وزارة التعليم
Ministry of Education

سياسات حوكمة البيانات

وكالة التخطيط والتطوير

مكتب إدارة البيانات

الفهرس

المعلومات العامة:

مالك الوثيقة	مكتب إدارة البيانات	رقم الوثيقة المرجعي	٤٢٠٠٠٣٤٤٣٤/س
دوريّة المراجعة	سنوي أو في حال وجود تغيير أيهما أقرب	موافقة واعتماد	وزير التّعليم
رقم النّسخة	الإصدار الثاني	تاريخ الإعتماد	١٤٤٤/١/١٠هـ

المراجعات:

الإسم	الوظيفة	ملخص التغييرات	رقم النّسخة	التاريخ
		إعداد		
		مراجعة		
		مراجعة		

الموافقات والإعتماد:

الإسم	الوظيفة	موافقة واعتماد	التاريخ	التوقيع
		☐ موافق ☐ غير موافق		
		☐ موافق ☐ غير موافق		
		☐ موافق ☐ غير موافق		
		☐ موافق ☐ غير موافق		

١ التّعريفات

يُقصد بالكلمات والمصطلحات الواردة أدناه - أينما وردت في هذه الوثيقة - المعاني الموضّحة أمام كلّ منها، ما لم يقتضِ سياق النّص خلاف ذلك:

الوزارة: وزارة التّعليم.

المكتب: مكتب إدارة البيانات في الوزارة.

البيانات: مجموعة من الحقّائق في صورتها الأوّليّة أو في صورة غير منظّمة مثل الأرقام أو الحروف أو الصّور الثابتة أو الفيديو أو التّسجيلات الصوتيّة أو الرّموز التعبيريّة.

الوصول إلى البيانات: القدرة على الوصول المنطقيّ والماديّ إلى البيانات والموارد التّقنية للوزارة لغرض استخدامها.

مستوى الوصول إلى البيانات: مستوى يعتمد على الأذونات والصّلاحيات التي تقيّد الوصول إلى البيانات والموارد التّقنيّة على الأشخاص المصرّح لهم وفقاً لما هو مطلوب لإنجاز المهام والمسؤوليّات المناطة بهم.

التّحقّق: التّأكد من هويّة أي مستخدم أو عمليّة أو جهاز بصفته متطلّباً أساسيّاً للسّماح بالوصول إلى الموارد التّقنيّة.

التّصريح: تعريف حقوق وصلاحيات الوصول إلى البيانات والموارد التّقنيّة لأي مستخدم أو برنامج أو عمليّة، والتّحكّم بمستويات الوصول إليها.

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

سرّية البيانات: الحفاظ على القيود المصرّح بها للوصول إلى البيانات أو الإفصاح عنها.

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

البيانات المحميّة: البيانات المصنّفة على أنّها (سرّي للغاية، سرّي، مقيّد).

المعلومات العامّة: البيانات بعد المعالجة - غير المحميّة - التي تتلقّاها أو تنتجها أو تتعامل معها الوزارة مهما كان مصدرها، أو شكلها أو طبيعتها.

البيانات المفتوحة: مجموعة محدّدة من المعلومات العامّة - مقروءة آلياً - تكون متاحة للعموم مجاناً ودون قيود ويمكن لأي فرد أو جهة عامّة أو خاصّة استخدامها أو مشاركتها.

البيانات الحسّاسة: البيانات التي يؤدّي فقدانها أو إساءة استخدامها أو الوصول غير المصرّح به إليها أو تعديلها إلى ضرر جسيم أو تأثير سلبي على المصالح الوطنيّة أو أنشطة الجهات الحكوميّة أو خصوصيّة الأفراد وحماية حقوقهم.

مستويات تصنيف البيانات: مستويات التّصنيف التّالية: (سرّي للغاية) ،(سرّي)، (مقيّد)، (عامّ).

الفرد: الشّخص المتقدّم بطلب الاطّلاع أو الحصول على المعلومات العامّة.

البيانات الشّخصيّة: كل بيان - مهما كان مصدره أو شكله - من شأنه أن يؤدّي إلى معرفة الفرد على وجه التّحديد، أو يجعل التّعرف عليه ممكنًا بصفة مباشرة أو غير مباشرة عند دمجه مع بيانات أخرى، ويشمل ذلك -على سبيل المثال لا الحصر- الاسم، ورقم الهويّة الشّخصيّة، والعناوين، وأرقام التواصل، وأرقام الرُّخص والسّجلات والممتلكات الشّخصيّة، وأرقام الحسابات البنكيّة والبطاقات الائتمانيّة، وصور الفرد الثّابتة أو المتحرّكة، وغير ذلك من البيانات ذات الطابع الشّخصي.

صاحب البيانات الشّخصيّة: الشّخص الطّبيعي الذي تتعلّق به البيانات الشّخصيّة أو من يمثّله أو من له الولاية الشرعيّة عليه.

معالجة البيانات الشّخصيّة: جميع العمليّات التي تُجرى على البيانات الشّخصيّة بأي وسيلة كانت يدويّة أو آليّة، وتشمل هذه العمليّات - 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 ترتبط تنظيميا بالوزارة: تحدد الغرض من معالجة البيانات الشخصية وكيفية ذلك: سواء تمت معالجة البيانات بواسطتها او عن طريق جهة المعالجة.

جهة المعالجة: أي جهة حكوميّة أو جهة اعتباريّة عامّة مستقلّة في المملكة، وأيّ شخصيّة ذات صفة طبيعيّة أو اعتباريّة خاصّة؛ تعالج البيانات الشّخصيّة لمصلحة جهة التّحكّم ونيابةً عنها.

الإفصاح عن البيانات الشّخصيّة: تمكين أي شخص - عدا جهة التّحكّم - من الحصول على البيانات الشّخصيّة أو استعمالها أو الاطّلاع عليها بأي وسيلة ولأي غرض.

تسريب البيانات الشّخصيّة: الإفصاح عن البيانات الشّخصيّة، أوالحصول عليها، أو تمكين الوصول إليها دون تصريح أو سند نظامي، سواء بقصد أو بغير قصد.

الموافقة الضّمنيّة: هي موافقة لا يتمّ منحها صراحةً من قِبل صاحب البيانات، ولكنّها تُمنح ضمنياً عن طريق أفعال الشخص ووقائع وظروف الموقف، كتوقيع العقود أو الموافقة على الشّروط والأحكام.

الأطراف الخارجيّة: أي جهة حكوميّة أو جهة اعتباريّة عامّة مستقلّة في المملكة، وأي شخصيّة ذات صفة طبيعيّة أو اعتباريّة خاصّة بخلاف صاحب البيانات أو جهة التّحكّم أو جهة المعالجة والأشخاص المصرّح لهم، تُعنى بمعالجة البيانات الشّخصيّة.

ممثّل بيانات أعمال: هو الشّخص المسؤول عن البيانات التي يتمّ جمعها والإحتفاظ بها من قبل الجهة العامّة التي يعمل بها، وغالباً ما يكون في مستوى إداري عالٍ، ويمكن أن يوجد في الجهة العامّة أكثر من ممثّل بيانات أعمال.

مستخدم البيانات: أي شخص يمنح صلاحيّة الوصول إلى البيانات بغرض الاطّلاع عليها أو استخدامها أو تحديثها وفقاً للمهام المصرّح بها من قبل ممثّل بيانات الأعمال.

البيانات الوصفيّة: هي المعلومات التي تصف البيانات وخصائصها، ومن بينها بيانات الأعمال والبيانات التّقنيّة والتّشغيليّة.

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

المنصّة الوطنيّة للبيانات المفتوحة: هي منصّة وطنيّة موحّدة على مستوى المملكة تُعنى بإدارة وحفظ ونشر مجموعات البيانات المفتوحة.

ترخيص البيانات المفتوحة: رخصة تنظّم استخدام البيانات المفتوحة.

الصيغة المفتوحة: أي صيغة مقبولة على نطاق واسع وغير مسجّلة الملكيّة وغير خاصّة بمنصّة معيّنة ويمكن قراءتها آلياً وتمكّن المعالجة الآلية لتلك البيانات، كما تيسّر قدرات التحليل والبحث.

مقدّم الطّلب: أي جهة من القطاعين العامّ أو الخاصّ، أوالقطاع الثّالث، أو أي فرد يتقدّم بطلب لمشاركة البيانات.

طلب مشاركة البيانات: النّموذج المخصّص لطلب مشاركة البيانات والذي يتضمّن معلومات عن مقدّم الطّلب والبيانات المطلوبة، والغرض الذي من أجله تمّ طلب مشاركة البيانات.

اتّفاقيّة مشاركة البيانات: اتّفاقيّة رسميّة موقّعة بين طرفين - جهة حكوميّة مع أي طرف آخر- للموافقة على مشاركة البيانات وفقاً لشروط وأحكام محدّدة ومتوافقة مع مبادئ مشاركة البيانات.

آليّة مشاركة البيانات: الطّريقة التي يتمّ عن طريقها مشاركة البيانات - تشمل كلّاً من وسيلة نقل البيانات، والأطراف المشاركة في مشاركة البيانات، ونموذج المشاركة: المشاركة المباشرة، المشاركة عن طريق مزوّد خدمة، المشاركة عن طريق أطراف متعدّدة.

الضّوابط الأمنيّة: الأجهزة والإجراءات والسّياسات والضّمانات الماديّة المستخدمة لضمان سلامة البيانات وحمايتها ووسائل معالجتها والوصول إليها.

الطّفل: كل شخص لم يتجاوز الثّامنة عشرة من عمره.

الأهليّة: صلاحيّة الشّخص لصدور التّصرّفات منه على وجه يعتدّ به شرعاً ونظاماً.

ناقص الأهليّة: من لديه أهليّة غير مكتملة كالصّغير المميز- وهو من أكمل السّابعة ولم يتمّ الثّامنة عشرة من العمر- وذي الغفلة، والسّفيه، ومن به عاهة عقليّة، ونحوهم. ومن في حكمه: فاقد أو ناقص الأهليّة.

الوليّ: أحد الوالدين أو من تكون له الولاية على شؤون الطّفل حسب أحكام الشّريعة أو الأنظمة ذات العلاقة.

الولاية: سلطة يثبتها الشّرع للوليّ تخوّله صلاحيّة التّصرف وإدارة شؤون الطّفل نيابة عنه فيما يتعلّق ببدنه ونفسه وماله وبما يحقّق مصالحه، ومنها اتخاذ القرارات الخاصّة بمعالجة بياناته الشّخصيّة.

البيانات الشّخصيّة الحسّاسة: كل بيان شخصيّ يتضمّن الإشارة إلى أصل الطّفل ومن في حكمه العرقيّ أو القبليّ، أو معتقده الدّينيّ أو الفكريّ أو السياسيّ، أو يدلّ على عضويّته في جمعيات أو مؤسّسات أهليّة. وكذلك البيانات الجنائيّة والأمنيّة، أو بيانات السّمات الحيويّة التي تحدّد الهويّة، أو البيانات الوراثيّة، أو البيانات الائتمانيّة، أو البيانات الصحيّة، وبيانات تحديد الموقع، والبيانات التي تدلّ على أنّ الفرد مجهول الأبوين أو أحدهما.

إشعار الخصوصيّة: هو بيان خارجي موجّه للأفراد يوضّح محتوى البيانات الشّخصيّة ووسائل جمعها والغرض من معالجتها وكيفيّة استخدامها والجهات التي سيتمّ مشاركة هذه البيانات معها وفترة الإحتفاظ بها وآلية التّخلّص منها.

سياسة الخصوصيّة: هي وثيقة داخليّة موجّهة إلى العاملين في الوزارة توضّح حقوق أصحاب البيانات والالتزامات التي يجب الإمتثال لها للمحافظة على خصوصيّة أصحاب البيانات وحماية حقوقهم.

الإفصاح عن البيانات: تمكين أي شخص - عدا جهة التّحكّم - من الحصول على البيانات الشّخصيّة أو استعمالها أو الاطّلاع عليها بأي وسيلة ولأي غرض.

نقل البيانات الشّخصيّة: إرسال البيانات الشّخصيّة إلى جهة خارج الحدود الجغرافيّة للمملكة - بأيّ وسيلة كانت - بهدف معالجتها سواء كانت بطريقة مباشرة أو غير مباشرة وفقاً لأغراض محدّدة مبنية على أسس نظاميّة، بما في ذلك النّقل لأغراض أمنيّة أو لحماية الصّحة أو السّلامة العامّة أو تنفيذاً لاتّفاقيّة تكون المملكة طرفاً فيها.

الموافقة الصّريحة: موافقة مكتوبة أو الكترونيّة تكون صريحة ومحدّدة وصادرة بإرادة حرّة ومطلقة من صاحب البيانات تدلّ على قبوله لمعالجة بياناته الشّخصيّة.

التّسويق المباشر: أي اتصال، بأي وسيلة كانت، يتمّ عن طريقه توجيه مادة تسويقيّة أو دعائيّة إلى شخص بعينه.

النّقل المباشر: نقل البيانات الشّخصيّة من الجهة المرسلة إلى الجهة المستقبلة دون مرور البيانات بأيّ جهة أخرى.

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

النّقل العرضي: نقل البيانات الشّخصيّة بشكل غير متكرر أو منتظم - عادةً ما يكون لمرة واحدة - لعدد محدود من الأشخاص، ومنها على سبيل المثال، نقل البيانات لغرض الإستفادة من خدمة في دولة أخرى لمصلحة صاحب البيانات.

قائمة الإعتماد: قائمة معتمدّة من مكتب إدارة البيانات الوطنيّة تتضمّن أسماء الدّول التي تتمتّع بمستوى كافٍ من الحماية لحقوق أصحاب البيانات فيما يتعلّق بمعالجة بياناتهم الشّخصيّة.

البيانات غير المعالجة: هي البيانات التي لم تخضع لعمليّات متقدّمة من المعاجلة ويتمّ تبادلها في صيغتها الأوّليّة كالبيانات الأساسيّة للمواطن التي يتمّ عرضها في بطاقة الهويّة الوطنيّة، باستثناء المعالجة التي تفرضها الأنظمة واللّوائح والسّياسات لغرض مشاركة البيانات، ومنها على سبيل المثال لا الحصر، المعالجة المسبقة قبل مشاركة البيانات الشّخصيّة كالتّعتيم (Data Masking) أو المزج (Data Scrambling) أو التّعمية (Data Anonymization).

منتجات البيانات: الخدمات أو التّطبيقات 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: الرّؤى والتّحليلات التنبؤيّة أو الوصفيّة، ولوحات المعلومات التّفاعليّة (المنصّات) وغيرها.

البيانات الحكوميّة: هي البيانات التي تنتجها الجهات الحكوميّة.

الخدمات الحكوميّة: الخدمات الأساسيّة التي تقدّمها الجهات الحكوميّة، والتي يمكن تقديمها عن طريق طرف ثالث نيابةً عن الجهة الحكوميّة.

مزوّد البيانات: أي فرد أو جهة حكوميّة أو جهة خاصّة تقوم بتزويد البيانات أو تقديم منتجات البيانات بمقابل مالي بشكل مباشر أو غير مباشر.

المستفيد من البيانات: أي فرد أو جهة حكوميّة أو جهة خاصّة تقوم بطلب البيانات أو الإستفادة من منتجات البيانات بمقابل مالي.

التّسويق: نشاط تبادل أو تداول أو تزويد البيانات الخام أو البيانات المعالجة مقابل مبلغ نقدي أو قيمة عينيّة أخرى.

الجهة الحكوميّة: أي جهة حكوميّة أو جهة عامّة مستقلّة بالمملكة، أو أيّ من الجهات التّابعة لها، ويعدّ في حكم الجهة الحكوميّة أي شركة تقوم بإدارة المرافق العامّة أو البنى التّحتيّة الوطنيّة أو تشغيلها أو صيانتها، أو تقوم بمباشرة خدمة عامّة فيما يخصّ إدارة تلك المرافق أو البنى التّحتيّة.

الجهة الخاصّة: أي شخصيّة ذات صفة اعتباريّة خاصّة مرخّصة بالعمل في المملكة - سواء أكانت محليّة أو أجنبيّة - ويعدّ في حكم الجهةالخاصّة الفرد المواطن أو المقيم بشكل رسمي في المملكة الذي يقوم بتزويد البيانات أو تقديم منتجات البيانات.

الجهة غير الربحيّة: أي جهة غير حكوميّة مرخّصة بالعمل في المملكة وتقدّم خدماتها ومنتجاتها بشكل غير ربحي.

المطوّر: أي شخصيّة ذات صفة طبيعيّة أو اعتباريّة تقوم بتطوير أنظمة الذّكاء الاصطناعي عن طريق بناء نماذج تنبؤيّة باستخدام البيانات والخوارزميّات لتحقيق أهداف محدّدة.

المستخدم: أي شخصيّة ذات صفة طبيعيّة أو اعتباريّة تقوم بتطبيق أو استخدام أنظمة الذّكاء الاصطناعي لتحقيق أهداف محدّدة.

صاحب البيانات: الفرد الذي تتعلّق به البيانات الشّخصيّة أو من يمثّله أو من له الولاية الشرعيّة عليه.
عينة البيانات: البيانات التي يتمّ استخدامها في بناء وتدريب واختبار النّماذج التنبؤيّة وخوارزميات الذّكاء الاصطناعي للوصول إلى نتائج معيّنة.
تقنيات الذكاء الاصطناعي: هي مجموعة من النماذج التنبؤيّة والخوارزميات المتقدّمة التي يمكن استخدامها لتحليل البيانات واستشراف المستقبل أو تسهيل عمليّة اتخاذ قرارات على أحداث متوقّعة بالمستقبل.

٢ الأهداف

تهدف هذه السّياسات إلى الإستفادة من الممارسات والمعايير العالمية الخاصّة بحوكمة البيانات وبما يتوافق مع سياسات وضوابط مكتب إدارة البيانات الوطنية وذلك لتحقيق الأهداف التّالية:

١. المشاركة في دعم وتعزيز جهود المملكة في تحقيق الرؤية والاستراتيجيّات الوطنيّة.
٢. نشر ثقافة مشاركة البيانات والتّعاون لتعزيز وتطوير البيانات والمعلومات والأصول المعرفيّة الخاصّة بوزارة التّعليم.
٣. تنظيم عمليّة نشر وتبادل واستخدام/ إعادة استخدام البيانات المحميّة والمعلومات العامّة الخاصّة بوزارة التّعليم.
٤. تحقيق دور فعّال في التّكامل بين الجهات الحكوميّة.
٥. المحافظة على خصوصيّة البيانات الشّخصيّة، وسرّية البيانات الحسّاسة.
٦. المحافظة على حقوق الأفراد عند التّعامل مع البيانات الشّخصيّة والمعلومات العامّة لدى وزارة التّعليم.
٧. تعزيز مفهوم وممارسات البيانات المفتوحة لتحسين الشّفافيّة وتشجيع البحث والابتكار ودفع النّمو الاقتصادي.
٨. تعزيز الشّفافيّة وإرساء قواعد الحوكمة عن طريق توزيع الأدوار والمسؤوليات.
٩. المشاركة في المحافظة على السيّادة الوطنيّة الرقميّة للبيانات الشّخصيّة.
١٠. رفع مستوى الثّقة في الخدمات المعتمدة على البيانات.
١١. رفع مستوى الخدمات والتّعاملات الالكترونيّة بما يحقّق التّكامليّة.
١٢. المشاركة في دعم البحوث العلميّة عن طريق تشجيع الباحثين للإستفادة من المعلومات العامّة والنّهوض بالدّور التنموي والرّقابي للمجتمع والمؤسّسات.
١٣. توفير الفرص المتكافئة لطالبي المعلومات العامّة ممّا يسهم في تعزيز المواطنة المتساوية والشراكة في الوعي بقضايا الوطن العامّة.

٣ حاكميّة سياسات حوكمة البيانات

٣,١ مالك الوثيقة

مكتب إدارة البيانات في وزارة التّعليم.

٣,٢ مراجعة وتعديل وتغيير السّياسات

١. على المكتب مراجعة السّياسات بشكل سنوي على الأقل أو في حال استحداث تغيير أو متطلّبات تستوجب تعديل سياسة أو أكثر أيّهما أقرب.

٢. على المكتب مشاركة تعديلات السّياسات مع الجهات المعنيّة داخل الوزارة للاطّلاع والمراجعة والتّغذية الراجعة لأغراض الموافقة والإعتماد.

٣. على المكتب توثيق تعديلات السّياسات في جدول المراجعات وإصدار نسخة جديدة تشمل التّعديلات.

٣,١ الامتثال للسّياسات

١. تنطبق أحكام هذه السّياسات على جميع البيانات التي تنتجها وزارة التّعليم الدّاخليّة والخارجيّة وإدارات ومكاتب التّعليم والمدارس التي تديرها أو تشرف عليها الوزارة ما لم يذكر أي استثناء في بند "نطاق السّياسة" الخاصّ بكل سياسة.

٢. مكتب إدارة البيانات في وزارة التّعليم المسؤول عن مراقبة الامتثال لبنود هذه السّياسات.

٣. يتمّ مراجعة الالتزام ببنود هذه السّياسات من قبل المكتب، ويتم رفع تقرير بالمخالفات لأحكام هذه السّياسة إلى مكتب وزير التّعليم مع التّوصيات لتصويب المخالفات.

٣,٢ استثناءات على السّياسات

يتم رفع طلب إلى المكتب في حال وجود أسباب تتطلّب مخالفة لسياسة أو أكثر من سياسات حوكمة البيانات مع توضيح المبرّرات بشكل تفصيلي، على أن يتمّ مراجعة الاستثناء كل ثلاث أشهر وتقييمه والنّظر فيما إذا كان هناك حاجة للإستثناء أو الرجوع عنه.

٤ سياسة تصنيف البيانات

٤,١ نطاق السّياسة

تنطبق أحكام هذه السّياسة على جميع البيانات التي تنتجها وزارة التّعليم الدّاخليّة والخارجيّة وإدارات ومكاتب التّعليم والمدارس التي تديرها أو تشرف عليها الوزارة مهما كان مصدرها، أو شكلها أو طبيعتها، ويشمل ذلك السّجلات الورقيّة والاجتماعات والاتصالات عبر وسائل التّواصل والتطبيقات ورسائل البريد الالكتروني والمعلومات المخزّنة على الكمبيوتر أو أشرطة الصّوت أو الفيديو أو الخرائط أو الصّور الفوتوغرافيّة أو المخطوطات أو الوثائق المكتوبة بخط اليد، أو أي شكل آخر من أشكال المعلومات المسجّلة.

٤,٢ المبادئ الرّئيسيّة لتصنيف البيانات

المبدأ الأوّل: الأصل في البيانات الإتاحة

الأصل في البيانات أن تكون متاحة (في المجال التنموي) ما لم تقتضِ طبيعتها أو حساسيّتها مستويات أعلى من التّصنيف والحماية، والسرّيّة للغاية (في المجال السّياسي والأمني) ما لم تقتضِ طبيعتها أو حساسيّتها مستويات أدنى من التّصنيف والحماية.

المبدأ الثّاني: الضّرورة والتّناسب

يتمّ تصنيف البيانات إلى مستويات وفقاً لطبيعتها، ومستوى حساسيّتها، ودرجة أثرها مع الأخذ بالاعتبار الموازنة بين قيمتها ودرجة سرّيتها.

المبدأ الثّالث: التّصنيف في الوقت المناسب

يتمّ تصنيف البيانات عند إنشائها أو حين تلقّيها من جهات أخرى ويكون التّصنيف خلال فترة زمنيّة محدّدة.

المبدأ الرّابع: المستوى الأعلى من الحماية

يتمّ اعتماد المستوى الأعلى من التّصنيف عندما يتضمّن محتوى مجموعة متكاملة من البيانات مستويات تصنيف مختلفة.

المبدأ الخامس: فصل المهام

يتمّ الفصل بين مهام ومسؤوليات العاملين - فيما يتعلّق بتصنيف البيانات أو الوصول إليها أو الإفصاح عنها أو استخدامها أو التّعديل عليها أو إتلافها - بطريقة تحول دون تداخل الاختصاص وتتلافى تشتيت المسؤوليّة.

المبدأ السّادس: الحاجة إلى المعرفة

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

المبدأ السّابع: الحدّ الأدنى من الامتيازات

يتمّ تقييد إدارة صلاحيات العاملين على الحدّ الأدنى من الإمتيازات اللّازمة لأداء المهام والمسؤوليّات المناطة بهم.

٤,٣ مستويات تصنيف البيانات

الجدول(١) أدناه يوضّح المستويات الرّئيسة لتصنيف البيانات بما يتوافق مع مستوى الأثر، كما يوضّح بعض الأمثلة الاسترشاديّة لكل مستوى.

مستوى التّصنيف	درجة الأثر	الوصف	أمثلة استرشادية
سري للغاية	عالي	تُصنّف البيانات على أنّها «بيانات سرّية للغاية»، إذا كان الوصول غير المصرّح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدّي إلى ضرر جسيم واستثنائي لا يمكن تداركه أو إصلاحه على: *المصالح الوطنيّة بما في ذلك الإخلال بالاتّفاقيّات والمعاهدات أو إلحاق الضّرر بسمعة المملكة أو بالعلاقات الدبلوماسيّة والانتماءات السياسيّة أو الكفاءة التشغيليّة للعمليّات الأمنيّة أو العسكريّة أو الإقتصاد الوطنيّ أو البنية التحتيّة الوطنيّة أو الأعمال الحكوميّة. *أداء الجهات العامّة مما يُلحقّ ضررًا بالمصلحة الوطنيّة. *صحة الأفراد وسلامتهم على نطاق واسع وخصوصيّة كبار المسؤولين. *الموارد البيئيّة أو الطبيعيّة.	* خطط وتفصيلات العمليّات العسكريّة أو أي معلومات ذات علاقة بها. * المعلومات المتعلّقة بأعمال وتدابير وتشكيلات الأجهزة الأمنيّة والاستخباراتيّة وتجهيزاتها. * المعلومات المتعلّقة بآليّات ومفاتيح التشفير المستخدمة للبنى التحتيّة الوطنيّة. * معلومات القضايا الإرهابيّة والمخطّطات المهدّدة للأمن. * المعلومات المتعلّقة بالأسلحة والذخائر أو المواقع العسكريّة الاستراتيجيّة أو أي مصدر من مصادر القوّة الدفاعيّة والهجوميّة. * معلومات عن تحرّكات القوات المسلحة، أو القوات العسكريّة الأخرى، أو تحرّكات الشخصيات الهامّة. * معلومات تمس سيادة الدولة.

مستوى التّصنيف	درجة الأثر	الوصف	أمثلة استرشادية
سري	متوسّط	تُصنّف البيانات على أنّها «بيانات سرّية» إذا كان الوصول غير المصرّح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدّي إلى ضرر جسيم على: * المصالح الوطنيّة مثل إلحاق ضرر جزئي بسمعة المملكة والعلاقات الدبلوماسيّة أو الكفاءة التّشغيليّة للعمليّات الأمنيّة أو العسكريّة أو الإقتصاد الوطنيّ أو البنية التّحتيّة الوطنيّة والأعمال الحكوميّة. * يُحدث خسارة ماليّة على المستوى التّنظيمي تؤدّي إلى إفلاس أو عجز الجهات عن أداء مهامها أو خسارة جسيمة للقدرة التنافسيّة أو كليهما معاً. * يتسبّب في حدوث أذى جسيم أو إصابة تؤثّر على حياة مجموعة من الأفراد. * تؤدّي إلى ضرر على المدى الطويل للموارد البيئيّة أو الطبيعيّة. * التّحقيق في القضايا الكبرى المحدّدة نظاماً، كقضايا تمويل الإرهاب.	* معلومات عن مواقع تخزين المواد اللوجستيّة أو المخازن الإقتصاديّة. * معلومات متعلّقة بالمنشآت الحيوية. * مذكرات التّفاهم مع الشّركات الدوليّة لإنشاء مصالح تجاريّة أو اقتصاديّة أو استراتيجيّة بالمملكة. * معلومات متعلّقة بالاتّفاقيات الثنائيّة ومذكّرات التّفاهم الدبلوماسيّة بين المملكة والدول الأخرى.
مقيّد	منخفض	تُصنّف البيانات على أنّها «مقيّدة»، إذا كان الوصول غير المصرّح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدّي إلى: * تأثير سلبي محدود على عمل الجهات العامّة أو الأنشطة الإقتصاديّة في المملكة أو على عمل شخص معيّن. * ضرر محدود على أصول أي جهة وخسارة محدودة على وضعها المالي والتنافسيّ. * ضرر محدود على المدى القريب للموارد البيئيّة أو الطبيعيّة.	* معلومات تضرّ بسمعة أي شخصيّة عامّة. * بيانات مفصّلة للمعاملات الفرديّة. * نتائج الأبحاث والدّراسات العمليّة قبل نشرها. * المعلومات المتعلّقة بالمنتجات تحت التطوير والتي قد تضرّ بعدالة المنافسة. * معلومات متعلّقة بالتعيينات والقرارات الإداريّة الحسّاسة. * معلومات الملفّ الصّحي للأفراد. * معلومات تحديد الهويّة مثل الاسم والعنوان وأرقام الهويّة الوطنيّة وأرقام الهواتف وأرقام الحسابات والتّراخيص وبيانات السّمات الحيويّة. * معلومات رواتب الموظفين. * وثائق مثل خطط المستوى التّخطيطي وبرامج التّسويق قبل الكشف عنها للجمهور وخطط الإبداع التّقني. * عقود موردين وعروض أسعارهم. * طلبات تقديم عروض. * مواصفات منتج جديد قبل طرحه للجمهور. * تفاصيل تصميم وتطبيق أنظمة أمنيّة (جدار الحماية وضوابط الوصول ومخطّطات الشّبكة وغيرها). * سياسيات وإجراءات الجهات الدّاخليّة، رسائل/ مذكّرات داخليّة. * قوائم هواتف داخليّة وقوائم البريد الالكتروني لبعض الجهات.

مستوى التّصنيف	درجة الأثر	الوصف	أمثلة استرشادية
عام	لا يوجد	تُصنّف البيانات على أنّها «بيانات عامّة» عندما لا يترتّب على الوصول غير المصرّح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها أي من الآثار المذكورة أعلاه في حال عدم وجود تأثير على ما يأتي: *المصلحة الوطنيّة. *أنشطة الجهات. *مصالح الأفراد. *الموارد البيئيّة.	* توجّهات استراتيجيّة وطنيّة معلنة. * الإحصاءات الوطنيّة حول عدد السّكان والبيئة والأعمال حسب الصّناعة وغيرها. * التنمية العامّة والدّراسات الإقتصاديّة. * إجراءات الحكومة وسياستها. * معلومات متعلّقة بالخدمات العامّة التي تقدّمها الحكومة للمواطنين. * جهات الاتّصال في المؤسسات. * إعلانات وظائف. * إعلانات عامّة. * تصريحات صحفيّة. * نتائج ماليّة معلنة للجمهور. * عروض منتجات (عامّة). * معلومات العلاقات العامّة. * أي معلومات متاحة علناً على مواقع أي مؤسّسة. * الإعلانات.

يمكن تصنيف البيانات المصنّفة على مستوى مقيّد إلى مستويات فرعيّة بناءً على نطاق الأثر على النّحو التالي:

- مقيّد - مستوى (أ): إذا كان نطاق الأثر على مستوى قطاع كامل أو نشاط اقتصادي عام.
- مقيّد - مستوى (ب): إذا كان نطاق الأثر على مستوى أنشطة عدة جهات أو على مصالح مجموعة من الأفراد.
- مقيّد - مستوى (ج): إذا كان نطاق الأثر على مستوى أنشطة جهة واحدة أو مصالح فرد معيّن.

وفي الجدول أدناه توضيح وتحديد لمستوى التّصنيف الصّحيح الذي يمكّن الوزارة من تقييم درجة الأثر المترتّبة على الوصول غير المصرّح به إلى البيانات أو الإفصاح عنها أو عن محتواها (ولمزيدٍ من المعلومات حول عمليّة تقييم الأثر، يمكن الاطّلاع على "الخطوات اللّازمة لتصنيف البيانات)". يجب على الوزارة أن تقوم بإجراء تقييم الآثار المترتّبة على عمليّة الوصول أوالإفصاح غير المصرّح به، كما تعتبر هذه القائمة غير شمولية.

فئات ودرجات تقييم الأثر وفقاً لمستويات تصنيف البيانات. جدول (٢)

فئة الأثر الرّئيسيّة	**المصلحة الوطنيّة**		
فئة الأثر الفرعيّة	سمعة المملكة		
الاعتبارات	هل ستخضع المعلومات لإهتمام وسائل الإعلام المحليّة أو الدّوليّة؟ هل ستعطي انطباع سلبي؟		
مستوى الاثر:			
سرّي للغاية	**سرّي**	**مقيّد**	**عام**
عالي	متوسّط	منخفض	لا يوجد أثر
تتأثّر السّمعة بشكل كبير.	تتأثّر السّمعة إلى حد ما.	لا تتأثّر السّمعة.	لا يوجد تأثير على المصالح الحيويّة الوطنيّة.

فئة الأثر الرّئيسيّة	**المصلحة الوطنيّة**
فئة الأثر الفرعيّة	-
الاعتبارات	هل تُشكّل المعلومات خطراً على العلاقات مع الدّول الصّديقة؟ هل ستزيد من حدّة التّوتّر الدوليّ؟ هل يمكن أن تؤدّي إلى احتجاجات أو عقوبات من دول أخرى؟

مستوى الاثر:			
سري للغاية	**سري**	**مقيّد**	**عام**
عالي	متوسّط	منخفض	لا يوجد أثر
قطع العلاقات الدبلوماسيّة والانتماءات السياسيّة أو تهديد الاتّفاقيات وشروط المعاهدات أو كليهما.	تتأثّر العلاقات الدبلوماسيّة سلباً على المدى الطّويل.	لن يحدث تأثير على العلاقات الدبلوماسيّة أوسيحدث تأثير بسيط على المدى القصير.	لا يوجد تأثير على المصالح الحيويّة الوطنيّة.

فئة الأثر الرّئيسيّة	**المصلحة الوطنيّة**		
فئة الأثر الفرعيّة	الإقتصاد الوطنيّ		
الاعتبارات	هل يؤدّي الكشف عن المعلومات إلى خسائر اقتصاديّة على المستوى الوطنيّ؟		
مستوى الاثر:			
سري للغاية	**سري**	**مقيّد**	**عام**
عالي	متوسّط	منخفض	لا يوجد أثر
تأثير طويل المدى على الإقتصاد الوطنيّ مع انخفاض لا يُمكن تداركه في النّاتج المحلّي الإجمالي أو أسعار الأسواق الماليّة أو نسبة البطالة أوالقوّة الشّرائيّة أو المؤشّرات الأخرى ذات الصّلة؛ مما ينعكس سلباً على جميع القطاعات في المملكة.	تأثير طويل المدى على الإقتصاد الوطنيّ مع انخفاض يُمكن تداركه في النّاتج المحلّي الإجمالي ونسبة البطالة أو أسعار الأسواق الماليّة أو القوّة الشّرائيّة؛ مما ينعكس سلباً على قطاع واحد أو أكثر.	تأثير بسيط على الإقتصاد الوطنيّ مع انخفاض يُمكن تداركه في وقت قصير في النّاتج المحلّي الإجمالي، ومعدّل العمالة أو أسعار الأسواق الماليّة أو القوّة الشرائيّة؛ مما ينعكس سلباً على قطاع واحد فقط.	-

فئة الأثر الرّئيسيّة	**المصلحة الوطنيّة**		
فئة الأثر الفرعيّة	البنى التّحتيّة الوطنيّة		
الاعتبارات	هل الوصول إلى المعلومات يؤدّي إلى تعطيل البنى التّحتيّة الحيويّة الوطنيّة (مثل الطّاقة، النّقل، الاتصالات)؟ في حال التّعرض لهجمات الكترونية، هل ستظل الخدمات الأساسية في المملكة متاحة؟		
مستوى الاثر:			
سري للغاية	**سري**	**مقيّد**	**عام**
عالي	متوسّط	منخفض	لا يوجد أثر
التّوقّف والتعطّل في آمن عمليّات البنى التّحتيّة الوطنيّة الحيويّة، كما تتأثّر العديد من القطاعات وتتعطّل الحياة الطبيعيّة.	التّوقّف والتعطّل لفترة قصيرة في آمن وعمليّات البنى التّحتيّة الوطنيّة الحيويّة، كما يتأثر قطاع واحد أو أكثر.	يحدث ضرر أو تأثير قصير المدى على آمن وعمليّات البنى التّحتيّة المحليّة / الإقليميّة.	-

فئة الأثر الرّئيسيّة	**المصلحة الوطنيّة**		
فئة الأثر الفرعيّة	مهام الجهات الحكوميّة		
الاعتبارات	هل سيؤدّي الكشف عن المعلومات إلى الحدّ من إمكانيّة الجهات الحكوميّة من تنفيذ عمليّاتها ومهامها اليوميّة؟		
مستوى الاثر:			
سرّي للغاية	**سرّي**	**مقيّد**	**عام**
عالي	متوسّط	منخفض	لا يوجد أثر
عدم قدرة جميع الجهات الحكوميّة على أداء مهامها وعمليّاتها الرّئيسة لفترة طويلة.	عدم قدرة جهة حكوميّة واحدة أو أكثر على أداء واحدة أو أكثر من مهامها الرّئيسة لفترة قصيرة.	عدم قدرة جهة حكوميّة واحدة أو أكثر على أداء واحدة أو أكثر من مهامها غير الرّئيسة لفترة قصيرة.	-

فئة الأثر الرّئيسيّة	**أنشطة الجهات**		
فئة الأثر الفرعيّة	أرباح الجهات الخاصّة		
الاعتبارات	هل سيؤدّي الكشف عن المعلومات إلى خسائر ماليّة أو إفلاس الجهات الخاصّة التي تقوم بإدارة المرافق العامّة؟ على سبيل المثال، احتماليّة الاحتيال، وتحويلات الأموال غير القانونيّة، والمصادرة غير القانونيّة للأصول؟		
مستوى الاثر:			
سرّي للغاية	**سرّي**	**مقيّد**	**عام**
عالي	متوسّط	منخفض	لا يوجد أثر
تأثير سلبي كبير على الجهات الخاصّة إلى الحدّ الذي يتسبّب في الإضرار بالمصالح الحيويّة الوطنيّة.	تكبّد الجهة خسائر ماليّة فادحة مما قد يؤدّي إلى الإفلاس.	ضرر محدود يتمثّل في خسارة ماليّة محدودة للجهة أو لأيٍ من أصولها.	لا يوجد تأثير على أنشطة الجهات.

فئة الأثر الرّئيسيّة	**أنشطة الجهات**		
فئة الأثر الفرعيّة	مهام الجهات الخاصّة		
الاعتبارات	هل سيؤدّي الكشف عن المعلومات إلى حدوث أضرار على الجهات الخاصّة التي تقوم بإدارة المرافق العامّة؟ هل سيؤدّي ذلك إلى فقدان الدّور الريادي التي تتمتّع به الجهة أو خسارة أيٍ من أصولها؟ هل سيؤدّي ذلك إلى إنهاء عقود عددٍ كبيرٍ من الموظفين؟ هل سيؤثر على القدرة التنافسيّة للجهة الخاصّة؟		
مستوى الاثر:			
سرّي للغاية	**سرّي**	**مقيّد**	**عام**
عالي	متوسّط	منخفض	لا يوجد أثر
تأثير سلبي كبير على الجهات الخاصّة إلى الحدّ الذي يتسبّب في الإضرار بالمصالح الحيويّة الوطنيّة.	عدم إمكانية الجهة من القيام بمهامها الرّئيسة، وفقدان القدرة على التنافسيّة إلى حدّ كبير.	عدم إمكانيّة الجهة من أداء إحدى مهامها الرّئيسة، وفقدان القدرة على التنافسيّة بشكل محدود.	لا يوجد تأثير على أنشطة الجهات.

فئة الأثر الرّئيسيّة	الأفراد		
فئة الأثر الفرعيّة	صحّة/ سلامة الأفراد		
الاعتبارات	هل سيؤدّي الكشف عن المعلومات إلى إفشاء أسماء أو مواقع أشخاص وما إلى ذلك؟ (على سبيل المثال، أسماء ومواقع العملاء السرّيين، والأشخاص الخاضعين لأنظمة حماية خاصّة).		
مستوى الاثر:			
سرّي للغاية	**سرّي**	**مقيّد**	**عام**
عالي	متوسّط	منخفض	لا يوجد أثر
خسارة عامّة أو فادحة في الأرواح، وفقدان حياة فرد أو مجموعة من الأفراد.	ضرر جسيم أو إصابة تهدّد حياة الفرد.	إصابة بسيطة دون أي خطر يهدّد حياة أو صحّة الفرد.	لا يوجد تأثير على الأفراد.

فئة الأثر الرّئيسيّة	**الأفراد**		
فئة الأثر الفرعيّة	الخصوصيّة		
الاعتبارات	هل سيؤدّي الكشف عن المعلومات إلى انتهاك خصوصيّة الأفراد؟		
مستوى الاثر:			
سرّي للغاية	**سرّي**	**مقيّد**	**عام**
عالي	متوسّط	منخفض	لا يوجد أثر
الكشف عن البيانات الشّخصيّة لشخصيّة مهمّة فئة أ.	الكشف عن البيانات الشّخصيّة لشخصيّة مهمّة فئة ب.	الكشف عن البيانات الشّخصيّة للفرد.	لا يوجد تأثير على الأفراد.

فئة الأثر الرّئيسيّة	**الأفراد**		
فئة الأثر الفرعيّة	-		
الاعتبارات	سيؤدّي ذلك إلى انتهاك أي حقوق ملكيّة فكريّة؟		
مستوى الاثر			
سرّي للغاية	**سرّي**	**مقيّد**	**عام**
عالي	متوسّط	منخفض	لا يوجد أثر
يؤثّر على المصلحة الوطنيّة.	-	-	-

فئة الأثر الرّئيسيّة	**البيئة**		
فئة الأثر الفرعيّة	الموارد البيئية		
الاعتبارات	هل سيتمّ استخدام هذه المعلومات لتطوير خدمة أو منتج يمكن أن يؤدّي إلى تدمير الموارد البيئيّة أو تعطّل للمملكة؟		
مستوى الاثر			
سرّي للغاية	**سرّي**	**مقيّد**	**عام**
عالي	متوسّط	منخفض	لا يوجد أثر
تأثير كارثي لا يمكن تداركه على البيئة أو الموارد الطبيعيّة.	تأثير طويل المدى على البيئة أو الموارد الطبيعيّة.	تأثير قصير المدى أو محدود على البيئة أو الموارد الطبيعيّة.	لا يوجد تأثير على البيئة.

٤,٤ ضوابط تصنيف البيانات

بناءً على مستويات التّصنيف، يتمّ تحديد وتطبيق الضّوابط الأمنيّة المناسبة لحماية البيانات وذلك لضمان التّعامل معها ومعالجتها ومشاركتها والتّخلّص منها بشكل آمن، وفي حال عدم تصنيف البيانات عند إنشائها أو تلقّيها وفقاً لمعايير التّصنيف، تُعامل هذه البيانات على أنّها "مقيّدة" حتى يتمّ تصنيفها بشكل صحيح.

كما يجب تصنيف البيانات التي لم يتمّ تصنيفها وقت إصدار هذه السّياسة خلال فترة زمنيّة محدّدة بموجب خطّة عمل يعدها المكتب ويتمّ اعتمادها من المسؤول الأوّل بالوزارة (او من يفوضه).

أدناه بعض الأمثلة على الضّوابط التي يمكن استخدامها عند تصنيف البيانات، ويمكن الرّجوع إلى ما يصدر من الهيئة الوطنيّة للأمن السّيبراني من ضوابط وإرشادات تتعلّق بحماية البيانات:

٤,٤,١ علامات الحماية

تُطبّق علامات الحماية النصيّة على الوثائق الورقيّة والالكترونيّة (بما في ذلك رسائل البريد الالكتروني) وفقاً لكل مستوى من مستويات التّصنيف.

٤,٤,٢ الوصول

١. يُمنح الوصول - المنطقي والماديّ - للبيانات بناءً على مبدأ "الحدّ الأدنى من الامتيازات "و"الحاجة إلى المعرفة."
٢. يجب منع حقّ الوصول إلى البيانات بمجرد انتهاء أو إنهاء الخدمة المهنيّة للعاملين بالوزارة.

٤,٤,٣ الاستخدام

تُستخدم البيانات المصنّفة وفقاً لمتطلبات مستويات التّصنيف، على سبيل المثال، يتمّ تقييد استخدام البيانات المصنّفة "سرّية للغاية" على مواقع محدّدة سواء ماديّة - كالمكاتب - أو افتراضيّة باستخدام ترميز الأجهزة أو تطبيقات خاصّة.

٤,٤,٤ التخزين

١. لا تُترك البيانات المصنّفة على أنّها "سرّي للغاية" و"سرّي" و "مقيّد" وكذلك الأجهزة المحمولة التي تعالج أو تخزّن هذه البيانات دون مراقبة.
٢. يجب حماية البيانات المصنّفة على أنّها "سرّي للغاية" و"سرّي" و "مقيّد" غير المراقبة أثناء تخزينها ماديّاً أو الكترونيّاً باستخدام أحد طرق التّشفير المعتمدة من قبل الهيئة الوطنيّة للأمن السّيبراني.

٤,٤,٥ مشاركة البيانات

١. يجب تحديد الوسائل الماديّة والرقميّة المناسبة لتبادل البيانات بشكل آمن بما يضمن تقليل المخاطر المحتملة والامتثال لأنظمة مشاركة البيانات.
٢. يجب الاتّفاق على آلية تبادل البيانات، سواء كانت الوزارة ستستخدم الوسائل المستخدمة حالياً لتبادل البيانات أم لا، على سبيل المثال قناة التّكامل الحكوميّة وشبكة مركز المعلومات الوطنيّ والشّبكة الحكوميّة الآمنة، أو إعداد اتصال مباشر جديد أو وسائط التّخزين القابلة للإزالة أو الشّبكة اللاسلكية، أو الوصول عن بعد، أو الشّبكة الخاصّة الافتراضيّة...الخ.

٤,٤,٦ الإحتفاظ بالبيانات

١. يتمّ إعداد جدول زمني يحدّد فترة الإحتفاظ بجميع البيانات.
٢. يتمّ تحديد فترة الإحتفاظ بناءً على ما تحدّده المتطلّبات التّجاريّة والتّعاقديّة والتّنظيميّة والقانونيّة ذات العلاقة.
٣. تتمّ مراجعة الجدول الزمني لفترة الإحتفاظ بشكل دوري سنوي أو إذا طرأت تغييرات على المتطلّبات ذات العلاقة.

٤,٤,٧ التّخلّص من البيانات

١. يتمّ التّخلّص من جميع البيانات بشكل آمن وفقاً للجدول الزمني للإحتفاظ بالبيانات بعد الحصول على موافقة ممثّل بيانات الأعمال.
٢. يتمّ التّخلّص من البيانات التي تمّ تصنيفها على أنّها "سرّية للغاية" و"سرّي" التي يتمّ التّحكم بها الكترونيّاً باستخدام أحدث طرق التّخلّص من الوسائط الالكترونيّة.
٣. يتمّ التّخلّص من جميع الوثائق الورقيّة باستخدام آلة تمزيق الورق.
٤. يتمّ إعداد سجل مفصّل عن جميع البيانات التي تمّ التّخلّص منها.

٤,٤,٨ الأرشفة

١. تتمّ أرشفة البيانات في مواقع تخزين آمنة وفقاً للطّريقة التي يوصي بها ممثّل بيانات الأعمال.
٢. يتمّ الإحتفاظ بنسخ احتياطيّة من البيانات المؤرشفة.
٣. تتمّ حماية البيانات المؤرشفة التي تمّ تصنيفها على أنها "سرّي للغاية" و"سرّي" باستخدام إحدى طرق التشفير المعتمدة من قبل الإدارة العامّة للأمن السّيبراني بالوزارة .
٤. يتمّ إعداد وتوثيق قائمة مفصّلة تتضمّن المستخدمين المصرّح لهم بالوصول إلى البيانات المؤرشفة.

٤,٤,٩ إلغاء التّصنيف (رفع السرّيّة)

١. يجب إلغاء تصنيف البيانات أو خفض مستوى تصنيفها إلى الحدّ المناسب بعد انتهاء مدّة التّصنيف عندما لا تكون الحماية مطلوبة أو أنّها لم تعد مطلوبة على المستوى الأصلي للتّصنيف.
٢. في حال تمّ تصنيف البيانات بشكل خاطئ، يجب على مستخدم البيانات إشعار ممثّل بيانات الأعمال لتحديد مدى الحاجة إلى إعادة تصنيفها بشكل مناسب.
٣. يجب تحديد عوامل تساعد على إلغاء تصنيف البيانات عند تحديد مستويات التّصنيف لأوّل مرة، كما يجب تسجيلها في سجل أصول البيانات، قد تتضمّن هذه العوامل ما يلي:
   - فترة زمنيّة محدّدة بعد إنشاء البيانات أو تلقيها (مثلا: عامين بعد الإنشاء).
   - فترة زمنيّة محدّدة بعد اتخاذ آخر إجراء على البيانات (مثلا: ستة أشهر من تاريخ آخر استخدام).
   - بعد انقضاء تاريخ محدّد (مثلا، من المقرر مراجعتها في ١ يناير ٢٠٢١).
   - بعد ظروف أو أحداث معيّنة لها تأثيراً مباشراً على البيانات (مثلا: إحداث تغيير في الأوّلويات الاستراتيجيّة أو تغيير موظفي الوزارة).
٤. يتطلب إلغاء التّصنيف - رفع السرّيّة - أو خفض مستويات التّصنيف، بعيداً عن العوامل المساعدة على إلغاء التّصنيف الواضحة تماماً، فهماً سليماً لمحتوى البيانات السرّيّة والسّياق الذي وردت فيه.

٤,٥ الخطوات اللّازمة لتصنيف البيانات

٤,٥,١ الخطوة ١ – تحديد جميع بيانات الوزارة

جرد وتحديد جميع البيانات التي تمتلكها الوزارة.

٤,٥,٢ الخطوة ٢ – تعيين مسؤول تصنيف البيانات

بمجرد تحديد جميع البيانات يتم تفويض شخص يتولى مسؤوليّة عمليّة التّصنيف بإشراف ومتابع المكتب، غالباً ما يكون هذا الشخص هو ممثّل بيانات الأعمال وهو الذي يفهم طبيعة البيانات وقيمتها داخل الوزارة ويتحمّل المسؤوليّة حيال إجراء التّصنيف الأوّليّ، ونظراً إلى وجود أكثر من مسؤول بيانات داخل الوزارة، فقد يوجد أكثر من شخص مسؤول عن تصنيف البيانات.

٤,٥,٣ الخطوة ٣ – إجراء عمليّة تقييم الأثر

يجب على مسؤول تصنيف البيانات اتباع الخطوات اللّازمة لعمليّة تقييم الأثر المحتمل الذي يترتّب على:

١. الإفصاح عن هذه البيانات أو الوصول غير المصرّح به إليها.
٢. إجراء تعديل على هذه البيانات أو إتلافها أو كليهما.
٣. عدم الوصول إلى هذه البيانات في الوقت المناسب.

تبدأ عمليّة تقييم الأثر بتطبيق مبدأ "الأصل في البيانات الإتاحة" (في المجال التنموي) ما لم تقتضِ طبيعتها أو حساسيتها مستويات أعلى من التّصنيف والحماية؛ السرّيّة للغاية (في المجال السّياسي والآمني) ما لم تقتضِ طبيعتها أو حساسيتها مستويات أدنى من التّصنيف.

٤,٥,٣,١ الخطوة أ-٣ - تحديد فئة الأثر:

يتمثّل العنصر الأوّل من عمليّة تقييم الأثر في تحديد الفئة الرّئيسة والفرعيّة للأثر المحتمل في أيٍ من الفئات الرّئيسة التّالية:

١. المصلحة الوطنيّة.
٢. أنشطة الوزارة.
٣. صحة أو سلامة الأفراد.
٤. الموارد البيئية.

٤,٥,٣,٢ الخطوة ب-٣ - تحديد مستوى الأثر:

يتعيّن على مسؤول التصنيف أن يحدّد لكل أثر محتمل مستوى معين، يعتمد تحديد المستوى على الآتي:

١. مدّة الأثر وصعوبة السّيطرة على الضرر.
٢. فترة تدارك وإصلاح الأضرار بعد وقوعها.
٣. حجم الأثر على مستوى وطني، مناطقي، عدّة جهات، جهة واحدة، عدّة أفراد ... إلخ

تحدّد هذه المعايير مستويات الأثر الأربعة:

١. عالي: يؤدّي الوصول إلى البيانات أو الإفصاح عنها إلى حدوث أضرارٍ جسيمة أو خطيرة للغاية على المدى الطويل لا يمكن تداركها أو إصلاحها.
٢. متوسّط: يؤدّي الوصول إلى البيانات أو الإفصاح عنها إلى حدوث أضرار جسيمة أو خطيرة يصعب السّيطرة عليها.
٣. منخفض: يؤدّي الوصول إلى البيانات أو الإفصاح عنها إلى أضرارٍ محدودة يمكن السّيطرة عليها أو أضرار متقطّعة على المدى القصير يمكن السّيطرة عليها.
٤. لا يوجد أثر: لا يؤدّي الوصول إلى البيانات أو الإفصاح عنها إلى أي ضرر على المدى البعيد أو القريب.

يجب أن تكون جميع الأضرار المحتملة خلال عمليّة تقييم الأثر محدّدة وقائمة على أدلّة، في محاولةٍ للحدّ من التّقديرات الشّخصيّة للمكلّف بإجراء تصنيف البيانات.

يحدّد مسؤول التصنيف مستوى تصنيف البيانات بناءً على الآثار المحدّدة ومستوياتها:

١. عالٍ: تُصنّف البيانات باعتبارها "سرّية للغاية".
٢. متوسّط: تُصنف البيانات على أنّها "سرّية".
٣. منخفض: يلزم إجراء مزيدٍ من التقييمات (يرجى الاطّلاع على الخطوة ٤ و ٥).
٤. لا يوجد أثر: تُصنّف البيانات على أنّها بياناتٍ "عامّة".

ويوجد وصف مفصّل للاعتبارات الرّئيسة لكل فئة من فئات الأثر ومستواه في الجدول (٢) "فئات ومستويات تقييم أثر تصنيف البيانات" .

يجب الأخذ بعين الاعتبار الخطوتين ٤ و٥ عندما يكون مستوى الأثر المحدّد منخفض. يتمّ الانتقال إلى الخطوة ٦ عندما تُصنّف البيانات على أنّها "سرّية للغاية" أو "سرّية" أو "عامّة".

٤,٥,٤ الخطوة ٤ – تحديد الأنظمة ذات العلاقة (فقط إذا كان مستوى الأثر منخفضاً)

يجب إجراء تقييمات إضافيّة إذا كان مستوى الأثر المحدّد "منخفض" وذلك بهدف زيادة مستوى تصنيف البيانات المصنّفة على أنّها بيانات "عامّة" إلى الحدّ الأقصى.

يجب على مسؤول التصنيف في هذا الصدد، دراسة ما إذا كان الإفصاح عن هذه البيانات يتعارض مع أنظمة المملكة العربيّة السعوديّة مثل نظام مكافحة الجرائم المعلوماتيّة ونظام التّجارة االلكترونيّة ... الخ وإذا كان الإفصاح عن البيانات مخالفاً للأنظمة، فيجب حينها تصنيف البيانات على أنّها بيانات "مقيّدة"، بخلاف ذلك يتعيّن على ممثّل بيانات الأعمال مواصلة تنفيذ الخطوة ٥.

٤,٥,٥ الخطوة ٥ – الموازنة بين مزايا الإفصاح عن البيانات والآثار السّلبية (فقط إذا كانت الإجابة على الخطوة ٤ "لا")

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

١. إذا كانت المزايا أكبر من الآثار السّلبية، تصنّف البيانات على أنّها "عامّة."
٢. إذا كانت المزايا أقل من الآثار السّلبية، تصنّف البيانات على أنّها "مقيّدة".

٤,٥,٦ الخطوة ٦ – مراجعة مستوى التّصنيف

يجب فحص جميع البيانات المصنّفة لضمان أن يكون مستوى التّصنيف المحدّد من جانب ممثّل بيانات الأعمال هو الأنسب، وتتمّ مراجعته خلال شهر واحد من التّصنيف الأوّلي.

٤,٥,٧ الخطوة ٧ – تطبيق الضّوابط المناسبة

تتمثّل الخطوة الأخيرة من عمليّة تصنيف البيانات في حماية جميع البيانات وفقاً لمستوى التّصنيف عن طريق تطبيق عناصر التّحكم ذات الصّلة.

- يتمّ الإنتهاء من عمليّة التّصنيف عند تصنيف جميع البيانات التي تملكها الوزارة والتّحقّق من مستويات التّصنيف وتطبيق الضّوابط ذات الصّلة. بعد تصنيف البيانات على نحو صحيح، يمكن للوزارة مشاركتها مع جهات أخرى، أو إتاحتها ونشرها بصفتها بيانات مفتوحة عند تصنيفها بيانات "عامّة".

٤,٦ الأدوار والمسؤوليات داخل الوزارة

يتمّ تكليف أشخاص يتولون مسؤوليّة أداء الالتزامات المسندة لكل دورٍ من الأدوار الوظيفيّة المرتبطة بعمليّة تصنيف البيانات وشروط حمايتها على النّحو المنصوص عليه أدناه.

- **ممثّل بيانات الأعمال:** الشّخص المسؤول عن البيانات التي تجمعها الوزارة أو تحتفظ بها، وعادةً ما يكون في مستوى إداري عالٍ، ويكون ممثّل بيانات الأعمال مسؤول عن:

١. **تصنيف البيانات:** تصنيف البيانات التي تجمعها الوزارة والإدارات والمكاتب التابعة لها.

٢. **تجميع البيانات:** التأكّد من تصنيف البيانات المجمّعة من مصادرٍ متعدّدة على أعلى مستويات التّصنيف المستخدمة في تصنيف أي بيانات بشكل فردي.

٣. **تنسيق تصنيف البيانات:** التّأكّد من أنّ البيانات المتبادلة مصنّفة ومحميّة بصورة متّسقة.

٤. **الامتثال لتصنيف البيانات (بالتّنسيق مع مختصّي بيانات الأعمال):** التأكد من أنّ البيانات محميّة وفقاً للضّوابط المحدّدة.

- **مراجع تصنيف البيانات:** الشّخص المسؤول عن مراجعة واعتماد مستويات تصنيف البيانات التي يحدّدها ممثّل 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، ويتحمّل مسؤوليّة حماية البيانات عن طريق تطبيق الضّوابط المعتمدة المحدّدة في قسم "ضوابط تصنيف البيانات" بالإضافة إلى ذلك، الحفاظ على الأنظمة وقواعد البيانات والخوادم التي تخزّن البيانات ودعمها، وتتألّف مسؤوليات مختص بيانات الأعمال في:
  - التّحكّم في الوصول: التّأكّد من تطبيق ضوابط التّحكم في الوصول ورصدها ومراجعتها وفقًا لمستويات تصنيف البيانات التي يحدّدها ممثّل بيانات الأعمال.
  - تقارير المراجعة: إرسال تقرير سنوي إلى مسؤولي البيانات يتناول توافر البيانات المصنّفة وسلامتها وسرّيتها.
  - النّسخ الاحتياطي للبيانات: إجراء نسخ احتياطية منتظمة للبيانات.
  - التّحقّق من صحة البيانات: التّحقّق من صحّة البيانات بشكل دوري.
  - استعادة البيانات: استعادة البيانات من وسائط النّسخ الاحتياطي.
  - نشاط المراقبة: مراقبة الأنشطة التي تتمّ على البيانات وتسجيلها، بما في ذلك البيانات المتعلّقة بالشخص الذي يصل إلى هذه البيانات.
  - الامتثال لتصنيف البيانات (بالاشتراك مع مسؤولي البيانات): التّأكّد من تصنيف بيانات الوزارة وحمايتها بعد العمليّة الموضّحة في هذه السّياسة ووفقاً للضّوابط المحدّدة.
- **مستخدم البيانات:** الموظّف الذي يتعامل مع البيانات أو يصل إليها أو يستخدمها أو يحدّثها بغرض أداء مهمة يخولّها له ممثّل بيانات الأعمال، ويستغلّ المستخدمون البيانات بطريقة تتوافق مع الغرض المحدّد، وكذلك الامتثال لهذه السّياسة وجميع السّياسات المتعلّقة باستخدام البيانات في المملكة العربيّة السعوديّة، ويُكلّف المسؤول الأوّل بالوزارة (او من يفوضه) من يراه من ذوي الاختصاص لأداء هذه الأدوار.

٥ سياسة حماية البيانات الشّخصيّة

٥,١ نطاق السّياسة

تنطبق أحكام هذه السّياسة على جميع إدارات وزارة التّعليم الدّاخليّة والخارجيّة وإدارات ومكاتب التّعليم والمدارس التي تديرها أو تشرف عليها الوزارة، التي تقوم كليّاً أو جزئيّاً بمعالجة البيانات الشّخصيّة.

يستثنى من نطاق تطبيق هذه السّياسة، جمع البيانات الشّخصيّة 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 التّالية:

١. إذا كان جمع البيانات الشّخصيّة أو معالجتها مطلوباً لتحقيق متطلّبات نظاميّة وفقاً للأنظمة واللّوائح والسّياسات المعمول بها في المملكة أو لاستيفاء متطلّبات قضائيّة أو لتنفيذ التزام بموجب اتّفاق تكون المملكة طرفاً فيه.
٢. إذا كان جمع البيانات الشّخصيّة أو معالجتها ضرورياً لحماية الصّحة أو السّلامة العامّة أو حماية المصالح الحيويّة للأفراد.
٣. عندما تحقّق المعالجة مصلحة متحقّقة لصاحب البيانات وكان الاتّصال به متعذّراً أو من كان من الصّعب تحقيق ذلك.
٤. عندما تكون المعالجة بمقتضى نظام آخر أو تنفيذاً لاتّفاق سابق يكون صاحب البيانات الشّخصيّة طرفاً فيه.
٥. إذا كانت البيانات قد تمّ جمعها من مصدر متاح للعموم.
٦. إذا كان الإفصاح سيقتصر على معالجتها لاحقاً بطريقة لا تؤدّي إلى معرفة هوية صاحب البيانات الشّخصيّة أو أي فرد آخر على وجه التّحديد.

٥,٢ المبادئ الرّئيسيّة لحماية البيانات الشّخصيّة

المبدأ الأوّل: المسؤوليّة

أن يتمّ تحديد وتوثيق سياسات وإجراءات الخصوصيّة الخاصّة بالوزارة واعتمادها من قبل المسؤول الأوّل بالوزارة (أو من يفوّضه)، ونشرها إلى جميع الأطراف المعنيّة بتطبيقها.

المبدأ الثّاني: الشّفافيّة

أن يتمّ إعداد إشعار عن سياسات وإجراءات الخصوصيّة الخاصّة بالوزارة يحدّد فيه الأغراض التي من أجلها تمّت معالجة البيانات الشّخصيّة وذلك بصورة محدّدة وواضحة وصريحة.

المبدأ الثّالث: الاختيار والموافقة

أن يتمّ تحديد جميع الخيارات الممكنة لصاحب البيانات الشّخصيّة والحصول على موافقته (الضمنيّة أو الصّريحة) فيما يتعلّق بجمع بياناته واستخدامها أو الإفصاح عنها.

المبدأ الرّابع: الحدّ من جمع البيانات

أن يقتصر جمع البيانات الشّخصيّة على الحدّ الأدنى من البيانات الذي يمكّن من تحقيق الأغراض المحدّدة في إشعار الخصوصيّة.

المبدأ الخامس: الحدّ من استخدام البيانات والإحتفاظ بها والتّخلّص منها

أن يتمّ تقييد معالجة البيانات الشّخصيّة بالأغراض المحدّدة في إشعار الخصوصيّة والتي من أجلها قدّم صاحب البيانات موافقته الضمنيّة أو الصّريحة، والإحتفاظ بها طالما كان ذلك ضرورياً لتحقيق الأغراض المحدّدة أو لما تقتضيه الأنظمة واللّوائح والسّياسات المعمول بها في المملكة وإتلافها بطريقة آمنة تمنع التسرّب، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو الوصول غير المصرّح به نظاماً.

المبدأ السّادس: الوصول إلى البيانات

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

المبدأ السّابع: الحدّ من الإفصاح عن البيانات

أن يتمّ تقييد الإفصاح عن البيانات الشّخصيّة للأطراف الخارجيّة بالأغراض المحدّدة في إشعار الخصوصيّة والتي من أجلها قدّم صاحب البيانات موافقته الضمنيّة أو الصّريحة.

المبدأ الثّامن: أمن البيانات

أن تتمّ حماية البيانات الشّخصيّة من التسرّب، أو التلف، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو التعديل أو الوصول غير المصرّح به – وفقاً لما يصدر من الهيئة الوطنيّة للأمن السّيبراني والجهات ذات الاختصاص.

المبدأ التّاسع: جودة البيانات

أن يتمّ الإحتفاظ بالبيانات الشّخصيّة بصورة دقيقة، وكاملة، وذات علاقة مباشرة بالأغراض المحدّدة في إشعار الخصوصيّة.

المبدأ العاشر: المراقبة والامتثال

أن تتمّ مراقبة الامتثال لسياسات وإجراءات الخصوصيّة الخاصّة بالوزارة، ومعالجة الاستفسارات والشّكاوى والنّزاعات المتعلّقة بالخصوصيّة.

٥,٣ حقوق صاحب البيانات

أوّلاً: الحقّ في العلم ويشمل ذلك إشعاره بالأساس النّظامي أو الاحتياج الفعلي لجمع بياناته الشّخصيّة، والغرض من ذلك، وألاّ تعالج بياناته لاحقّاً بصورة تتنافى مع الغرض من جمعها والذي من أجله قدّم موافقته الضمنيّة أو الصّريحة.

ثانياً: الحقّ في الرجوع عن موافقته على معالجة بياناته الشّخصيّة - في أي وقت - ما لم تكن هناك أغراض مشروعة تتطلّب عكس ذلك.

ثالثاً: الحقّ في الوصول إلى بياناته الشّخصيّة لدى الوزارة، وذلك للاطّلاع عليها، وطلب تصحيحها، أو إتمامها، أو تحديثها، وطلب إتلاف ما انتهت الحاجة إليه منها، والحصول على نسخة منها بصيغة واضحة.

٥,٤ التزامات الوزارة فيما يخص حماية البيانات الشخصية

١. يقوم مكتب البيانات بالوزارة بإعداد وتطبيق السّياسات والإجراءات المتعلّقة بحماية البيانات الشّخصيّة، ويكون المسؤول الأوّل بالوزارة - أو من يفوّضه - مسؤولاً عن الموافقة عليها واعتمادها. ويكون المكتب هو المسؤل عن مراقبة الامتثال لهذه السّياسة بشكل دوري.

٢. يقوم المكتب بإنشاء وحدة لحوكمة البيانات وتسند إليها مسؤوليّة تطوير وتوثيق ومراقبة تنفيذ السّياسات والإجراءات المعتمدة من المسؤول الأوّل بالوزارة، على أن تتضمّن مهام ومسؤوليات الوحدة وضع المعايير المناسبة لتحديد مستويات حساسيّة البيانات الشّخصيّة.

٣. يقوم المكتب بتقييم المخاطر والآثار المحتملة لأنشطة معالجة البيانات الشّخصيّة وعرض نتائج التّقييم على المسؤول الأوّل بالوزارة - أو من يفوّضه - لتحديد مستوى قبول المخاطر وإقرارها.

٤. يقوم المكتب بمراجعة وتحديث العقود واتّفاقيات مستوى الخدمة والتّشغيل بما يتوافق مع سياسات وإجراءات الخصوصيّة المعتمدة من المسؤول الأوّل بالوزارة.

٥. يقوم المكتب بإعداد وتوثيق الإجراءات اللاّزمة لإدارة ومعالجة انتهاكات الخصوصيّة وتحديد المهام والمسؤوليّات المتعلّقة بفريق العمل المختص، والحالات التي يستوجب إشعار مكتب إدارة البيانات الوطنيّة بها حسب التّسلسل الإداري، بناءً على قياس شدّة الأثر.

٦. يقوم المكتب بإعداد برامج توعوية لتعزيز ثقافة الخصوصيّة ورفع مستوى الوعي وفقاً لسياسات وإجراءات الخصوصيّة المعتمدة من المسؤول الأوّل بالوزارة.

٧. يجب أن يتمّ إشعار صاحب البيانات - بطريقة ملائمة وقت جمع البيانات - بالغرض والأساس النّظامي /الاحتياج الفعلي والوسائل والطّرق المستخدمة لجمع ومعالجة ومشاركة البيانات الشّخصيّة وكذلك التّدابير الأمنيّة لضمان حماية الخصوصيّة حسب الأنظمة واللّوائح والسّياسات المعمول بها في المملكة.

٨. يجب أن يتمّ إشعار صاحب البيانات عن المصادر الأخرى التي يتمّ استخدامها في حال تمّ جمع بيانات إضافيّة بطريقة غير مباشرة (من جهات أخرى).

٩. يجب أن يتمّ تزويد صاحب البيانات بالخيارات المتاحة فيما يتعلّق بمعالجة البيانات الشّخصيّة والآليّة المستخدمة لممارسة هذه الخيارات، ومنها على سبيل المثال (Preferences, Opt-in and Opt-out) .

١٠. يجب أن يتمّ أخذ موافقة صاحب البيانات على معالجة البيانات الشّخصيّة بعد تحديد نوع الموافقة (صريحة أو ضمنيّة) بناءً على طبيعة البيانات وطرق جمعها.

١١. يقوم المكتب بالتأكّد من أنّ الغرض من جمع البيانات متوافقاً مع الأنظمة واللّوائح والسّياسات المعمول بها في المملكة وذا علاقة مباشرة بنشاط الوزارة.

١٢. أن يكون محتوى البيانات مقتصراً على الحدّ الأدنى من البيانات اللاّزمة لتحقيق الغرض من جمعها.

١٣. تقييد جمع البيانات على المحتوى المعدّ سلفاً (الموضح في القاعدة ١٢) ويكون بطريقة عادلة (مباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التّضليل) .

١٤. اقتصار استخدام البيانات على الغرض التي جُمعت من أجله.
١٥. يقوم المكتب بإعداد وتوثيق سياسة وإجراءات الإحتفاظ بالبيانات وفقاً للأغراض المحدّدة والأنظمة والتّشريعات ذات العلاقة.
١٦. يجب أن يتمّ تخزين البيانات الشّخصيّة ومعالجتها من قبل الوزارة داخل الحدود الجغرافيّة للمملكة لضمان المحافظة على السّيادة الوطنيّة الرقميّة لهذه البيانات، ولا تجوز معالجتها خارج المملكة إلا بعد حصول الوزارة على موافقة كتابيّة من الجهة التّنظيميّةالمسؤلة، بعد تنسيق الجهة التّنظيميّة مع مكتب إدارة البيانات الوطنيّة.
١٧. يقوم المكتب بإعداد وتوثيق سياسة وإجراءات التّخلّص من البيانات لإتلاف البيانات بطريقة آمنة تمنع فقدانها أو إساءة استخدامها أو الوصول غير المصرّح به إليها - وتشمل البيانات التشغيليّة، المؤرشفة، والنّسخ الاحتياطيّة - وذلك وفقاً لما يصدر من الهيئة الوطنيّة للأمن السّيبراني.
١٨. يجب تضمين أحكام سياستي الإحتفاظ والتّخلّص من البيانات الخاصّة بالوزارة في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.
١٩. تحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشّخصيّة وذلك لمراجعتها وتحديثها.
٢٠. التّحقّق من هويّة الأفراد قبل منحهم الوصول إلى بياناتهم الشّخصيّة وفقاً للضّوابط المعتمدة من قبل الهيئة الوطنيّة للأمن السّيبراني والجهات ذات الاختصاص.
٢١. يحظر مشاركة البيانات الشّخصيّة مع جهات أخرى إلا وفقاً للأغراض المحدّدة وبعد موافقة صاحب البيانات ووفقاً للأنظمة واللّوائح والسّياسات على أن تُزوّد الجهات الأخرى بسياسات وإجراءات الخصوصيّة المتّبعة وتضمينها في العقود والاتّفاقيات.
٢٢. إشعار أصحاب البيانات وأخذ الموافقة منهم في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الأغراض المحدّدة.
٢٣. أخذ موافقة مكتب إدارة البيانات الوطنيّة قبل مشاركة البيانات الشّخصيّة مع جهات أخرى خارج المملكة.
٢٤. أن يقوم المكتب بإعداد وتوثيق ومتابعة تطبيق الإجراءات اللّازمة لضمان دقّة البيانات الشّخصيّة واكتمالها وحداثتها وارتباطها بالغرض الذي جُمعت من أجله.
٢٥. استخدام الضّوابط الإداريّة والتّدابير التّقنيّة المعتمدة في سياسات الوزارة لأمن المعلومات لضمان حماية البيانات الشّخصيّة ومنها على سبيل المثال لا الحصر:

- منح صلاحيات الوصول إلى البيانات وفقاً لمهام العاملين ومسؤوليّاتهم بطريقة تحول دون تداخل الاختصاص وتتلافى تشتيت المسؤوليات.
- تطبيق الإجراءات الإداريّة والتّدابير التّقنيّة التي توثّق مراحل معالجة البيانات وتوفّر إمكانيّة تحديد المستخدم المسؤول عن كل مرحلة من هذه المراحل (سجّلات الاستخدام) .
- توقيع العاملين الذين يباشرون عمليّات معالجة البيانات على تعهّد للمحافظة على البيانات وعدم الإفصاح عنها إلا وفقاً للسّياسات والإجراءات والأنظمة والتّشريعات.
- اختيار العاملين الذين يباشرون عمليّات معالجة البيانات ممن يتّصفون بالأمانة والمسؤوليّة ووفقاً لطبيعة وحساسيّة البيانات وسياسة الوصول المعتمدة من قبل الوزارة.
- استخدام التّدابير الأمنيّة المناسبة - كالتّشفير، وعزل بيئة التّطوير والاختبار عن بيئة التّشغيل - لأمن البيانات الشّخصيّة وحمايتها بما يتناسب مع طبيعتها وحساسيّتها والوسائط المستخدمة لنقلها وتخزينها وفقاً لما يصدر من الهيئة الوطنيّة للأمن السّيبراني والجهات ذات الاختصاص.

٢٦. يقوم المكتب بمراقبة الامتثال لسياسات وإجراءات الخصوصيّة بشكل دوري ويتمّ عرضها على المسؤول الأوّل بالوزارة - أو من يفوّضه - كما يتمّ تحديد وتوثيق الإجراءات التّصحيحيّة التي سيتمّ اتخاذها في حال عدم الامتثال.
٢٧. يتولى مكتب إدارة البيانات بالوزارة مواءمة أحكام هذه السّياسة مع وثائقها التّنظيميّة وتعميمها على جميع الجهات التّابعة لها أو المرتبطة بها بما يحقّق التّكامل ويضمن تحقيق الهدف المنشود من إعداد هذه السّياسة.
٢٨. أن تكون الوزارة مسؤولة عن مراقبة الإمتثال لتنفيذ هذه السّياسات وفقاً للآليات والإجراءات التي تحدّدها الجهات التّنظيميّة.
٢٩. على الوزارة إبلاغ الجهات التّنظيميّة بالتنسق مع مكتب إدارة البيانات الوطنية فوراً ودون تأخير وبما لا يتجاوز ٧٢ ساعة من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشّخصيّة وفقاً للآليات والإجراءات التي تحدّدها الجهات التّنظيميّة.

٣٠. يجب على الوزارة عند تعاقدها مع جهات المعالجة أن تتحقّق بشكل دوري من امتثال جهات المعالجة لهذه السّياسة وفقاً للآليّات والإجراءات التي تحدّدها الجهات التّنظيميّة، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها جهات المعالجة.

٣١. يحقّ للوزارة وضع قواعد إضافيّة لمعالجة أنواع محدّدة من البيانات الشّخصيّة وفقاً لطبيعة وحساسيّة هذه البيانات بعد التّنسيق مع مكتب إدارة البيانات الوطنيّة.

٣٢. تقوم الوزارة - بعد التّنسيق مع مكتب إدارة البيانات الوطنيّة - بإعداد الآليات والإجراءات التي تنظّم عمليّة معالجة الشّكاوى وفقاً لإطار زمني محدّد وحسب التّسلسل التّنظيمي للجهات.

٦ سياسة مشاركة البيانات

٦,١ نطاق السّياسة

تنطبق أحكام هذه السّياسة على جميع إدارات وزارة التّعليم الدّاخليّة والخارجيّة وإدارات ومكاتب التّعليم والمدارس التي تديرها أو تشرف عليها الوزارة وذلك عند مشاركة البيانات التي تنتجها وزارة التّعليم - مع جهات حكوميّة أخرى أو جهات خاصّة أو أفراد - مهما كان مصدر هذه البيانات، أو شكلها أو طبيعتها، ويشمل ذلك السّجلات الورقيّة ورسائل البريد الالكتروني والبيانات المخزّنة على الوسائط الالكترونيّة أو أشرطة الصّوت أو الفيديو أو الخرائط أو الصّور الفوتوغرافيّة أو المخطوطات أو الوثائق المكتوبة بخط اليد، أو أي شكل آخر من أشكال البيانات المسجّلة.

لا تنطبق أحكام هذه السّياسة في حال كانت الجهة الطّالبة للبيانات جهة حكوميّة وكان الطّلب لأغراض أمنيّة أو لإستيفاء متطلّبات قضائيّة.

٦,٢ المبادئ الرّئيسيّة لمشاركة البيانات

المبدأ الأوّل: تعزيز ثقافة المشاركة

أن تشارك الوزارة بياناتها مع الجهات الحكوميّة الأخرى لتحقيق التّكامل وتبنّي "مبدأ المرّة الواحدة" للحصول على البيانات من مصادرها الصّحيحة والحدّ من ازدواجيتها وتعارضها وتعدّد مصادرها. وفي حال أنّ الوزارة ليست هي المصدر الرئيسي للبيانات المطلوب مشاركتها فعلى مكتب إدارة البيانات بالوزارة أخذ موافقة الجهة الرّئيسيّة ومصدر البيانات قبل مشاركتها مع الجهة الطّالبة.

المبدأ الثّاني: مشروعيّة الغرض

أن يكون الغرض من مشاركة الوزارة بياناتها مع جهة أخرى مشروع ومبني على أساس نظامي أو احتياج عملي مسوّغ يهدف إلى تحقيق مصلحة عامّة دون إلحاق أي ضرر بالمصالح الوطنيّة، أو أنشطة الوزارة أو خصوصيّة الأفراد أو سلامة البيئة، ويستثنى من ذلك البيانات والجهات المستثناة بأوامر سامية.

المبدأ الثّالث: الوصول المصرّح به

أن يكون لدى جميع الأطراف المُشارِكة في مشاركة البيانات صلاحيّة الاطّلاع على هذه البيانات والحصول عليها واستخدامها (وهذه الصّلاحية قد تتطلّب المسح الأمني قبل منحها حسب طبيعة وحساسيّة البيانات)، بالإضافة إلى المعرفة، والمهارة، والأشخاص المؤهّلين والمدرّبين بشكل صحيح للتّعامل مع البيانات المشتركة.

المبدأ الرّابع: الشّفافيّة

أن تقوم جميع الأطراف المشاركة في عمليّات مشاركة البيانات بإتاحة جميع المعلومات الضّرورية لتبادل البيانات بما في ذلك: البيانات المطلوبة، الغرض من جمعها، ووسائل نقلها، وطرق حفظها، والضّوابط المستخدمة لحمايتها وآلية التّخلّص منها.

المبدأ الخامس: المسؤوليّة المشتركة

أن تكون جميع الأطراف المشاركة في مشاركة البيانات مسؤولين مسؤوليّة مشتركة عن قرارات مشاركة البيانات ومعالجتها وفقاً للأغراض المحدّدة، وضمان تطبيق الضّوابط الأمنيّة المنصوص عليها في اتّفاقيّة مشاركة البيانات، والأنظمة والتّشريعات والسّياسات ذات العلاقة.

المبدأ السّادس: أمن البيانات

أن تقوم جميع الأطراف المُشارِكة في مشاركة البيانات بتطبيق الضّوابط الأمنيّة المناسبة لحماية البيانات ومشاركتها في بيئة آمنة وموثوقة وفقاً للأنظمة والتّشريعات ذات العلاقة، ووفقاً لما يصدر من الهيئة الوطنيّة للأمن السّيبراني.

المبدأ السّابع: الاستخدام الأخلاقي

أن تقوم جميع الأطراف المُشارِكة في مشاركة البيانات بتطبيق الممارسات الأخلاقيّة أثناء عمليّة مشاركة البيانات لضمان استخدامها في إطار من العدالة والنّزاهة والأمانة والإحترام، وعدم الإكتفاء بالالتزام بسياسات أمن المعلومات أو الالتزام بالمتطلّبات التّنظيميّة والتّشريعيّة ذات العلاقة.

٦,٣ الخطوات اللّازمة لإجراء عمليّة مشاركة البيانات

فيما يلي الخطوات الأساسيّة لعمليّة مشاركة البيانات لتوحيد ممارسات المشاركة داخل الوزارة وضمان استيفاء جميع الضّوابط والمتطلّبات اللّازمة، والتي قد لا تتجاوز ٣ أشهر.

١. يقوم مقدّم الطّلب - سواء أكان جهة حكوميّة أو خاصّة أو فرداً - بإرسال طلب مشاركة بيانات إلى مكتب إدارة البيانات بالوزارة على أن يُرسل الطّلب عن طريق مكتب إدارة البيانات بالجهة في حال كان مقدّم الطّلب جهة حكوميّة.

٢. يقوم المكتب بالتّحقّق الأوّلي من مشروعيّة الطّلب ثم يتمّ إحالة الطّلب إلى ممثّل بيانات الأعمال المختص بالوزارة والذي بدوره يقوم بتوجيه هذا الطّلب إلى أحد مختصيّ بيانات الأعمال لتقييم هذا الطّلب ومعالجته.

٣. يقوم مختص بيانات الأعمال بالتّحقّق من مستوى تصنيف البيانات المطلوبة:

- في حالة عدم تحديد مستوى التّصنيف، يجب على المكتب تصنيف البيانات المطلوبة وفقاً لسياسة تصنيف البيانات.
- في حالة تحديد مستوى التّصنيف على أنّه "عامّ"، يمكن لمختص بيانات الأعمال مشاركة البيانات المطلوبة دون تقييم الطّلب وفقاً للمبادئ الرّئيسيّة لمشاركة البيانات. ويكون توقيع اتفاقية مشاركة البيانات اختيارياً وحسب ما تراه الوزارة مناسباً.
- في حالة تحديد مستوى التّصنيف على أنّه "مقيّد" أو "سرّي" أو "سرّي للغاية"، يتعيّن على مختص بيانات الأعمال تقييم الطّلب وفقاً للمبادئ الرّئيسيّة لمشاركة البيانات.

٤. يجب على مختص بيانات الأعمال استكمال عمليّة المشاركة إذا تمّ استيفاء جميع مبادئ مشاركة البيانات بالكامل.

٥. لا يجوز لمختص بيانات الأعمال الاستمرار في مشاركة البيانات في حالة عدم استيفاء مبدأ واحد أو أكثر من مبادئ مشاركة البيانات. كما يجب عليه أن يردّ الطّلب إلى مقدّم الطّلب مع الملاحظات وإتاحة الفرصة لتلبية جميع مبادئ مشاركة البيانات غير المتوافقة.

٦. عند استيفاء جميع مبادئ مشاركة البيانات، يقوم مختص بيانات الأعمال بالحصول على موافقة ممثّل بيانات الأعمال على استكمال عمليّة مشاركة البيانات.

٧. يقوم مختص بيانات الأعمال بتحديد الضّوابط المناسبة لضمان الالتزام بمبادئ مشاركة البيانات وتحقيق الأهداف المحدّدة لكلّ منها، كما يجب أن يتمّ الاتّفاق بين مختص بيانات الأعمال ومقدّم الطّلب والأطراف الأخرى المشاركة في عمليّة المشاركة على تطبيق هذه الضّوابط.

٨. بعد الاتّفاق على ضوابط مشاركة البيانات والالتزام بتطبيقها، ينبغي لمختص بيانات الأعمال توضيحها بالتّفصيل في الاتّفاقيّة ويجب على جميع الأطراف المُشارِكة في عمليّة المشاركة التّوقيع على اتّفاقيّة مشاركة البيانات.

٩. يمكن لممثّل بيانات الأعمال مشاركة البيانات المطلوبة مع الجهة الطّالبة بعد توقيع اتّفاقيّة مشاركة البيانات.

٦,٤ الإطار الزمني لعمليّة مشاركة البيانات

الخطوة	المدّة الزمنيّة كحد أعلى (يوم)
تقييم الطّلب من تاريخ استلام الطّلب إلى إشعار مقدّم الطّلب بقرار المشاركة.	٣٠
وفي حال عدم الموافقة على طلب المشاركة، فيحقّ لمقدّم الطّلب استكمال المتطلّبات لتصويب الملاحظات وطلب الاستئناف لإعادة تقييم الطّلب وإصدار قرار المشاركة من تاريخ استلام الاستئناف.	١٤
إعداد وتوقيع اتّفاقيّة مشاركة بيانات.	٦٠
مشاركة البيانات مع مقدم الطّلب بعد قبول الطّلب ووجود اتّفاقيّة مشاركة بيانات موقّعة وسارية المفعول.	٧

٦,٥ ضوابط مشاركة البيانات

يجب الالتزام والموافقة على الضّوابط التّالية قبل مشاركة بيانات الوزارة مع أي جهة أخرى:

الأساس النّظامي: (المبادئ ذات العلاقة: المبدأ الأوّل: تعزيز ثقافة المشاركة، المبدأ الثّاني: مشروعيّة الغرض، المبدأ الخامس: المسؤوليّة المشتركة، المبدأ السّابع: الاستخدام الأخلاقي).

- أن يُوضّح الأساس النّظامي أو الاحتياج الفعلي لمشاركة البيانات، ومنها على سبيل المثال: تنظيم الجهة الطّالبة (الأمر الملكي/السّامي) الذي يسمح لها بمشاركة بيانات الوزارة، أو وجود اتّفاقيّة مشاركة بيانات موقّعة بين الوزارة وهذه الجهة.
- أن يتمّ الالتزام بمستويات تصنيف البيانات والمحافظة على حقوق الملكيّة الفكريّة وخصوصيّة البيانات الشّخصيّة.

التّفويض: (المبادئ ذات العلاقة: المبدأ الثّالث: الوصول المصرّح به، المبدأ السّادس: أمن البيانات).

- أن يتمّ تحديد الجهات والأشخاص المخوّلين بطلب البيانات وتلقّيها (يمكن التّحقّق من الامتثال لسياسة تصنيف البيانات وضوابط الإستخدام والوصول إلى البيانات).

نوع البيانات: (المبادئ ذات العلاقة: المبدأ الأوّل: تعزيز ثقافة المشاركة، المبدأ الثّاني: مشروعيّة الغرض، المبدأ الرّابع: الشّفافيّة).

- أن يتمّ التّأكّد من أنّ البيانات المطلوبة ضمن البيانات الرّئيسيّة التي تنتجها الوزارة لضمان طلب البيانات من مصدرها الصّحيح.
- أن يُحدّد الحدّ الأدنى من البيانات المطلوبة لتحقيق الأغراض المحدّدة.
- أن تحدّد البيانات المطلوبة وصيغتها والمتطلّبات المتعلّقة بتعديلها أو تغييرها (مثل صيغة البيانات، دقّة البيانات، مستوى التّفاصيل، هيكلة البيانات، نوع البيانات خام أو بيانات مُعالجة).

المعالجة المسبقة للبيانات: (المبادئ ذات العلاقة: المبدأ السّادس: أمن البيانات).

- أن تحدّد ما إذا كان هناك حاجة لمعالجة البيانات قبل مشاركتها، وفي حال الحاجة لذلك يتمّ الاتّفاق على أساليب المعالجة المطلوبة على سبيل المثال، الحجب وإخفاء الهويّة والتجميع (على ألا تتمّ معالجة البيانات بشكل يغيّر المحتوى).
- أن تُقيّم جودة البيانات المطلوبة وصحّتها وسلامتها وتحديد ما إذا كانت تتطلّب إجراء تحسين قبل مشاركتها، وفي حال الحاجة لذلك يجب على الجهة المسؤولة داخل الوزارة تدقيق البيانات قبل مشاركتها.

وسائل مشاركة البيانات: (المبادئ ذات العلاقة: المبدأ السّادس: أمن البيانات).

- الالتزام بضوابط أمن وحماية البيانات التي تصدّرها الإدارة العامّة للأمن السّيبراني داخل الوزارة والهيئة الوطنيّة للأمن السّيبراني.
- أن يتمّ تحديد وسائل مشاركة البيانات الماديّة والرقميّة.
- أن يتمّ التّحقّق من أمن وموثوقيّة وسائل المشاركة للتقليل من المخاطر المحتملة، كما يمكن الاستفادة من وسائل المشاركة الآمنة المعتمدة بين الجهات.
- أن يتمّ تحديد آلية مشاركة البيانات، وما إذا كانت الجهة المختصّة بالوزارة ستقوم بنقل البيانات مباشرةً إلى الجهة الطّالبة أو سيتمّ الاستعانة بمقدّم خدمة لإتمام عمليّة المشاركة.
- أن يتمّ تحديد ما إذا كان سيتمّ استخدام وسائط المشاركة الموجودة (على سبيل المثال، قناة التّكامل الحكوميّة، شبكة مركز المعلومات الوطني) أو سيتمّ استخدام وسائط مختلفة (شبكة الإنترنت اللّاسلكية، وإمكانيّة الوصول عن بعد، والشّبكة الافتراضيّة الخاصّة، وواجهة برمجة التّطبيقات).
- أن يتمّ الاتّفاق على آلية إتلاف الوسائط الماديّة المستخدمة في مشاركة البيانات.

استخدام البيانات والحفاظ عليها: (المبادئ ذات العلاقة: المبدأ الثّاني: مشروعيّة الغرض، المبدأ الرّابع: الشّفافيّة، المبدأ السّادس: أمن البيانات، المبدأ السّابع: الاستخدام الأخلاقي).

- أن تحدّد متطلّبات حماية البيانات عند مشاركتها، وتطبيق الضّوابط المحدّدة لحماية البيانات بعد مشاركتها.
- أن تُفرض قيود مناسبة على الاستخدام أو المعالجة المسموح بها للبيانات (إن وُجدت)، مثل قيود خاصّة بالمعالجة، أو قيود مكانيّة أو زمانيّة، أو حقوق حصريّة أو تجاريّة.
- أن تحدّد حقوق جميع الأطراف المشاركة في عمليّة المشاركة، وإجراءات تسوية النّزاعات والتّحكيم.
- أن تحدّد ما إذا كان هنالك طرف ثالث سيستفيد من البيانات بعد المشاركة والاتّفاق على الآلية المنظّمة لذلك.

مدّة مشاركة البيانات وعدد مرات المشاركة وإلغاء المشاركة: (المبادئ ذات العلاقة: المبدأ الثّاني: مشروعيّة الغرض، المبدأ السّادس: أمن البيانات).

- أن تحدّد مدّة مشاركة البيانات والموعد النّهائي للوصول إلى البيانات أو تخزينها.
- أن تحدّد عدد مرات مشاركة البيانات، والمتطلّبات اللّازمة للمراجعة، وإجراء التّعديلات، والإجراءات التي سيتمّ اتخاذها عند انتهاء الاتّفاقيّة (مثل إخفاء هويّة أصحاب البيانات أو إلغاء الوصول إلى البيانات أو إتلافها).

- أن تحدّد الأطراف الذين يحقّ لهم إنهاء مشاركة البيانات قبل التّاريخ المتّفق عليه، المستند النّظامي، وفترة الإشعار المسموح بها.

أحكام المسؤوليّة: (المبادئ ذات العلاقة: المبدأ الخامس: المسؤوليّة المشتركة).

- أن يُتّفق على تحديد المسؤوليّات في حال عدم الالتزام ببنود الاتّفاقيّة، وغيرها من الالتزامات بين الأطراف المشاركة كإنهاء الاتّفاقيّة والإجراءات التّصحيحيّة.
- أن تحدّد القواعد المتعلّقة بأحكام المسؤوليّة عند مشاركة بيانات خاطئة، وجود مشاكل فنيّة أثناء عمليّة نقل البيانات، أو فقدان البيانات بشكل غير مقصود أو غير نظامي مما قد يتسبّب في أضرار أخرى.

٦,٦ القواعد العامّة لمشاركة البيانات

فيما يلي القواعد العامّة التي يجب اتباعها عند مشاركة البيانات:

١. يجب منح الأولويّة لوسائط المشاركة المعتمدة والآمنة لتبادل البيانات، ومنها على سبيل المثال قناة التّكامل الحكوميّة، شبكة مركز المعلومات الوطني.
٢. يتولى مختص بيانات الأعمال بالوزارة مسؤوليّة مشاركة البيانات بعد استيفاء جميع مبادئ مشاركة البيانات، بالإضافة إلى تحديد الضّوابط المناسبة للمشاركة.
٣. يجب على كل جهة تعيين أو تفويض الشّخص المناسب - حسب المؤهّلات والتّدريب المطلوب - للتّعامل مع البيانات بطريقة صحيحة، على أن يكون مصرّح له طلب البيانات المشتركة وتلقّيها والوصول إليها وتخزينها وإتلافها.
٤. يجب إخفاء هوية أصحاب البيانات الشّخصيّة، إلا إذا كان ذلك ضرورياً لغرض المشاركة مع تحديد الضّوابط اللّازمة للحفاظ على خصوصيّة أصحاب البيانات وفقاً لسياسة خصوصيّة البيانات الشّخصيّة.
٥. إرفاق البيانات الوصفيّة (metadata) عند مشاركة البيانات في الحالات التي تتطلّب ذلك.
٦. تكون الجهات المشاركة في مشاركة البيانات مسؤولة عن حماية البيانات واستخدامها وفقاً للأغراض المحدّدة، ويحقّ لمكتب البيانات في الوزارة مراجعة مدى الالتزام بشكل دوري أو عشوائي بما يتوافق مع الضّوابط المحدّدة في اتّفاقيّة مشاركة البيانات.
٧. في حال وجود نزاع بين الأطراف المشاركة في عمليّة مشاركة البيانات، يحقّ للجهات التّابعة لنفس الجهة التّنظيميّة إشعار الجهة التّنظيميّة والمطالبة بتسوية النزاع بين الأطراف المشاركة، وفي حال لم يتمّ حل النّزاع، يتمّ إشعار مكتب إدارة البيانات الوطنيّة بذلك ليتولى تسوية النّزاع إذا كانت الجهتان غير خاضعتين لنفس الجهة التّنظيميّة.
٨. على الجهات المشاركة في مشاركة البيانات إيجاد التّوازن المناسب بين الحاجة إلى مشاركة البيانات وضمان حماية سرّية البيانات والمخاطر المحتملة على الفرد أو المجتمع.
٩. يجب على الجهات عند استلامها للبيانات المشتركة عدم مشاركتها مع طرف آخر أو جهة أخرى دون موافقة الجهة المنتجة للبيانات.
١٠. إخضاع جميع الاتّفاقيات والعمليّات التي تتعلّق بمشاركة البيانات أو معالجتها لمراجعة دوريّة من قبل المكتب بالتّعاون مع الوكالات والإدارات الشّريكة بالوزارة لتّأكّد من أنّها تحقّق غرضها وأنّ العمليّات تعمل على نحو فعّال.
١١. يجب على المكتب الإحتفاظ بسجلات خاصّة بطلبات مشاركة البيانات والقرارات المتعلّقة بها.
١٢. أن يكون المكتب مسؤول عن مراقبة الإمتثال لتنفيذ هذه السّياسات.

٧ سياسة حرّية المعلومات

٧,١ نطاق السّياسة

تنطبق هذه السّياسة على جميع طلبات الأفراد للاطّلاع أو الحصول على المعلومات العامّة - غير المحميّة - التي تنتجها جميع إدارات الوزارة الدّاخليّة والخارجيّة وإدارات ومكاتب التّعليم والمدارس التي تديرها أو تشرف عليها الوزارة، ويشمل ذلك السّجلات الورقيّة ورسائل البريد الالكتروني والمعلومات المخزّنة على الوسائط الالكترونيّة أو أشرطة الصّوت أو الفيديو أو الخرائط أو الصّور الفوتوغرافيّة أو المخطوطات أو الوثائق المكتوبة بخط اليد، أو أي شكل آخر من أشكال المعلومات المسجّلة.

لا تنطبق أحكام هذه السّياسة على المعلومات المحميّة التالية:

١. المعلومات التي يؤدّي إفشاؤها إلى الإضرار بالأمن الوطنيّ للدّولة أو سياساتها أو مصالحها أو حقوقها.
٢. المعلومات العسكريّة والأمنيّة.
٣. المعلومات والوثائق التي يتمّ الحصول عليها بمقتضى اتّفاق مع دولة أخرى وتصنّف على أنّها محميّة.
٤. التّحريات والتّحقيقات وأعمال الضّبط وعمليّات التّفتيش والمراقبة المتعلّقة بجريمة أو مخالفة أو تهديد.
٥. المعلومات التي تتضّمن توصيات أو اقتراحات أو استشارات من أجل إصدار تشريع أو قرار حكومي لم يصدر بعد.
٦. المعلومات ذات الطّبيعة التّجاريّة أو الصّناعيّة أو الماليّة أو الاقتصاديّة التي يؤدّي الإفصاح عنها إلى تحقيق ربح أو تلافي خسارة بطريقة غير مشروعة.
٧. الأبحاث العلميّة أو التّقنيّة، أو الحقوق المشتملة على حقّ من حقوق الملكيّة الفكريّة التي يؤدّي الكشف عنها إلى المساس بحقّ معنوي.
٨. المعلومات المتعلّقة بالمنافسات والعطاءات والمزايدات التي يؤدّي الإفصاح عنها إلى الإخلال بعدالة المنافسة.
٩. المعلومات التي تكون سرّية أو شخصيّة بموجب نظام آخر، أو تتطلّب إجراءات نظاميّة معيّنة للوصول إليها أو الحصول عليها.

٧,٢ المبادئ الرّئيسيّة لحرّية المعلومات

المبدأ الأوّل: الشّفافيّة

للفرد الحقّ في معرفة المعلومات المتعلّقة بأنشطة الجهات العامّة تعزيزاً لمنظومة النّزاهة والشّفافيّة والمساءلة.

المبدأ الثّاني: الضرورة والتناسب

أي قيود على طلب الاطّلاع أو الحصول على المعلومات المحميّة التي تتلقّاها أو تنتجها أو تتعامل معها الجهات العامّة يجب أن تكون مسوّغة بطريقة واضحة وصريحة.

المبدأ الثّالث: الأصل في المعلومات العامّة الإفصاح

لكل فرد الحقّ في الاطّلاع على المعلومات العامّة - غير المحميّة - وليس بالضرورة أن يتمتّع مقدّم الطّلب بحيثيّة معيّنة أو باهتمام معيّن بهذه المعلومات ليتمّكن من الحصول عليها، كما لا يتعرّض لأي مساءلة قانونية متعلّقة بهذا الحقّ.

المبدأ الرّابع: المساواة

يتمّ التّعامل مع جميع طلبات الاطّلاع أو الحصول على المعلومات العامّة على أساس المساواة وعدم التمييز بين الأفراد.

٧,٣ حقوق الأفراد فيما يتعلّق بالاطّلاع على المعلومات العامّة أو الحصول عليها

أوّلاً: حقّ الاطّلاع والحصول على أي معلومة غير محميّة لدى الوزارة.

ثانياً: الحقّ في معرفة سبب رفض الاطّلاع أو الحصول على المعلومات المطلوبة.

ثالثاً: الحقّ في التظلّم على قرار رفض طلب الاطّلاع والحصول على المعلومات المطلوبة.

٧,٤ الخطوات الرّئيسيّة للاطلاع على المعلومات أو الحصول عليها

٧,٤,١ المتطلّبات الرّئيسيّة لطلبات الوصول إلى المعلومات العامّة أو الحصول عليها:

١. طلب خطّي أو الكتروني.
٢. تعبئة "نموذج طلب معلومات عامّة" المعتمد من قبل الوزارة.
٣. أن يكون الطّلب لأغراض الوصول إلى المعلومات العامّة أو الحصول عليها.
٤. تضمين نموذج الطّلب على تفاصيل حول كيفيّة إرسال القرار النّهائي والإشعارات إلى الفرد (العنوان الوطني أو البريد الالكتروني أو الموقع... إلخ).
٥. إرسال نموذج الطّلب مباشرة إلى الوزارة.

٧,٤,٢ الخطوات الرّئيسة لطلب الاطّلاع أو الحصول على المعلومات العامّة:

أوّلاً: يتمّ تقديم الطّلبات عن طريق تعبئة "نموذج طلب معلومات عامّة" - الكتروني أو ورقي - وتقديمه لمكتب إدارة البيانات بالوزارة الذي بدوره يتأكّد من مشروعيّة الطّلب وأنّه لأغراض الوصول الى المعلومات العامّة أو الحصول عليها ومن ثمّ يتمّ توجيه الطّلب لممثّل بيانات الأعمال بالوزارة لتقييم الطّلب ومعالجته.

ثانياً: يقوم المكتب خلال فترة زمنيّة محدّدة (٣٠ يومًا) من استلام طلب الاطّلاع أو الحصول على المعلومات العامّة، باتخاذ أحد القرارات الآتية:

١. الموافقة: في حال تمّت موافقة الوزارة على طلب الوصول إلى المعلومات أو الحصول عليها كلّيًا أو جزئيًا؛ فيجب إشعار الفرد خطيّاً أو الكترونيّاً بالرّسوم المطبّقة، ومن ثمّ إتاحة هذه المعلومات للفرد خلال فترة زمنيّة لا تتجاوز (١٠) أيام عمل من استلام المبلغ.
٢. الرّفض: في حال تمّ رفض طلب الوصول إلى المعلومات أو الحصول عليها، فيجب أن يكون الرّفض خطيّاً أو الكترونيّاً على أن يتضمّن المعلومات التّالية:
   - تحديد ما إذا كان رفض الطّلب كلّيًا أو جزئيًا.
   - أسباب الرّفض، إن أمكن.
   - الحقّ في التظلّم على هذا الرّفض وكيفيّة ممارسة هذا الحقّ.
٣. التّمديد: في حال عدم إمكانيّة معالجة طلب الوصول إلى المعلومات في الوقت المحدّد، ينبغي على المكتب تمديد الفترة التي سيتمّ الرد فيها بمدّة معقولة حسب حجم وطبيعة المعلومات المطلوبة - على سبيل المثال لا تتجاوز (٣٠) يوماً إضافياً - وتزويد الفرد بالمعلومات التّالية:
   - إشعار التّمديد والتّاريخ المتوقع فيه إكمال الطّلب .
   - أسباب التّأخير.
   - الحقّ في التّظلّم على هذا التّمديد وكيفيّة ممارسة هذا الحقّ.
٤. الإشعار: في حال كانت المعلومات المطلوبة متاحة على موقع الوزارة، أو ليست من اختصاصها، فيجب على المكتب إشعار الفرد بذلك خطيّاً أو الكترونيّاً على أن يتضمّن المعلومات التّالية:
   - نوع الإشعار، على سبيل المثال، البيانات المطلوبة متاحة على موقع الوزارة، أو ليست من اختصاصها.
   - الحقّ في التظلّم على هذا الإشعار وكيفيّة ممارسة هذا الحقّ.

ثالثاً: في حالة رغبة الفرد في التظلّم على رفض الطّلب من قبل الوزارة، فيمكنه تقديم إشعار خطّي أو الكتروني بالتظلّم إلى المكتب خلال فترة زمنيّة لا تتجاوز (١٠) أيام عمل من استلامه قرار الرّفض، ويقوم المكتب (او اللّجنة المشكّلة لهذا الغرض) بمراجعة الطّلب واتخاذ القرار المناسب وإشعار الفرد برسوم المراجعة - يتمّ استرجاعها في حال الموافقة على الطّلب - وقرار الاستئناف.

٧,٥ أحكام عامّة

١. على مكتب إدارة البيانات بالوزارة إعداد وتطبيق السّياسات والإجراءات المتعلّقة بممارسة حقّ الوصول إلى المعلومات العامّة أو الحصول عليها، وتكون المسؤول الاول بالوزارة -او من يفوضه- مسؤولة عن الموافقة عليها واعتمادها.
٢. على المكتب تطوير وتوثيق ومراقبة تنفيذ السّياسات والإجراءات المعتمدة من المسؤول الاول بالوزارة -او من يفوضه- والمتعلّقة بحقّ الوصول إلى المعلومات، على أن تتضمّن مهام ومسؤوليات المكتب وضع المعايير المناسبة لتحديد مستويات تصنيف البيانات في حال عدم وجودها - وفقاً لوثيقة المبادئ الرّئيسيّة والقواعد الاسترشاديّة لتصنيف البيانات - واستخدامها كمرجع رئيس عند معالجة طلبات الاطّلاع على المعلومات العامّة أو الحصول عليها.

٣. على المكتب مواءمة هذه السّياسة مع وثائقها التّنظيميّة - السّياسات والإجراءات - وتعميمها على جميع الجهات التّابعة لها أو المرتبطة بها بما يحقّق التّكامل ويضمن تحقيق الهدف المنشود من إعدادها.

٤. على المكتب موازنة حقّ الاطّلاع والحصول على المعلومات مع المتطلّبات الضّرورية الأخرى كتحقيق الأمن الوطنيّ والمحافظة على خصوصيّة البيانات الشّخصيّة.

٥. على المكتب متابعة وتوثيق الامتثال لهذه السّياسة بشكل دوري وفقاً للآليات والإجراءات التي تحدّدها الوزارة بعد التّنسيق مع مكتب إدارة البيانات الوطنيّة.

٦. على المكتب - بعد التّنسيق مع مكتب إدارة البيانات الوطنيّة - إعداد الآليات والإجراءات والضّوابط المتعلّقة بمعالجة الشّكاوى وفقاً لإطار زمني محدّد وحسب التّسلسل التّنظيمي.

٧. يحق للمكتب إشعار مكتب إدارة البيانات الوطنيّة في حال تمّ رفض طلب الاطّلاع أو الحصول على المعلومات العامّة أو تمديد الفترة المحدّدة لتقديم هذه المعلومات وهي ضمن النّطاق.

٨. يجب على المكتب عند تعاقد الوزارة مع جهات أخرى - كالشّركات التي تقوم بمباشرة خدمات عامّة - أن يتحقّق بشكل دوري من امتثال الجهات الأخرى لهذه السّياسة وفقاً للآليّات والإجراءات التي تحدّدها الوزارة، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها الجهات الأخرى.

٩. يحقّ للوزارة وضع قواعد إضافيّة لمعالجة الطّلبات المتعلّقة بأنواع محدّدة من المعلومات العامّة وفقاً لطبيعتها وحساسيّتها بعد التّنسيق مع مكتب إدارة البيانات الوطنيّة.

١٠. يقوم المكتب بالتّنسيق مع الجهات ذات العلاقة بالوزارة بإعداد نماذج للاطّلاع أو الحصول على المعلومات العامّة - سواء أكانت ورقيّة أو الكترونيّة - يحدّد فيها المعلومات اللّازمة والوسائل الممكنة لتقديم المعلومات المطلوبة.

١١. تحديد وتوفير الوسائل الممكنة (نموذج طلب المعلومات العامّة) - سواءً كانت ورقيّة أو الكترونيّة - والتي من خلالها يمكن للفرد طلب الاطّلاع على المعلومات العامّة أو الحصول عليها.

١٢. التّحقّق من هويّة الأفراد قبل منحهم حقّ الاطّلاع على المعلومات العامّة أو الحصول عليها وفقاً للضّوابط المعتمدة من قبل الهيئة الوطنيّة للأمن السّيبراني والجهات ذات العلاقة.

١٣. وضع المعايير اللّازمة لتحديد الرّسوم المترتّبة على معالجة طلبات الاطّلاع على المعلومات العامّة أو الحصول عليها بناءً على طبيعة البيانات وحجمها والجهد المبذول والوقت المستغرق وفقاً لوثيقة سياسة تحقيق الدّخل من البيانات.

١٤. توثيق جميع سجلات طلبات الوصول إلى المعلومات أو الحصول عليها والقرارات المتّخذة حيال هذه الطّلبات، على أن يتمّ مراجعة هذه السّجلات لمعالجة حالات سوء الاستخدام أو عدم الاستجابة.

١٥. على المكتب إعداد وتوثيق سياسات وإجراءات الإحتفاظ بسجلات الطّلبات والتّخلّص منها وفقاً للأنظمة والتّشريعات ذات العلاقة بأعمال وأنشطة الوزارة.

١٦. على المكتب إعداد وتوثيق الإجراءات اللّازمة لإدارة ومعالجة وتوثيق طلبات التّمديد، والطّلبات المرفوضة وتحديد المهام والمسؤوليات المتعلّقة بفريق العمل المختص، والحالات التي يتمّ بها إشعار الجهة التّنظيميّة اومكتب إدارة البيانات الوطنيّة حسب التسلسل الإداري وفقاً للفترة الزمنيّة المحدّدة لمعالجة الطّلبات.

١٧. إشعار الفرد - بطريقة ملائمة - في حال تمّ رفض الطّلب كليّاً أو جزئيّاً، مع إيضاح أسباب الرّفض والحقّ في التظلّم وكيفيّة ممارسة هذا الحقّ خلال فترة لا تتجاوز (١٥) يوم من اتخاذ القرار.

١٨. على المكتب بالتّعاون مع الجهات ذات العلاقة بإعداد برامج توعوية لتعزيز ثقافة الشّفافيّة ورفع مستوى الوعي وفقاً لسياسات وإجراءات حرّية المعلومات المعتمدة من المسؤول الاول بالوزارة -او من يفوضه-.

١٩. على المكتب مراقبة الامتثال لسياسات وإجراءات حرّية المعلومات بشكل دوري ويتمّ عرضها على المسؤول الاول بالوزارة -او من يفوضه- كما يتمّ تحديد وتوثيق الإجراءات التّصحيحيّة التي سيتمّ اتخاذها في حال عدم الامتثال.

٨ سياسة البيانات المفتوحة

٨,١ نطاق السّياسة

تنطبق أحكام هذه السّياسة على جميع البيانات والمعلومات العامّة - غير المحميّة - التي تنتجها وزارة التّعليم الدّاخليّة والخارجيّة وإدارات ومكاتب التّعليم والمدارس التي تديرها أو تشرف عليها الوزارة مهما كان مصدرها، أو شكلها أو طبيعتها، ويشمل ذلك السّجلات الورقيّة ورسائل البريد الالكتروني والمعلومات المخزّنة على الكمبيوتر أو أشرطة الصّوت أو الفيديو أو الخرائط أو الصّور الفوتوغرافيّة أو المخطوطات أو الوثائق المكتوبة بخطّ اليد، أو أي شكل آخر من أشكال المعلومات المسجّلة.

٨,٢ المبادئ الرّئيسيّة للبيانات المفتوحة

المبدأ الأوّل: الأصل في البيانات الإتاحة

يضمن هذا المبدأ إتاحة بيانات الوزارة للجميع من خلال الإفصاح عنها أو تمكين الوصول إليها أو استخدامها ما لم تقتضِ طبيعتها عدم الإفصاح عنها أو حماية خصوصيتها أو سرّيتها.

المبدأ الثّاني: الصّيغة المفتوحة وإمكانيّة القراءة آلياً

يتمّ إتاحة البيانات وتوفيرها بصيغة مقروءة آليّاً تسمح بمعالجتها بشكل آلي، بحيث يتمّ حفظها بصيغ الملفّات شائعة الاستخدام (مثل: CSV، أو XLS، أو JSON، أو XML).

المبدأ الثّالث: حداثة البيانات

يتمّ نشر أحدث إصدار من مجموعات البيانات (Data Sets) المفتوحة بصفة منتظمة وإتاحتها للجميع حال توافرها. كما يتمّ نشر البيانات المجمّعة من قبل الوزارة في أسرع وقت ممكن بمجرّد جمعها، كلّما أمكن ذلك، وتُعطى الأولويّة للبيانات التي تقلّ فائدتها بمرور الوقت.

المبدأ الرّابع: الشّمولية

يجب أن تكون مجموعات البيانات المفتوحة شاملة وتتضمن أكبر قدر ممكن من التّفاصيل، وأن تعكس البيانات المسجّلة بما لا يتعارض مع سياسة حماية البيانات الشّخصيّة. كما يجب إدراج البيانات الوصفيّة التي توضّح وتشرح البيانات الأوّلية، مع تقديم التّفسيرات أو المعادلات التي توضّح كيفيّة استخلاص البيانات أو احتسابها.

المبدأ الخامس: عدم التّمييز

يجب إتاحة مجموعات البيانات للجميع دون تمييز ودون حاجة للتّسجيل، يكون بإمكان أي شخص الوصول إلى البيانات المفتوحة المنشورة في أي وقت دون الحاجة إلى التّحقّق من الهويّة أو تقديم مسوّغ للوصول إليها.

المبدأ السّادس: بدون مقابل مالي

يجب إتاحة البيانات المفتوحة للجميع مجاناً.

المبدأ السّابع: ترخيص البيانات المفتوحة في المملكة

تخضع البيانات المفتوحة لترخيص يحدّد الأساس النّظامي لاستخدام البيانات المفتوحة وكذلك الشّروط والالتزامات والقيود المفروضة على المستخدم. كما يدلّ استخدام البيانات المفتوحة على قبول شروط التّرخيص.

المبدأ الثّامن: تطوير نموذج الحوكمة وإشراك الجميع

تمكّن البيانات المفتوحة عمليّة الاطّلاع والمشاركة للجميع، وتعزّز شفافية ومساءلة الوزارة ودعم عمليّة صنع القرار وتقديم الخدمات.

المبدأ التّاسع: التّنمية الشّاملة والابتكار

من المفترض أن تلعب الوزارة دوراً فعّالاً في تعزيز إعادة استخدام البيانات المفتوحة وتوفير الموارد والخبرات اللّازمة الدّاعمة، ويجب على الوزارة أن تعمل بتكامل بين الأطراف المعنيّة على تمكين الجيل القادم من المبتكرين في مجال البيانات المفتوحة وإشراك الأفراد والمؤسّسات والجميع بوجه عامّ في إطلاق قدرات البيانات المفتوحة.

٨,٣ تقييم قيمة البيانات العامّة لتحديد مجموعات البيانات المفتوحة

عمليّة تقييم قيمة البيانات (Data Valuation) لتمكين نشر أكبر قدر ممكن من البيانات المفتوحة تمرّ بعدّة مراحل رئيسة، على النّحو التالي:

الخطوة الأولى: تحديد البيانات والمعلومات العامّة

لتقييم قيمة البيانات، يجب على الوزارة أن تقوم بتصنيف البيانات (وفقاً لسياسة تصنيف البيانات) وتحديد جميع مجموعات البيانات التي يمكن تصنيفها على المستوى "عامّ" والتي قد تتكوّن من ملفات أو جداول أو سجلات محدّدة ضمن قاعدة بيانات، وغيرها. بعد ذلك، يجب تحديد الفوائد والتّطبيقات 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 بيانات الوزارة الجيومكانية لخدمة القطاع الصحي. بالإضافة إلى ذلك، يمكن الأخذ بعين الاعتبار مصادر البيانات؛ بيانات تمّ جمعها عن طريق المستخدمين بشكل مباشر، بيانات تمّ جمعها آلياً عن طريق سجلات الأحداث مثل التّعاملات الالكترونيّة، بيانات مجمّعة أو بيانات تمّ تطويرها من بيانات أخرى ... إلخ.

الخطوة الثّانية: تقييم الفائدة من البيانات

بعد تحديد مجموعات البيانات في الخطوة السّابقة، يتمّ دراسة العوامل الرّئيسة المتعلّقة بفائدة البيانات (Usefulness) والتي تلعب دوراً رئيسيّاً في تقييم قيمتها، ومنها اكتمال البيانات، دقّتها، تناسقها، حداثتها، القيود المفروضة عليها، حصريّتها للوزارة، المخاطر المحتملة من نشرها، إمكانيّة الوصول إليها ودمجها مع بيانات أخرى.

الخطوة الثّالثة: تحديد ذوي المصلحة المحتملين

بعد تقييم الفائدة من البيانات في الخطوة السابقة، يتمّ تحديد جميع الجهات أو الأشخاص ذوي المصلحة المحتملين في سلسلة القيمة بأكملها (Value Chain)، وبذلك يمكن للوزارة معرفة الدّوافع الرّئيسة لذوي المصلحة، ومنها تحقيق الإيرادات من خلال تطوير منتجات البيانات أو تطوير الخدمات للصّالح العامّ كالتي تساهم في تحسين جودة الحياة. بعد الإنتهاء من تقييم قيمة البيانات، يمكن البدء بمراحل دورة حياة البيانات المفتوحة، حسب ما هو موضح أدناه.

٨,٤ القواعد العامّة للبيانات المفتوحة

تحدّد سياسة البيانات المفتوحة القواعد العامّة والالتزامات التي يجب على الوزارة الامتثال لها خلال مراحل دورة حياة البيانات المفتوحة، وتشمل:

١. التّخطيط للبيانات المفتوحة.
٢. تحديد البيانات المفتوحة.
٣. نشر البيانات المفتوحة.
٤. تحديث البيانات المفتوحة.
٥. متابعة أداء البيانات المفتوحة.

٨,٤,١ التّخطيط للبيانات المفتوحة

١. تعيين مسؤول البيانات المفتوحة والمعلومات في المكتب وتتمثّل مسؤوليّته الأساسيّة في دعم التّخطيط والتّنفيذ وإعداد التّقارير بشأن أجندة البيانات المفتوحة لدى الوزارة وبما يتماشى مع هذه السّياسة.
٢. وضع خطّة للبيانات المفتوحة، تتضمّن ما يلي:
   - الأهداف الاستراتيجيّة للبيانات المفتوحة على مستوى الوزارة.
   - تحديد مجموعات البيانات الخاصّة بالوزارة المطلوب نشرها على المنصّة الوطنيّة للبيانات المفتوحة وترتيب تلك المجموعات بحسب الأولويّة.
   - مؤشّرات الأداء الرّئيسيّة والأهداف المتعلّقة بالبيانات المفتوحة بالنّسبة للوزارة.
   - منهجيّة ومعايير تحديد الأولويّة.
   - احتياجات التّدريب ذات الصّلة بالبيانات المفتوحة.
   - الجداول الزمنيّة لنشر وتحديث البيانات المفتوحة.
٣. تطوير وتوثيق العمليّات المطلوبة في جميع مراحل دورة حياة البيانات المفتوحة، ويشمل ذلك، على سبيل المثال لا الحصر، ما يلي:
   - عمليّات تحديد مجموعات البيانات العامّة التي سيتمّ نشرها من جانب الوزارة.
   - عمليّات التّحقّق من التزام البيانات المفتوحة بالمتطلّبات المتعلّقة بأمن المعلومات وخصوصيّة البيانات الشّخصيّة وجودة البيانات ومراجعة ذلك بشكل منتظم والتّعامل مع المخاوف المتعلّقة بذلك.

- عمليّات ضمان نشر مجموعات البيانات وتحديثها بالصّيغة المناسبة ووفق الجدول الزمني المحدّد وضمان شموليتها وجودتها العالية وضمان استبعاد أي بيانات مقيّدة.
- عمليّات جمع الملاحظات وتحليل الأداء على مستوى الوزارة وتحسين التأثير العامّ للبيانات المفتوحة على الصعيد الوطني.

٤. ضمان مراجعة خطّة البيانات المفتوحة وتحديثها بصفة دوريّة.
٥. تقديم تقرير سنوي لمكتب إدارة البيانات الوطنيّة حول خطّة البيانات المفتوحة ومستوى التّقدم في تحقيق أهداف البيانات المفتوحة المحدّدة في الخطّة.
٦. تنظيم دورة تدريبيّة عن جميع ما يتعلّق بالبيانات المفتوحة بدعم من مكتب إدارة البيانات الوطنيّة أو بالتّنسيق معه.
٧. إطلاق حملات توعية لضمان معرفة المستخدمين المحتملين بتوافر البيانات المفتوحة المنشورة من جانب الوزارة وطبيعتها وجودتها.

٨,٤,٢ تحديد البيانات المفتوحة

١. تحديد جميع البيانات المصنّفة على أنّها بيانات عامّة بصفة منتظمة وتقييم مدى أولويّة كل مجموعة من مجموعات البيانات المحدّدة لنشرها كبيانات مفتوحة.
٢. تقدير قيمة مجموعة البيانات وتحديد مدى أولويّة نشرها بمجرد استلام طلب النّشر أو حينما يُلغى تصنيف أي مجموعة بيانات باعتبارها مقيّدة وتصنيفها كمجموعة بيانات عامّة.
٣. تسجيل البيانات الوصفيّة (Metadata) لمجموعات البيانات المفتوحة المحدّدة ونشرها.
٤. دراسة ما إذا كان الجمع بين عدّة مجموعات من البيانات المفتوحة سيؤدّي إلى رفع مستوى تصنيف البيانات إلى بيانات محميّة وفقاً لما يصدر من مكتب إدارة البيانات الوطنيّة من أدلّة إرشاديّة في هذا الخصوص.

٨,٤,٣ نشر البيانات المفتوحة

١. نشر مجموعات البيانات المفتوحة الخاصّة بها على المنصّة الوطنيّة للبيانات المفتوحة.
٢. التأكّد من نشر البيانات بصيغ معياريّة موحّدة وهيكلة مقروءة آلياً وغير مسجّلة الملكيّة، تشمل على سبيل المثال لا الحصر (CSV)، و(JSON)، و(XML)، و(RDF) ويجب أن تكون ملفّات مجموعات البيانات مصحوبة بالوثائق ذات الصّلة بالصّيغة والتّعليمات المتعلّقة بكيفيّة استخدامها.
٣. توفير البيانات بعدّة صيغ كلما أمكن.

٨,٤,٤ تحديث البيانات المفتوحة

١. ضمان تحديث جميع مجموعات البيانات المفتوحة المنشورة بصفة منتظمة بحسب الآليّة المحدّدة في البيانات الوصفيّة.
٢. المراجعة المستمرّة لمجموعات البيانات المنشورة لضمان استيفائها للمتطلّبات التّنظيميّة المحدّدة.
٣. ضمان تحديث البيانات الوصفيّة وخاصّة تحديثها كلّما تغيّرت عناصر البيانات في مجموعات البيانات المفتوحة المنشورة.
٤. الحفاظ على إمكانيّة تتبّع البيانات من خلال توثيق مصادر البيانات والحفاظ على سجل إصدارات مجموعة البيانات.
٥. نشر مجموعات البيانات المفتوحة مع تحديد القيود المتعلّقة بالجودة وتوثيقها في البيانات الوصفيّة.

٨,٤,٥ متابعة أداء البيانات المفتوحة

١. تحليل حجم الطّلب على البيانات المفتوحة ومعدّل استخدامها لفهم حجم الطّلب العامّ وإعادة ترتيب مجموعات البيانات بحسب الأولويّة وفقاً لذلك.
٢. جمع طلبات المستخدمين المقدّمة بصورة مباشرة أو من خلال المنصّة الوطنيّة للبيانات المفتوحة لنشر مجموعات بيانات إضافيّة وتحليل تلك الطّلبات والردّ عليها في حينها.

٨,٥ الأدوار والمسؤوليّات

تحدّد سياسة البيانات المفتوحة الأدوار والمسؤوليّات التّالية على مستوى الوزارة مع الأخذ في الإعتبار أدوار ومسؤوليات مكتب إدارة البيانات الوطنيّة - التي نصّت عليها سياسات حوكمة البيانات الوطنيّة - بصفتة الجهة المسؤولة عن الإشراف على مبادرات البيانات المفتوحة في المملكة. حيث تتمثل المسؤوليّة الأساسيّة للوزارة في ضمان نشر بياناتها المفتوحة وفقاً لسياسة البيانات المفتوحة. وبالتالي، يجب على الوزارة تعيين من يتولون مسؤوليّة تنفيذ الأنشطة المتعلّقة بالبيانات المفتوحة على النّحو المنصوص عليه أدناه.
يتحمل مكتب إدارة البيانات بالوزارة المسؤوليّة الأساسيّة المتعلّقة بأنشطة البيانات المفتوحة لدى الوزارة.

- **المسؤول الأوّل بالوزارة (او من يفوضه):** يعد المسؤول الأوّل بالوزارة - أو من يفوّضه - هو الشخص المسؤول عن الممارسات المتعلّقة بالبيانات المفتوحة داخل الوزارة، وتشمل مسؤولياته:

١. **اعتماد خطّة البيانات المفتوحة:** الموافقة على تنفيذ خطّة البيانات المفتوحة لدى الوزارة والإشراف عليها.
٢. **تخصيص الأدوار المتعلّقة بالبيانات المفتوحة:** تخصيص الأدوار المختلفة المتعلّقة بالبيانات المفتوحة.
٣. **اعتماد التّقرير السنوي للبيانات المفتوحة:** اعتماد التّقرير السنوي للبيانات المفتوحة الذي يُعدّه مدير المكتب.

- **مدير مكتب البيانات بالوزارة:** يعتبر المدير الاستراتيجي للعمليّات المتعلّقة بالبيانات المفتوحة في الوزارة، وتتضمّن مسؤولياته ما يلي:

١. **التّخطيط الاستراتيجي للبيانات المفتوحة:** الإشراف على وضع خطّة البيانات المفتوحة وتقديمها إلى المسؤول الأوّل بالوزارة (أو من يفوّضه). كما يتولى مراجعة أداء البيانات المفتوحة وتحديد فرص التّحسين والاسترشاد بذلك في خطّة البيانات المفتوحة.
٢. **الإشراف على البيانات المفتوحة:** مراجعة أنشطة تحديد البيانات المفتوحة وترتيبها بحسب الأولويّة والموافقة على نشرها وضمان تنفيذ أنشطة تحديثها.
٣. **الامتثال لسياسة البيانات المفتوحة:** ضمان امتثال أنشطة البيانات المفتوحة لدى الوزارة للسّياسات الوطنيّة المتعلّقة بالبيانات، ويشمل ذلك على سبيل المثال لا الحصر، تصنيف البيانات وحماية خصوصيّة البيانات الشّخصيّة وحرّية المعلومات.
٤. **التّنسيق مع مكتب إدارة البيانات الوطنيّة:** يُعدّ مدير المكتب المنسّق الأوّل بين الوزارة ومكتب إدارة البيانات الوطنيّة فيما يتعلّق بالبيانات المفتوحة. ويتولى حلّ المشاكل المتعلّقة بالبيانات المفتوحة بالنّسبة للوزارة وتصعيدها إلى مكتب إدارة البيانات الوطنيّة إذا لزم الأمر.

- **مسؤول البيانات المفتوحة والمعلومات:** هو المدير التشغيلي للبيانات المفتوحة داخل الوزارة .وتشمل مسؤولياته:

١. **التّخطيط للبيانات المفتوحة:** وضع خطّة البيانات المفتوحة، بما في ذلك منهجيّة تحديد البيانات المفتوحة ذات الأولويّة ووضع الأهداف ومؤشّرات الأداء الرّئيسيّة التي يعتمدها المكتب بناء على إعتماد المسؤول الأوّل بالوزارة (أو من يفوّضه).
٢. **إدارة البيانات المفتوحة:** إدارة أنشطة البيانات المفتوحة داخل الوزارة، وعلى وجه التّحديد:
   - تحديد البيانات المفتوحة.
   - ترتيب مجموعات البيانات بحسب أولويّة النّشر.
   - إعداد مجموعات البيانات للنّشر وتوثيق البيانات الوصفيّة.
   - نشر مجموعات البيانات المفتوحة على المنصّة الوطنيّة للبيانات المفتوحة.
   - تحديث مجموعات البيانات المنشورة وصيانتها ومراجعة جودتها.
٣. **جمع طلبات البيانات المفتوحة:** مراجعة الملاحظات على البيانات المفتوحة ذات الصّلة بالوزارة وتسجيل وتحليل طلبات نشر البيانات المحدّدة كبيانات مفتوحة.
٤. **التّثقيف والتّوعية بالبيانات المفتوحة:** تثقيف موظفي الوزارة وتوعيتهم بشأن البيانات المفتوحة ودعم حملات التّوعية الوطنيّة بالتّنسيق مع مدير المكتب.
٥. **التّنسيق مع مكتب إدارة البيانات الوطنيّة (بشكل ثانوي):** يقوم مسؤول البيانات المفتوحة والمعلومات بالتّنسيق مع إدارة البيانات الوطنيّة عند الحاجة كمستوى ثانٍ.

- **ممثّل بيانات أعمال:** يتولى المسؤوليات التّالية:

١. **التّصديق على خطّة البيانات المفتوحة:** المساهمة في تطوير خطّة البيانات المفتوحة وإدارة الفرق المسؤولة عن تنفيذ الخطّة بالتّنسيق مع مسؤول البيانات المفتوحة والمعلومات.
٢. **تحديد أولويّة البيانات المفتوحة:** تقديم المشورة إلى مسؤول البيانات المفتوحة والمعلومات بشأن قيمة مجموعات البيانات العامّة والاستثمارات المطلوبة لنشرها وتحديثها.
٣. **مراجعة مجموعات البيانات واعتمادها:** مراجعة مجموعات البيانات واعتمادها للتّأكّد من استيفائها للمواصفات المحدّدة في اللائحة من حيث الجودة والكمال وتوثيق البيانات الوصفيّة قبل تقديمها للنشر.

- **مختصّ بيانات الأعمال:** يعدّ أحد أفراد فريق ممثّلي بيانات الأعمال المسؤول عن:

١. **تحديد مجموعات البيانات المفتوحة:** يتولى مختصّ بيانات الأعمال مراجعة وتحديد البيانات التي يتمّ إنشاؤها ومعالجتها من قبل الإدارة التي يعمل فيها بصفة منتظمة وتصنيفها بصفتها بيانات عامّة إذا لزم الأمر.
٢. **إعداد مجموعات البيانات المفتوحة:** إعداد مجموعات البيانات المفتوحة التي سيتمّ نشرها لضمان استيفائها للمواصفات المحدّدة في السّياسة من حيث الجودة والكمال وتوثيق البيانات الوصفيّة قبل تقديمها للنّشر.
٣. **تحديث مجموعات البيانات المفتوحة:** تحديث مجموعات البيانات المفتوحة المنشورة والبيانات الوصفيّة ذات الصّلة.

٨,٦ الإمتثال

يقوم مكتب إدارة البيانات الوطنيّة - بصفته الجهة التّنظيميّة للبيانات الوطنيّة - بمراقبة الامتثال لسياسة البيانات المفتوحة بدعم من الوزارة.

٨,٦,١ شروط الامتثال

١. على الوزارة الالتزام بسياسة البيانات المفتوحة وتقديم تقرير سنوي إلى مكتب إدارة البيانات الوطنيّة يشمل، على سبيل المثال لا الحصر، ما يلي:
   - التّقدم ومستوى الإنجاز الذي حقّقته الوزارة في خطّتها المحدّدة.
   - الأهداف ومؤشّرات الأداء الرّئيسيّة المحدّدة في خطّة البيانات المفتوحة.
   - عدد مجموعات البيانات المفتوحة المحدّدة.
   - عدد مجموعات البيانات المفتوحة المنشورة.
٢. تقوم الوزارة - بعد التّنسيق مع مكتب إدارة البيانات الوطنيّة - بإعداد الآليات والإجراءات والضّوابط المتعلّقة بتسوية النّزاعات المتعلّقة بالبيانات المفتوحة وفقاً لإطار زمني محدّد وحسب التّسلسل التّنظيمي.
٣. يقوم مكتب إدارة البيانات الوطنيّة بمراجعة التّقارير السّنوية التي تمّ إعدادها من قبل الوزارة حول الامتثال العامّ بسياسة البيانات المفتوحة ومشاركتها مع الوزارة.
٤. يقوم مكتب إدارة البيانات الوطنيّة بإجراء عمليّات التّدقيق بشكل دوري أو عشوائي للتّحقّق من امتثال الوزارة ومراجعة القرارت المتعلّقة بنشر البيانات أو رفض نشرها واتخاذ مايلزم من إجراءات بهذا الخصوص.

٩ سياسة حماية البيانات الشّخصيّة للأطفال ومن في حكمهم

٩,١ نطاق السّياسة

تنطبق أحكام هذه السّياسة على جميع إدارات وزارة التّعليم الدّاخليّة والخارجيّة وإدارات ومكاتب التّعليم والمدارس التي تديرها أو تشرف عليها الوزارة، التي تقوم بجمع ومعالجة البيانات الشّخصيّة للأطفال ومن في حكمهم بشكل كلّي أو جزئي وبأي وسيلة سواء أكانت يدويّة أو الكترونيّة.

٩,٢ حقوق الطفل ومن في حكمه فيما يتعلّق بمعالجة بياناته الشّخصيّة

١. يتمتّع الطّفل ومن في حكمه بجميع حقوق صاحب البيانات المنصوص عليها في سياسة الوزارة المعتمدة لحماية البيانات الشّخصيّة، ويتمّ ممارسة هذه الحقوق من قبل الوليّ.

٢. يحقّ للطّفل ومن في حكمه طلب إتلاف بياناته الشّخصيّة بعد بلوغه السّن النّظاميّة أو انتهاء الولاية في حال كانت الموافقة على جمع ومعالجة بياناته الشّخصيّة مقدّمه من قبل الوليّ.

٩,٣ القواعد العامّة

دون إخلال بالقواعد العامّة المنصوص عليها في سياسة حماية البيانات الشّخصيّة، تلتزم الوزارة بالقواعد الإضافيّة التّالية التي تضمن المحافظة على خصوصيّة الأطفال ومن في حكمهم وحماية حقوقهم:

١. أن يكون مكتب إدارة البيانات بالوزارة مسؤولاً عن إعداد وتطبيق السّياسات والإجراءات المتعلّقة بحماية البيانات الشّخصيّة للأطفال ومن في حكمهم، ويكون المسؤول الأوّل بالوزارة - أو من يفوّضه - مسؤولاً عن الموافقة عليها واعتمادها.

٢. يقوم المكتب بتقييم الآثار السّلبية والمخاطر المحتملة المترتّبة على جميع أنشطة معالجة البيانات الشّخصيّة للأطفال ومن في حكمهم، مع الأخذ بعين الاعتبار مصالحهم وحقوقهم وجميع ما يتعلّق بأحوال أسرهم، وعرض نتائج التّقييم على المسؤول الأوّل بالوزارة - أو من يفوّضه - لتحديد مستوى قبول المخاطر وإقرارها.

٣. يقوم المكتب بمراجعة وتحديث العقود واتّفاقيات مستوى الخدمة والتّشغيل بما يتوافق مع السّياسات والإجراءات المتعلّقة بحماية البيانات الشّخصيّة للأطفال ومن في حكمهم المعتمدة من المسؤول الأوّل بالوزارة - أو من يفوّضه -.

٤. يقوم المكتب بإعداد وتوثيق الإجراءات اللّازمة لإدارة ومعالجة انتهاكات الخصوصيّة المتعلّقة بالأطفال ومن في حكمهم وتحديد المهام والمسؤوليّات المتعلّقة بفريق العمل المختصّ، والحالات التي يتمّ بها إشعار مكتب إدارة البيانات الوطنيّة حسب التّسلسل الإداري بناءً على قياس شدّة الأثر.

٥. يقوم المكتب بالتّنسيق مع الجهات المعنيّة داخل الوزارة بإعداد برامج توعوية لتعزيز ثقافة الخصوصيّة ورفع مستوى الوعي فيما يتعلّق بجمع ومعالجة البيانات الشّخصيّة للأطفال ومن في حكمهم.

٦. يقوم المكتب بإعداد وتطوير إشعار الخصوصيّة بشكل واضح ودقيق وبلغة تناسب هذه الفئة والتّنسيق مع الجهات المعنيّة داخل الوزارة لنشره على الموقع الالكتروني أو التّطبيق الخاص (حسب الدّليل الإرشادي لتطوير إشعار الخصوصيّة الصّادر من المكتب) وإشعار الوليّ -بطريقة تناسب وقت جمع البيانات - بالغرض والأساس النّظامي أو الاحتياج الفعلي والوسائل والطّرق المستخدمة لجمع ومعالجة ومشاركة البيانات الشّخصيّة للأطفال ومن في حكمهم وكذلك كيفيّة ممارسة الحقوق، والتّدابير الأمنيّة لحماية خصوصيّتهم، وأي تغييرات جوهريّة تطرأ عليه.

٧. تلتزم الوزارة بإشعار الوليّ عن المصادر الأخرى التي يتمّ استخدامها في حال تمّ جمع بيانات إضافيّة بطريقة غير مباشرة (من جهات أخرى).

٨. تلتزم الوزارة بتزويد الوليّ بالخيارات المتاحة فيما يتعلّق بمعالجة البيانات الشّخصيّة للأطفال ومن في حكمهم والآلية المستخدمة لممارسة هذه الخيارات، ومنها على سبيل المثال، التّفضيلات الشّخصيّة التي من خلالها يمكن التّعبير عن الرّغبة في مدى مشاركة بياناتهم لأغراض أخرى.

٩. تلتزم الوزارة بتبنّي مفهوم الخصوصيّة بالتّصميم وبشكل افتراضي - يضمن مستوى الحماية دون تدخل مباشر من الطّفل أو من في حكمه - عند تقديم الخدمات التي تستهدف هذه الفئة على وجه التّحديد.

١٠. تلتزم الوزارة بأخذ موافقة الوليّ - التي يمكن التّحقّق منها بعد بذل الجهود المعقولة - على معالجة البيانات الشّخصيّة للأطفال ومن في حكمهم بعد تحديد نوع الموافقة (صريحة أو ضمنيّة) بناءً على طبيعة البيانات وطرق جمعها.

١١. أن يكون الغرض من جمع البيانات الشّخصيّة للأطفال ومن في حكمهم متوافقاً مع الأنظمة ذات الصّلة وذو علاقة مباشرة بنشاط الوزارة.
١٢. أن يكون محتوى البيانات مقتصراً على الحدّ الأدنى من البيانات اللّازمة لتحقيق الغرض من جمعها.
١٣. أن يتمّ تقييد جمع البيانات الشّخصيّة للأطفال ومن في حكمهم على المحتوى المعدّ سلفاً (الموضح في القاعدة ١٢) ويكون بطريقة عادلة (مباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التّضليل).
١٤. أن يقتصر استخدام البيانات على الغرض التي جُمعت من أجله والذي تمّت الموافقة عليه من قبل الوليّ.
١٥. يقوم المكتب بإعداد وتوثيق سياسة وإجراءات الإحتفاظ بالبيانات الشّخصيّة للأطفال ومن في حكمهم وفقاً للأغراض المحدّدة والأنظمة والتّشريعات ذات العلاقة.
١٦. تلتزم الوزارة بتخزين البيانات الشّخصيّة للأطفال ومن في حكمهم ومعالجتها داخل الحدود الجغرافيّة للمملكة لضمان المحافظة على السّيادة الوطنيّة على هذه البيانات، ولا يجوز معالجتها خارج المملكة إلا بعد التّنسيق مع مكتب إدارة البيانات الوطنيّة متى ما استدعى الأمر ذلك.
١٧. تلتزم الوزارة بإعداد وتوثيق سياسة وإجراءات التّخلّص من البيانات لإتلاف البيانات بطريقة آمنة تمنع فقدانها أو إساءة استخدامها أو الوصول غير المصرّح به - وتشمل البيانات التشغيليّة، المؤرشفة، والنّسخ الاحتياطيّة - وذلك وفقاً لما يصدر من الهيئة الوطنيّة للأمن السّيبراني.
١٨. تلتزم الوزارة بتضمين أحكام سياستي الإحتفاظ والتّخلّص من البيانات في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.
١٩. تلتزم الوزارة بتحديد وتوفير الوسائل التي من خلالها يمكن للوليّ الوصول إلى البيانات الشّخصيّة للطّفل ومن في حكمه وذلك لمراجعتها وتحديثها.
٢٠. تلتزم الوزارة بالتّحقّق من هويّة الوليّ قبل منحه الوصول إلى بيانات الطّفل الشّخصيّة ومن في حكمه وفقاً للضّوابط المعتمدة من قبل الهيئة الوطنيّة للأمن السّيبراني والجهات ذات الاختصاص.
٢١. يحظر مشاركة البيانات الشّخصيّة للأطفال ومن في حكمهم مع جهات أخرى إلا وفقاً للأغراض المحدّدة بعد موافقة الوليّ ووفقاً للأنظمة واللّوائح والسّياسات ذات الصّلة على أن يتمّ تزويد الجهات الأخرى بالسّياسات والإجراءات المتعلّقة بحماية البيانات الشّخصيّة للأطفال ومن في حكمهم وتضمينها في العقود والاتّفاقيات.
٢٢. تلتزم الوزارة بإشعار الوليّ وأخذ الموافقة منه في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الأغراض المحدّدة.
٢٣. تلتزم الوزارة بإشعار الوليّ في حال الرغبة في التّواصل مع الطّفل أو من في حكمه بطريقة مباشرة لأي غرض كان وإتاحة الفرصة له لرفض هذا التّواصل مع إيضاح كيفيّة قيامه بذلك.
٢٤. تلتزم الوزارة بأخذ موافقة مكتب إدارة البيانات الوطنيّة قبل مشاركة البيانات الشّخصيّة للأطفال ومن في حكمهم مع جهات أخرى خارج المملكة.
٢٥. يحظر على الوزارة جمع بيانات شخصيّة من الطّفل أو من في حكمه تتعلّق بأحد أفراد أسرته في أي حال من الأحوال، ماعدا البيانات الشّخصيّة للولي.
٢٦. تلتزم الوزارة بمتطلّبات حماية خصوصيّة الأطفال ومن في حكمهم منذ المراحل الأولى من تصميم الخدمات والمنتجات التي تستهدف هذه الفئة، بما في ذلك المواقع الالكترونيّة أو التّطبيقات الرقميّة.
٢٧. تلتزم الوزارة بتطبيق التّدابير المناسبة التي تمنع الأطفال ومن في حكمهم من إتاحة بياناتهم الشّخصيّة والحسّاسة للجمهور بطريقة يمكن من خلالها التّعرف عليهم وعلى أسرهم بشكل مباشر.
٢٨. تلتزم الوزارة بتطبيق التّدابير المناسبة والممكنة عملياً في حدود المعقول لحذف البيانات الشّخصيّة والحسّاسة من منشورات الطّفل ومن في حكمه قبل نشرها، بما في ذلك عرض الملفّات الشّخصيّة والنّشر عبر حسابات التّواصل الاجتماعي.
٢٩. تلتزم الوزارة بعدم اتخاذ قرارات آلية بناءً على معالجة البيانات الشّخصيّة للأطفال ومن في حكمه واستخدامها لأغراض متعدّدة لها تأثير كبير عليهم، ومنها على سبيل المثال التّسويق المباشر.
٣٠. تلتزم الوزارة باستخدام الضّوابط الإداريّة والتّدابير التّقنيّة والضّمانات القانونيّة الكافية لحماية البيانات الشّخصيّة للأطفال ومن في حكمهم.

٣١. يقوم المكتب بمراقبة الامتثال للسّياسات والإجراءات المتعلّقة بحماية البيانات الشّخصيّة للأطفال ومن في حكمهم بشكل دوريّ ويتمّ عرضها على المسؤول الأوّل بالوزارة - أو من يفوّضه - كما يتمّ تحديد وتوثيق الإجراءات التّصحيحيّة التي سيتمّ اتخاذها في حال عدم الامتثال وإشعار مكتب إدارة البيانات الوطنيّة حسب التّسلسل التّنظيمي.

٣٢. يقوم المكتب عند تعاقد الوزارة مع جهات معالجة أخرى بالتّحقّق بشكل دوري من امتثال الجهات الأخرى لهذه السّياسة وفقاً للآليات والإجراءات التي تحدّدها الوزارة، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها الوزارة.

٩,٤ الإستثناءات

١. لا يشترط الحصول على موافقة الوليّ في حال كانت الخدمة المقدّمة للطّفل أو من في حكمه هي خدمة وقائيّة أو استشاريّة وفقاً لمهام واختصاصات الوزارة (الجهات ذات العلاقة بحماية الطّفل)، على أن تلتزم الوزارة بجمع الحدّ الأدنى من البيانات اللّازمة لتحقيق الغرض، وإتلافها فور الانتهاء من تقديم الخدمة.

٢. لا يشترط الحصول على موافقة الوليّ في حال الإفصاح عن بياناته الشّخصيّة لطرف ثالث من أجل تنفيذ التزام مشروع على الوزارة أو لتنفيذ نظام آخر أو لتنفيذ اتّفاقيّة تكون المملكة طرفاً فيه أو كانت الجهة التي سيتمّ الإفصاح لها جهة قضائيّة أو أمنيّة.

٣. لا يشترط الحصول على موافقة الوليّ عندما يكون الغرض الوحيد من جمع بيانات الاتصال بالطّفل أو من في حكمه هو الردّ مباشرة على طلب محدّد من الطّفل ومن في حكمه، ولا تستخدم هذه البيانات بمعاودة الاتصال به مرّة أخرى أو لأي غرض آخر، ولا يتمّ الإفصاح عنها، وتقوم الوزارة بحذفها من سجلّاتها فور الاستجابة لطلب الطّفل.

٤. لا يشترط الحصول على موافقة الوليّ عندما يكون الغرض من جمع بيانات الاتصال للولي والطّفل ومن في حكمه هو الاستجابة مباشرة - مرّة أو أكثر - لطلب الطّفل ومن في حكمه المحدّد، ولا يتمّ استخدام هذه البيانات لأي غرض آخر، ولا يتمّ الإفصاح عنها، أو دمجها مع أي بيانات أخرى، ويتمّ تزويد الوليّ بإشعار بذلك.

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

٩,٥ الأحكام الخاصّة المتعلّقة بالوليّ الشرعي

١. يجوز للوزارة أن تحصل على البيانات الشّخصيّة للوليّ من الطّفل ومن في حكمه مباشرة، على أن تلتزم بالحصول على الحدّ الأدنى من البيانات اللّازمة - الاسم وطريقة التّواصل مع الوليّ - فقط من أجل إشعار الوليّ والحصول على موافقته.

٢. تلتزم الوزارة باستخدام الوسائل المناسبة للتحقّق من هويّة الوليّ قبل أخذ موافقته ومنحه الوصول إلى بيانات الطّفل الشّخصيّة ومن في حكمه وفقاً للضوابط المعتمدة من قبل الهيئة الوطنيّة للأمن السّيبراني والجهات ذات الاختصاص.

٣. في حال تم طلب موافقة الوليّ ولم يقدم موافقته خلال (١٠) أيام من تاريخ التواصل معه، تلتزم الوزارة بإتلاف بيانات الطّفل الشّخصيّة ومن في حكمه وبيانات الوليّ التي جُمعت.

٤. تلتزم الوزارة بعدم استخدام البيانات الشّخصيّة للولي لغير الغرض الذي جُمعت من أجله في حدود الموافقة على جمع ومعالجة البيانات الشّخصيّة للطّفل ومن في حكمه.

٥. تلتزم الوزارة بإشعار الوليّ بالطّلبات المقدّمة من الطّفل ومن في حكمه فيما يتعلّق بالبيانات الشّخصيّة له وأخذ موافقته عليها.

١٠ القواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة

١٠,١ نطاق السّياسة

تنطبق أحكام هذه الوثيقة على جميع إدارات الوزارة الدّاخليّة والخارجيّة وإدارات ومكاتب التّعليم والمدارس التي تديرها أو تشرف عليها الوزارة، والتي تقوم بنقل البيانات الشخصية إلى جهات أخرى خارج الحدود الجغرافية للمملكة بغرض معالجتها، ويستثنى من ذلك نقل البيانات الشخصية من وإلى الأفراد مباشرة.

١٠,٢ 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 الوزارة 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 الوزارة، وذلك للاطلاع عليها، وطلب تصحيحها، أو إتمامها، أو تحديثها، وطلب إتلاف ما انتهت الحاجة إليه منها، والحصول على نسخة منها بصيغة واضحة.

١٠,٣ التزامات الوزارة

الأصل في المعالجة أن تكون داخل الحدود الجغرافية للمملكة، حيث تقوم الوزارة 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:

١. إذا كانت جهة المعالجة الخارجية المسند إليها أنشطة معالجة البيانات الشخصية في دولة ضمن قائمة الاعتماد، فتقوم جهة المعالجة الداخلية بأخذ موافقة كتابية من المسؤول الأول بالوزارة على نقل البيانات، وعلى مكتب إدارة البيانات بالوارة التنسيق مع مكتب إدارة البيانات الوطنية.

٢. 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 مكتب إدارة البيانات الوطنية – بعد إجراء تقييم مستوى الحماية التي توفرها جهة المعالجة الخارجية.

٣. 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.

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

في جميع الحالات الواردة في الفقرات (٢) و (٣) و(٤) أعلاه، يجب على المعالجة الداخلية داخل الوزارة الحصول على موافقة كتابية من من المسؤول الأول بالوزارة على نقل البيانات، وعلى مكتب إدارة البيانات بالوزارة التنسيق مع مكتب إدارة البيانات الوطنية.

أولاً: تقييم مستوى الحماية

يجب أن تقوم الوزارة عند رغبتها بنقل البيانات خارج الحدود الوطنية بإجراء تقييم الآثار والمخاطر المحتملة – كل حالة على حدة – لتحديد ما إذا كانت جهة المعالجة الخارجية ستوفر مستوى كافٍ من الحماية لحقوق أصحاب البيانات وعرض نتائج التقييم على المسؤول الأوّل بالوزارة لتحديد مستوى قبول المخاطر وإقرارها. وللقيام بذلك يجب أن تقوم الوزارة 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 الوزارة عند تقييم مستوى الحماية أن تأخذ بعين الاعتبار نوع وقيمة وحجم البيانات المراد نقلها ودرجة حساسيتها، حيث إن نقل البيانات الشخصية الحساسةيتطلب مستوى عالٍ من الحماية.
- الغرض من معالجة البيانات: يجب على الوزارة 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 الوزارة 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 الوزارة 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 الوزارة 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 الوزارة 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 الوزارة عند نقل البيانات خارج الحدود الوطنية مراعاة 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 الوزارة 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 الوزارة 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 الوزارة 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 الوزارة أن تضمّن في العقود والاتفاقيات بنوداً نموذجية أو قياسية – يتم الموافقة عليها من قبل مكتب إدارة البيانات الوطنية – لتقييد نقل البيانات الشخصية خارج الحدود الجغرافية للمملكة بما يضمن المحافظة على خصوصية أصحابها وحماية حقوقهم.

- القواعد المشتركة الملزمة: يجب على جهة المعالجة داخل الوزارة 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 مكتب إدارة البيانات الوطنية، ويتم تضمين هذه القواعد المشتركة بصفتها ملحقاً لاتفاقيات مستوى الخدمة أو العقود المبرمة بين الجهتين. كما يجب على جهة المعالجة أخذ موافقة المسؤول الأول بالوزارة 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 الوزارة باستخدام قواعد السلوك المعتمدة من المسؤول الأول بالوزارة أو مكتب إدارة البيانات الوطنية بصفتها أداة فعّالة تحدّد الالتزامات على جهات المعالجة لضمان المحافظة على خصوصية أصحاب البيانات وحماية حقوقهم.
- الشهادات المعتمدة: أن تقوم الوزارة بالاستعانة بأطراف خارجية مستقلة تتولى إصدار شهادات اعتماد تؤكد وجود الضمانات المناسبة التي توفرها جهات التحكم أو جهات المعالجة الخارجية. كما تقوم الوزارة بتقديم التزامات قابلة للتنفيذ لتطبيق هذه الضمانات بما في ذلك الأحكام المتعلقة بحقوق أصحاب البيانات.
- الاتفاقيات الملزمة بين الجهات العامة: أن تقوم الوزارة بتوقيع اتفاقية ملزمة قانونياً لنقل البيانات الشخصية على أن تتضمن هذهالاتفاقية بنوداً تعاقدية ملزمة تضمن المحافظة على خصوصية أصحاب البيانات وتحمي حقوقهم.

ثالثاً: الاستثناءات لحالات محددة

يمكن للوزارة 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:

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

في جميع هذه الحالات الواردة في الفقرات (١)، (٢)، (٣)، (٤)، (٥)، يجب على جهة التحكم أو المعالجة الداخلية الحصول على موافقة كتابية من المسؤول الأول بالوزارة على نقل البيانات – كل حالة على حدة – وعلى مكتب إدارة البيانات بالوزارة التنسيق مع مكتب إدارة البيانات الوطنية. أما ما يتعلق بالحالة الواردة في الفقرة (٦) فيجب على جهة التحكم أو جهة المعالجة إشعار مكتب إدارة البيانات بالوزارة فقط، وعلى مكتب إدارة البيانات بالوزارة إشعار مكتب إدارة البيانات الوطنية بذلك.

١٠,٤ أحكام عامة

١. يتولى مكتب إدارة البيانات بالوزارة مواءمة هذه الوثيقة مع وثائق الوزارة التنظيمية وتعميمها على جميع الجهات التابعة للوزارة أو المرتبطة بها بما يحقق التكامل ويضمن تحقيق الهدف المنشود من إعداد هذه القواعد.
٢. تقوم مكتب إدارة البيانات بالوزارة بمراقبة امتثال الجهات التابعة للوزارة أو المرتبطة بها لهذه القواعد بشكل دوري.
٣. يجب على جهة التحكم وجهة المعالجة الامتثال لهذه القواعد وتوثيق الامتثال وفقاً للآليات والإجراءات التي يحددها مكتب إدارة البيانات بالوزارة.
٤. يجب على جهة التحكم عند تعاقدها مع جهات المعالجة – داخل أو خارج المملكة – أن تتحقق بشكل دوري من امتثال جهات المعالجة لهذه القواعد وفقاً للآليات والإجراءات التي يحددها مكتب إدارة البيانات بالوزارة، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها جهات المعالجة.
٥. يحق للوزارة وضع قواعد إضافية لنقل أنواع محددة من البيانات الشخصية وفقاً لطبيعة وحساسية هذه البيانات بعد التنسيق مع مكتب إدارة البيانات الوطنية.
٦. يقوم مكتب إدارة البيانات بالوزارة بمراجعة معايير التقييم – العامة والقانونية – المتعلقة بحماية البيانات الشخصية عند نقلها خارج الحدود الجغرافية للمملكة واتخاذ القرارات المنظمة لها.

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

٨. يقوم مكتب إدارة البيانات بالوزارة بالتنسيق مع مكتب إدارة البيانات الوطنية 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 مكتب إدارة البيانات الوطنية.

٩. يقوم مكتب إدارة البيانات بالوزارة بإعداد البنود القياسية ومراجعتها لحماية البيانات الشخصية.