الأجهزة، والبرامج والتطبيقات، والموارد البشرية، ...إلخ، وكذلك التكاليف المتعلقة بالربط المباشر.

يجب على الجهة تقدير تكاليف الجمع والتطوير لكل وحدة من منتجات البيانات على حدة. كما يجب تبرير أي تكاليف إضافية يتم تحملها وإضافتها إلى التكاليف المذكورة أعلاه.

2. تتمتع الجهات الحكومية بالسلطة التقديرية لتسعير البيانات أو منتجات البيانات بأقل من استرداد التكلفة المقدرة.
3. إذا رأت جهة حكومية أنه يجب إضافة هامش ربح أعلى من استرداد التكلفة، فيجب أخذ الموافقة من المكتب بعد تزويده بالمبررات الكافية.
4. تحدد الجهات الحكومية سعر البيانات أو منتجات البيانات بشكل موحد بين المستفيدين من البيانات، كما يجب رفع أي استثناء إلى المكتب للموافقة عليه.

الأدوار والمسؤوليات

أولاً: تقوم الوحدة الإدارية/ فريق العمل المسؤول عن تطوير الأعمال وتحقيق الإيرادات بالجهة بتطوير متجر إلكتروني أو دليل يتضمن البيانات ومنتجات البيانات التي ترغب في تزويدها أو تقديمها وتحديد نموذج التسعير التفصيلي لكل خدمة أو منتج وفقاً للمسارات الموضحة أعلاه وإرسالها إلى مكتب الجهة.

ثانياً: يقوم مكتب الجهة بمراجعة الخدمات والمنتجات المعروضة في المتجر أو الدليل للتأكد من أن البيانات المراد تزويدها أو المستخدمة لتطوير منتجات البيانات مصنفة على مستوى مقيّد أو عام، والتحقق من استيفاء متطلبات الخصوصية وفقاً لسياسة حماية البيانات الشخصية، وأن نماذج التسعير التفصيلية تم تحديدها وفقاً للمسارات الموضحة في هذه السياسة.

ثالثاً: تقوم الجهة التي ترغب في الحصول على البيانات أو منتجات البيانات بتقديم الطلب على مكتب الجهة مثل مشاركة وفقاً للخطوات الموضحة في سياسة مشاركة البيانات، على أن يقوم مكتب الجهة بالتحقق من الالتزام بأحكام سياسة مشاركة البيانات وبالقواعد العامة المنصوص عليها في سياسة تحقيق الإيرادات.

رابعاً: يقوم مكتب الجهة بتوثيق جميع طلبات مشاركة البيانات والقرارات المتعلقة بها في سجلات خاصة.

5.1.6. أحكام عامة

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

ثانياً: تلتزم الجهات التنظيمية بتحديد أدوات المتابعة لتحصيل الإيرادات من البيانات –بما لا يتعارض مع نظام إيرادات الدولة– ومراقبة الامتثال لهذه السياسة وتزويد المكتب بتقارير الامتثال بشكل دورياً.

ثالثاً: يجب على كل جهة حكومية تحصيل جميع إيراداتها من البيانات الحكومية –سواء كانت بيانات غير معالجة أو منتجات بيانات– وتسجيلها في سجل مفصّل بما لا يتعارض مع نظام إيرادات الدولة ولائحته التنفيذية.

رابعاً: تلتزم كل جهة حكومة بالحصول على موافقة رسمية وموثّقة على أي إيراد يتعلق بالبيانات غير المعالجة أو منتجات البيانات من رئيس الجهة أو من يفوضه.

خامساً: بما لا يخل بأحكام نظام إيرادات الدولة، تلتزم الجهات الحكومية بتزويد المكتب ووزارة المالية بتقارير سنوية عن إيراداتها من البيانات الحكومية (المعالجة وغير المعالجة)، في شهر (ديسمبر) من كل عام بدءاً من أول ديسمبر لإصدار هذه السياسة.

سادساً: يمارس المكتب أدوار ومهام الجهات التنظيمية على الجهات غير الخاضعة لجهات تنظيمية.

سابعاً: يحق للجهات التنظيمية –بعد موافقة المكتب– اقتراح إضافة بعض نماذج تحقيق الإيرادات ووضع معايير إضافية لتطوير نماذج التسعير وفقاً لطبيعة أنشطة الجهات التابعة لها أو المرتبطة بها.

ثامناً: تقوم الجهات التنظيمية –بعد التنسيق مع المكتب– بإعداد الآليات والإجراءات التي تنظم عملية معالجة الشكاوى والنزاعات المتعلقة بتحقيق الإيرادات وفقاً لإطار زمني محدد وحسب التسلسل التنظيمي.

تاسعاً: يقوم المكتب –بالتنسيق مع الجهات ذات العلاقة– بمراجعة نماذج تحقيق الإيرادات ونماذج التسعير بشكل دورياً وبما يتوافق مع متطلبات السوق وبما يضمن تحقيق المنافسة العادلة ومنع الممارسات الاحتكارية في قطاع البيانات.

القواعد العامة لحوكمة البيانات عند تطوير أو استخدام أنظمة الذكاء الاصطناعي

5.2. القواعد العامة لحوكمة البيانات عند تطوير أو استخدام أنظمة الذكاء الاصطناعي

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

5.2.1. النطاق

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

5.2.2. المبادئ الأساسية لتطوير واستخدام أنظمة الذكاء الاصطناعي

المبدأ الأول: العدالة

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

المبدأ الثاني: الشفافية

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

المبدأ الثالث: المساءلة/ المسؤولية

أن تكون أنظمة الذكاء الاصطناعي والنماذج التنبؤية خاضعة للمساءلة وذلك بإجراء تقييم الآثار السلبية والمخاطر المحتملة عند تطويرها أو استخدامها بشكل غير مسؤول مع توفير إمكانية الاعتراض على القرارات المهمة التي تتعلق بمصالح الأفراد.

المبدأ الرابع: الشمولية

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

المبدأ الخامس: الإنسانية

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

المبدأ السادس: الأمان

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

المبدأ السابع: جودة البيانات

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

5.2.3. حقوق أصحاب البيانات

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

1. تبعات نظامية تتمثل في قيام الجهات المختصة باتخاذ الإجراءات اللازمة في حقه ومن ذلك استدعائه وسماع أقواله وطلب التحقق من معلوماته وغيرها من الإجراءات.
2. أضرار مادية أو معنوية تتمثل في زوال منفعة أو إساءة سمعة ونحوها من الأضرار الأخرى.

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

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

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

5.2.4. القواعد العامة لاستخدام تطبيقات الذكاء الاصطناعي وتطويرها

أولاً: الالتزامات الخاصة بمطوري أنظمة الذكاء الاصطناعي

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

2. اتخاذ الإجراءات اللازمة والخطوات الكافية لضمان تنوع عينة البيانات وتمثيلها لجميع شرائح المجتمع أو الفئات المستهدفة بشكل عادل دون أي تمييز.
3. إجراء تقييم الانحياز وتوثيق النتائج واعتمادها من المسؤول الأول في الجهة أو من يفوضه قبل البدء بتطوير النماذج التنبؤية المبنية على البيانات وخوارزميات الذكاء الاصطناعي.
4. عدم استخدام البيانات الشخصية الحسّاسة بصفتها عينة بيانات أثناء مرحلة تدريب أنظمة الذكاء الاصطناعي وتطويرها أو النماذج التنبؤية.
5. عدم استخدام البيانات الشخصية التي تؤدي إلى معرفة الفرد على وجه التحديد بدون أساس نظامي سواء موافقة صاحب البيانات أو غيرها من الأسس النظامية المنصوص عليها في سياسة حماية البيانات الشخصية على أن يتم إيضاح الأغراض الرئيسة لجمع هذه البيانات وتحليلها.
6. إجراء تقييم أثر الخصوصية لتقييم الآثار النفسية والاجتماعية عند استخدام البيانات الشخصية بصفتها عينة بيانات لضمان المحافظة على خصوصية أصحابها وحماية حقوقهم.
7. الالتزام بمبدأ الشفافية عند بناء النماذج التنبؤية المبنية على البيانات وخوارزميات الذكاء الاصطناعي وذلك عن طريق شرح آلية عمل الخوارزميات المستخدمة بطريقة قابلة للفهم والتفسير تساعد على معرفة أسباب وصول هذه النماذج إلى نتائج معينة بما لا يتعارض مع أنظمة الملكية الفكرية أو الأنظمة الأخرى ذات الصلة.
8. اتخاذ الإجراءات اللازمة والخطوات الكافية للتحقق من صحة تفسير النتائج بشكل دقيق وغير متعارض وذلك لتفادي القياسات المضللة.
9. إثبات عدالة القرارات المهمة وذلك بتوفير إمكانية التحقق من العوامل الرئيسة التي تؤدي إلى اتخاذ أي قرار يمكن أن يؤثر على المصالح الحيوية للأفراد.
10. توفير آلية للتدخل اليدوي تتيح للأفراد إمكانية تتبع مراحل اتخاذ القرارات المهمة المتعلقة بمصالحهم الحيوية والاعتراض عليها.
11. إعداد آلية تتضمن مجموعة من المعايير اللازمة لتقييم مدى الاعتمادية على أنظمة الذكاء الاصطناعي في التنبؤ واتخاذ القرارات المستقبلية.
12. تبني منهجية شاملة لاختبار جودة الأنظمة والنماذج التنبؤية المبنية على البيانات وخوارزميات الذكاء الاصطناعي وفقاً للممارسات القياسية.
13. اتخاذ الإجراءات اللازمة والخطوات الكافية لضمان جودة عينة البيانات ودقتها وصحتها وعلاقتها بالغرض من بناء النماذج التنبؤية وأنظمة الذكاء الاصطناعي.

ثانياً: الالتزامات الخاصة بمستخدمي أنظمة الذكاء الاصطناعي

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

2. الالتزام بسياسات حوكمة البيانات الوطنية الصادرة من المكتب والمعتمدة من مجلس إدارة الهيئة السعودية للبيانات والذكاء الاصطناعي.
3. أخذ موافقة المكتب –بعد التنسيق مع الجهة التنظيمية– قبل تحليل البيانات المصنفة على إحدى درجات السرية وفقاً لسياسة تصنيف البيانات.
4. أن يقتصر تحليل البيانات على مستويات التصنيف (مقيّد، عام) على أن يتم تحديد ما إذا كان هناك حاجة لمعالجة البيانات قبل تحليلها، ومنها على سبيل المثال لا الحصر الحجب وإخفاء الهوية والتجميع.
5. اتخاذ الإجراءات اللازمة والخطوات الكافية لضمان جودة البيانات المراد تحليلها ودقتها وصحتها وموثوقية مصادرها ومناسبة طرق جمعها وخلوها من أساليب الخداع أو التضليل.
6. توفير قنوات مناسبة تمكّن الأفراد من الحصول على التفسيرات المتعلقة بالنتائج والقرارات المهمة التي تمس مصالحهم الحيوية وتمكينهم من الاعتراض على هذه القرارات أو طلب إثبات عدالتها.
7. إعداد الأدلة الاسترشادية المتعلقة بإيضاح آلية عمل النماذج التنبؤية أو خوارزميات الذكاء الاصطناعي المستخدمة والبيانات المراد تحليلها والفئات المستهدفة والعوامل التي تؤثر في النتائج والقرارات المهمة.
8. إعداد سجل تفصيلي لجميع أنشطة تحليل البيانات إذ يتضمن تاريخ جميع العمليات والإجراءات التي تمت على كل مجموعة من مجموعات البيانات.
9. اتخاذ الخطوات اللازمة لضمان عدم سيطرة الآلة وقيام أنظمة الذكاء الاصطناعي باتخاذ القرارات المهمة بالنيابة عن الأشخاص المعنيين أو التأثير على قراراتهم دون الحصول على موافقتهم المسبقة.
10. إعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات وفقاً للأغراض المحددة والأنظمة والتشريعات ذات العلاقة.
11. التخلص من البيانات وإتلافها بطريقة آمنة –بما في ذلك البيانات المؤرشفة والنسخ الاحتياطية– وفقاً لسياسة التخلص من البيانات المعتمدة من قبل الجهة ووفقاً للأنظمة والسياسات ذات العلاقة.
12. إعداد دليل إجرائي يوضح الخطوات اللازمة لتقييم المخاطر والأثار المحتملة المترتبة على تحليل البيانات باستخدام النماذج التنبؤية وخوارزميات الذكاء الاصطناعي وذلك لقياس مدى تحقيق الأهداف العامة بأقل أثر ممكن على خصوصية الأفراد.
13. إعداد دليل إجرائي يوضح الخطوات اللازمة لتقييم أثر الانحياز في النتائج لضمان تنوع مجموعة البيانات المراد تحليلها وتمثيلها لجميع الفئات المستخدمة بشكل عادل دون أي تمييز.
14. أن يتم تقييد استخدام نتائج تحليل البيانات على الغرض الذي استخدمت من أجله وأن يكون الغرض متوافق مع الأنظمة واللوائح والسياسات ذات العلاقة.

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

ثالثاً: الالتزامات المتعلقة بتقنيات التعرّف على الوجه

1. إجراء تقييم الآثار السلبية والمخاطر المحتملة عند تحديد الأغراض المتعلقة باستخدام تقنيات التعرف على الوجه.
2. يحظر استخدام تقنيات التعرف على الوجه لأغراض المراقبة المستمرة –تتبع تحركات شخص أو مجموعة من الأشخاص بشكل دائم في الأماكن العامة وعلى نطاق واسع– سواء كان ذلك لحظياً أو عن طريق الرجوع إلى السجلات التاريخية، ويستثنى من ذلك استخدامها لأغراض محددة وفقاً للأنظمة واللوائح والسياسات المعمول بها في المملكة.
3. تقييد استخدام تقنيات التعرف على الوجه على الحد الأدنى من البيانات لتحقيق الأغراض المحددة بناءً على أسس نظامية مع تحديد فترة الاحتفاظ بها والأطراف المراد مشاركة هذه البيانات معها.
4. اتخاذ الإجراءات اللازمة والخطوات الكافية لتقييم الجودة والدقة والأداء النسبي للأنظمة المبنية على تقنيات التعرف على الوجه قبل استخدامها وذلك وفقاً للممارسات القياسية.
5. يحظر استخدام الكاميرات المثبتة على الجسم أو التي يمكن ارتداؤها (Body Worn Cameras) والمدمجة بتقنيات التعرف على الوجه لأغراض المراقبة المستمرة.
6. الالتزام بمبدأ الشفافية وإشعار الأفراد بطريقة ملائمة في حال وجود كاميرات مدمجة بتقنيات التعرف على الوجه في الأماكن المسموح بها استخدام هذه التقنيات (مثل المطارات ومقرات بعض الجهات الحكومية).
7. إعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات وفقاً للأغراض المحددة والأنظمة والتشريعات ذات العلاقة.

5.2.5. أحكام عامة

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

ثانياً: تلتزم الجهة التنظيمية بمراقبة وتوثيق الامتثال لهذه القواعد العامة بشكل دورياً.

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

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

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

سادساً: يمارس المكتب أدوار ومهام الجهات التنظيمية على الجهة غير الخاضعة لجهات تنظيمية.

سابعاً: يحق للجهة التنظيمية وضع قواعد إضافية لاستخدام بعض التقنيات والخوارزميات الخاصة بالذكاء الاصطناعي بعد التنسيق مع المكتب.

ثامناً: تلتزم الجهة التنظيمية –بعد التنسيق مع المكتب– بإعداد الآليات والإجراءات التي تنظم عملية معالجة الشكاوى والاعتراضات وفقاً لإطار زمني محدد وحسب نموذج الحوكمة الصادر من المكتب.