وزارة التعليم
Ministry of Education

سياسات حوكمة البيانات

مساعد الوزير للتطوير والتحول

مكتب إدارة البيانات

المعلومات العامة:

اسم الوثيقة	سياسات حوكمة البيانات	عدد الصفحات	74
مالك الوثيقة	مكتب إدارة البيانات	رقم الوثيقة المرجعي	4600710188
دوريّة المراجعة	سنوي أو في حال وجود تغيير أيهما أقرب	موافقة واعتماد	وزير التعليم
رقم النّسخة	3	تاريخ الاعتماد	1446/8/5

المراجعات:

الاسم	الوظيفة	ملخص التغييرات	رقم النّسخة	التاريخ
د. خالد بن عبدالله المجلي	مدير عام مكتب إدارة البيانات	إعداد	1	1443/5/24هـ
		تحديث	1.1	

الموافقات والاعتماد:

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

سجل الاصدارات:

الاصدار	سبب الاصدار	تاريخ النشر
1	إعداد السياسات	1444/2/5هـ
1.1	1.تعديلات نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ ودخوله حيز النفاذ، وصدور اللائحة التنفيذية لنظام حماية البيانات الشخصية. 2.بدء العمل بالهيكل والدليل التنظيمي لوزارة التعليم. 3. صدور تحديث سياسة مشاركة البيانات من الهيئة السعودية للبيانات والذكاء الاصطناعي. 4.تطوير سياسات (إدارة المحتوى والوثائق، وتحقيق القيمة من البيانات، وذكاء الأعمال.	1446/8/5

الفهرس

التعريفات

1 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 المادي والرقمي إلى البيانات والمواد التقنية 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: حالة بحقوق وصلاحيات الوصول إلى البيانات والموارد التّقنية لأي مستخدم أو برنامج أو عمليّة، والتحكم 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: الفرد الذي تتعلق به البيانات الشخصية.

معالجة البيانات الشخصية: أي عملية تُجرى على البيانات الشخصية بأي وسيلة كانت يدوية أو آلية، ومن ذلك: عمليات الجمع، والتسجيل، والحفظ، والفهرسة، والترتيب، والتنسيق، والتخزين، والتعديل، والتحديث، والدمج، والاسترجاع، والاستعمال، والإفصاح، والنقل، والنشر، والمشاركة في البيانات أو الربط البيني، والحجب، والمسح، والإتلاف.

جهة التحكم: أي جهة ترتبط تنظيميا بالوزارة، تحدد الغرض من معالجة البيانات الشخصية وكيفية ذلك، سواء تمت معالجة البيانات بواسطتها أو 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، أو الحصول عليها، أو تمكين الوصول إليها دون تصريح أو سند نظامي، سواء بقصد أو بغير قصد.

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 الأعمال: هو الشّخص المسؤول عن البيانات التي يتمّ جمعها والاحتفاظ 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.

مختص بيانات الأعمال: عادة ما يكون من أعضاء إدارة تقنية المعلومات أو الأمن السيبراني أو كليهما، ويتحمل صيانة وتخزين وحماية البيانات.

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 معلومات تفصيلية تصف البيانات وخصائص استخدامها سواء كانت بيانات أعمال أو بيانات تقنيّة أو تشغيلية.

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

قناة التكامل الحكومية: قناة آمنة لمشاركة البيانات بين الجهات الحكومية بهدف تحقيق التكامل والترابط بين الجهات وتمكينها من أتمتة الخدمات الخاصة بها.

منصة سوق البيانات: هي إحدى منصات البيانات الموجودة لدى بنك البيانات الوطني وتهدف إلى أتمتة كافة عمليات مشاركة البيانات -وفقاً لأحكام هذه السياسة- بين الجهات الحكومية؛ حيث تتيح المنصة للجهات طلب الاشتراك في خدمات مشاركة البيانات (APIs) المنشورة في المنصة بصورة آلية أو طلب خدمات جديدة.

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 حكومية أو خاصة أو فرد يتقدّم بطلب مشاركة البيانات.

الجهة المصدر: هي الجهة الحكومية المعنية -وفقاً لاختصاصاتها النظامية- بوضع المعايير الفنية لحقل محدد أو مجموعة من حقول البيانات، ومعايير التحقق من صحتها والاحتفاظ بها.

الجهة المفوضة: هي الجهة المفوضة بمشاركة البيانات بموجب تفويض من الجهة المصدر وفقاً للإجراءات الموضحة في هذه السياسة، وذلك بعد اتخاذ الخطوات اللازمة لضمان حداثة البيانات.

أطراف عملية مشاركة البيانات: أي جهة تكون طرفاً في عملية مشاركة البيانات، وتشمل مقدم الطلب والجهة المطلوبة منها مشاركة 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.

اتفاقية مشاركة البيانات: اتفاقية قياسية موقعة بين طرفين -عند مشاركة البيانات من قبل الجهة الحكومية مع جهة خاصة أو فرد- تحدد أدوار ومسؤوليات أطراف عملية مشاركة البيانات وفقاً للأحكام والضوابط المحددة في هذه السياسة.

نموذج ضو ابط مشاركة البيانات: نموذج قياسي يتضمن الضوابط اللازمة للتعامل مع البيانات وتحديد الأدوار والمسؤوليات في حال كان أطراف عملية مشاركة البيانات جهات حكومية.

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.

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

الطّفل: كل شخص لم يتجاوز الثامنة 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 الثامنة 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 الشخصية الحسّاسة: كل بيان شخصيّ يتعلق بأصل الفرد العرقي أو أصله الإثني، أو معتقده الدّينيّ أو الفكريّ أو السياسيّ. وكذلك البيانات الأمنيّة والجنائيّة، أو بيانات السّمات الحيويّة التي تحدد الهويّة، أو البيانات الوراثيّة، أو البيانات الصحيّة، والبيانات التي تدل على أن 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 الاحتفاظ بها وآلية التّخلّص منها.

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

الإفصاح عن البيانات الشخصية: تمكين أي شخص -عدا جهة التحكّم أو جهة المعالجة بحسب الأحوال- من الحصول على البيانات الشّخصيّة أو استعمالها أو الاطّلاع عليها بأي وسيلة ولأي غرض.

الموافقة الصّريحة: موافقة تمنح بشكل مباشر وصريح من صاحب البيانات الشخصية بأي شكل من الأشكال وتدل على قبوله بمعالجة بياناته الشخصية بحيث لا يمكن تفسيرها بخلاف ذلك، وتكون قابلة للإثبات.

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

نقل البيانات الشخصية: نقل البيانات الشخصية من مكان إلى آخر لمعالجتها.

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

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

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

النشر للبيانات الشخصية: بث أي من البيانات الشخصية عبر وسيلة نشر مقروءة أو مسموعة أو مرئية، أو إتاحتها.

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

المعالجة: أي عملية تُجرى على البيانات بأي وسيلة كانت يدوية أو آلية، ومن ذلك: عمليات الجمع، والتسجيل، والحفظ، والفهرسة، والترتيب، والتنسيق، والتخزين، والتعديل، والتحديث، والدمج، والاسترجاع، والاستعمال، والإفصاح، والنقل، والنشر، والمشاركة في البيانات أو الربط البيني، والحجب، والمسح، والإتلاف.

البيانات غير المعالجة: هي البيانات التي لم تخضع لعمليّات متقدّمة من المعالجة 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.

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

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

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 الاستفادة 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 الجهة الخاصّة 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 تنبؤيه 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.

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

إتلاف البيانات الشخصية: أي إجراء يتم على البيانات الشخصية ويجعل من المتعذر الاطلاع عليها أو استعادتها مرة أخرى أو معرفة صاحبها على وجه التحديد.

الأهداف

2 الأهداف

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

1. المشاركة في دعم وتعزيز جهود المملكة في تحقيق الرؤية والاستراتيجيّات الوطنيّة.
2. نشر ثقافة مشاركة البيانات والتّعاون لتعزيز وتطوير البيانات والمعلومات والأصول المعرفيّة الخاصّة بوزارة التّعليم.
3. تنظيم عمليّة نشر وتبادل واستخدام/ إعادة استخدام البيانات المحميّة والمعلومات العامّة الخاصّة بوزارة التّعليم مع ضمان المحافظة على حقوق الملكيّة الفكريّة.
4. تحقيق دور فعّال في التّكامل بين الجهات الحكوميّة.
5. المحافظة على خصوصيّة البيانات الشّخصيّة، وسرّية البيانات الحسّاسة.
6. المحافظة على حقوق الأفراد عند التّعامل مع البيانات الشّخصيّة والمعلومات العامّة لدى وزارة التّعليم.
7. تعزيز مفهوم وممارسات البيانات المفتوحة لتحسين الشّفافيّة وتشجيع البحث والابتكار ودفع النّمو الاقتصادي.
8. تعزيز الشّفافيّة وإرساء قواعد الحوكمة عن طريق توزيع الأدوار والمسؤوليات.
9. المشاركة في المحافظة على السيّادة الوطنيّة الرقميّة للبيانات الشّخصيّة.
10. رفع مستوى الثّقة في الخدمات المعتمدة على البيانات.
11. رفع مستوى الخدمات والتّعاملات الالكترونيّة بما يحقّق التّكامليّة.
12. المشاركة في دعم البحوث العلميّة عن طريق تشجيع الباحثين للاستفادة من المعلومات العامّة والنّهوض بالدّور التنموي والرّقابي للمجتمع والمؤسّسات.
13. توفير الفرص المتكافئة لطالبي المعلومات العامّة ممّا يسهم في تعزيز المواطنة المتساوية والشراكة في الوعي بقضايا الوطن العامّة.
14. دعم جهود تعزيز النزاهة ومكافحة الفساد عن طريق الاطلاع على المعلومات العامة كحق إنساني مكفول.

حاكمية سياسات حوكمة البيانات

3 حاكميّة سياسات حوكمة البيانات

3.1 مالك الوثيقة

مكتب إدارة البيانات في وزارة التّعليم.

3.2 مراجعة وتعديل وتغيير السّياسات

1. على المكتب مراجعة السّياسات بشكل سنوي على الأقل أو في حال استحداث تغيير أو متطلّبات تستوجب تعديل سياسة أو أكثر أيّهما أقرب.
2. على المكتب مشاركة تعديلات السّياسات مع الجهات المعنيّة داخل الوزارة للاطّلاع والمراجعة والتّغذية الراجعة لأغراض الموافقة والاعتماد.
3. على المكتب توثيق تعديلات السّياسات في جدول المراجعات وإصدار نسخة جديدة تشمل التّعديلات.

3.3 الامتثال للسّياسات

1. دون إخلال بما ورد في الأنظمة واللوائح والتعليمات ذات الصلة 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.
2. المكتب في وزارة التّعليم المسؤول عن مراقبة الامتثال لبنود هذه السّياسات.
3. يتمّ مراجعة الالتزام ببنود هذه السّياسات من قبل المكتب، ويتم رفع تقرير بالمخالفات لأحكام هذه السّياسة إلى مكتب وزير التّعليم مع التّوصيات لتصويب المخالفات.

3.4 التعامل مع حالات عدم الامتثال

1. عند مراجعة حالات عدم الامتثال، يجب على المكتب اتباع منهجية تدريجية لتحليل سبب عدم الامتثال ومدى الآثار والمخاطر المترتبة على ذلك، والتعامل مع هذه الحالات وفقاً للمستويات التالية:
2. التوعية - يقوم المكتب باستخدام التوعية عند التعامل مع حالات عدم الامتثال العرضية أو غير المقصودة ذات الآثار السلبية المحدودة جداً.
3. التعاون - يقوم المكتب بالتعاون مع الجهة العامة لمنع أو ردع أو معالجة حالات عدم الامتثال ذات الآثار السلبية المحدودة الناجمة عن الإهمال وعدم الامتثال بأحكام وقواعد هذه السياسة.
4. التدخل المباشر - يقوم المكتب بالتحقيق في حالات عدم الامتثال المستمرة والمتكررة أو المتعمدة أو ذات الآثار السلبية الشديدة واتخاذ القرارات التي تتناسب مع حجم وطبيعة الآثار السلبية.

3.5 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 للاستثناء أو الرجوع عنه.

سياسة تصنيف البيانات

4 سياسة تصنيف البيانات

4.1 نطاق السّياسة

تنطبق أحكام هذه السّياسة على جميع البيانات التي تنتجها جهة التحكم وجهة المعالجة مهما كان مصدرها، أو شكلها أو طبيعتها.

4.2 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 الامتيازات اللّازمة لأداء المهام والمسؤوليّات المناطة بهم.

4.3 مستويات تصنيف البيانات

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

مستوى التّصنيف	درجة الأثر	الوصف	أمثلة استرشاديه
سرّي 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 الاقتصاد 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 استرشاديه
سرّي	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 الاقتصاد 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 الاقتصادية. * 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 الاقتصادية 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 استرشاديه
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 الاقتصادية. * 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 أو الإفصاح غير المصرّح به، كما تعتبر هذه القائمة غير شمولية.

فئات ودرجات تقييم الأثر وفقاً لمستويات تصنيف البيانات. جدول (2)

فئة الأثر الرّئيسيّة	**المصلحة الوطنيّة**		
فئة الأثر الفرعيّة	سمعة المملكة		
الاعتبارات	هل ستخضع المعلومات لاهتمام 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:			
سرّي للغاية	**سرّي**	**مقيّد**	**عام**
عالي	متوسّط	منخفض	لا يوجد أثر
قطع العلاقات الدبلوماسيّة والانتماءات السياسيّة أو تهديد الاتّفاقيات وشروط المعاهدات أو كلهما.	تتأثّر العلاقات الدبلوماسيّة سلباً على المدى الطّويل.	لن يحدث تأثير على العلاقات الدبلوماسيّة أو سيحدث تأثير بسيط على المدى القصير.	لا يوجد تأثير على المصالح الحيويّة الوطنيّة.

فئة الأثر الرّئيسيّة	**المصلحة الوطنيّة**		
فئة الأثر الفرعيّة	الاقتصاد الوطنيّ		
الاعتبارات	هل يؤدّي الكشف عن المعلومات إلى خسائر اقتصاديّة على المستوى الوطنيّ؟		
مستوى الاثر:			
سرّي للغاية	**سرّي**	**مقيّد**	**عام**
عالي	متوسّط	منخفض	لا يوجد أثر
تأثير طويل المدى على الاقتصاد الوطنيّ مع انخفاض لا يُمكن تداركه في النّاتج المحلّي الإجمالي أو أسعار الأسواق الماليّة أو نسبة البطالة أو القوّة الشّرائيّة أو المؤشّرات الأخرى ذات الصّلة؛ مما ينعكس سلباً على جميع القطاعات في المملكة.	تأثير طويل المدى على الاقتصاد 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 الاقتصاد 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:			
سرّي للغاية	**سرّي**	**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.

4.4 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 (أو من يفوضه).

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

4.4.1 علامات الحماية

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

4.4.2 الوصول

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

4.4.3 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.

4.4.4 التخزين

1. لا تُترك البيانات المصنّفة على أنّها "سرّي للغاية" و" سرّي" و "مقيّد" وكذلك الأجهزة المحمولة التي تعالج أو تخزّن هذه البيانات دون مراقبة.
2. يجب حماية البيانات المصنّفة على أنّها "سرّي للغاية" و" سرّي" و "مقيّد" غير المراقبة أثناء تخزينها مادّياً أو إلكترونيّاً باستخدام أحد طرق التّشفير المعتمدة من قبل الإدارة العامة للأمن السّيبراني.

4.4.5 مشاركة البيانات

1. يجب تحديد الوسائل الماديّة والرقميّة المناسبة لتبادل البيانات بشكل آمن بما يضمن تقليل المخاطر المحتملة والامتثال لأنظمة مشاركة البيانات.
2. 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.

4.4.6 الاحتفاظ بالبيانات

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

4.4.7 التّخلّص من البيانات

1. يتمّ التّخلّص من جميع البيانات بشكل آمن وفقاً للجدول الزمني للاحتفاظ بالبيانات بعد الحصول على موافقة ممثّل بيانات الأعمال.
2. يتمّ التّخلّص من البيانات التي تمّ تصنيفها على أنّها "سرّية للغاية" و" سرّي" التي يتمّ التّحكم بها إلكترونياً باستخدام أحدث طرق التّخلّص من الوسائط الإلكترونية.
3. يتمّ التّخلّص من جميع الوثائق الورقيّة حسب اللوائح والأنظمة.
4. يتمّ إعداد سجل مفصّل عن جميع البيانات التي تمّ التّخلّص منها.

4.4.8 الأرشفة

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

4.4.9 إلغاء التّصنيف (رفع السرّيّة)

1. يتم 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.
2. في حال تمّ تصنيف البيانات بشكل خاطئ، يجب على مستخدم البيانات إشعار ممثّل بيانات الأعمال لتحديد مدى الحاجة إلى إعادة تصنيفها بشكل مناسب.
3. 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 1 يناير 2021).
   - بعد ظروف أو أحداث معيّنة لها تأثيراً مباشراً على البيانات (مثلا: إحداث تغيير في الأوّلويات الاستراتيجيّة أو تغيير موظفي الوزارة).
4. 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.

4.5 الخطوات اللّازمة لتصنيف البيانات

4.5.1 الخطوة 1 – تحديد جميع بيانات الوزارة

جرد وتحديد جميع البيانات التي تمتلكها الوزارة.

4.5.2 الخطوة 2 – تعيين مسؤول تصنيف البيانات

بمجرد تحديد جميع البيانات يتم تفويض شخص يتولى مسؤوليّة عمليّة التّصنيف بإشراف ومتابعة المكتب.

4.5.3 الخطوة 3 – إجراء عمليّة تقييم الأثر

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

1. الإفصاح عن هذه البيانات أو الوصول غير المصرّح به إليها.
2. إجراء تعديل على هذه البيانات أو إتلافها أو كليهما.
3. 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 والأمني) ما لم تقتضِ طبيعتها أو حساسيتها مستويات أدنى من التّصنيف.

4.5.3.1 الخطوة أ-3 - تحديد فئة الأثر:

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

1. المصلحة الوطنيّة.
2. أنشطة الوزارة.
3. صحة أو سلامة الأفراد.
4. الموارد البيئية.

4.5.3.2 الخطوة ب-3 - تحديد مستوى الأثر:

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

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

تحدّد هذه المعايير مستويات الأثر الأربعة:

1. عالي: يؤدّي الوصول إلى البيانات أو الإفصاح عنها إلى حدوث أضرارٍ جسيمة أو خطيرة للغاية على المدى الطويل لا يمكن تداركها أو إصلاحها.
2. متوسّط: يؤدّي الوصول إلى البيانات أو الإفصاح عنها إلى حدوث أضرار جسيمة أو خطيرة يصعب السّيطرة عليها.
3. منخفض: يؤدّي الوصول إلى البيانات أو الإفصاح عنها إلى أضرارٍ محدودة يمكن السّيطرة عليها أو أضرار متقطّعة على المدى القصير يمكن السّيطرة عليها.
4. 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:

1. عالٍ: تُصنّف البيانات باعتبارها "سرّية للغاية".
2. متوسّط: تُصنف البيانات على أنّها "سرّية".
3. منخفض: يلزم إجراء مزيدٍ من التقييمات (يرجى الاطّلاع على الخطوة 4 و5).
4. لا يوجد أثر: تُصنّف البيانات على أنّها بياناتٍ "عامّة".

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

يجب الأخذ بعين الاعتبار الخطوتين 4 و5 عندما يكون مستوى الأثر المحدّد منخفض. يتمّ الانتقال إلى الخطوة 6 عندما تُصنّف البيانات على أنّها "سرّية للغاية" أو "سرّية" أو "عامّة".

4.5.4 الخطوة 4 – 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 حماية البيانات الشخصية ونظام مكافحة الجرائم المعلوماتيّة ونظام التّجارة الالكترونيّة ... 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 5.

4.5.5 الخطوة 5 – الموازنة بين مزايا الإفصاح عن البيانات والآثار السّلبية (فقط إذا كانت الإجابة على الخطوة 4 "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.

1. إذا كانت المزايا أكبر من الآثار السّلبية، تصنّف البيانات على أنّها "عامّة."

2. إذا كانت المزايا أقل من الآثار السّلبية، تصنّف البيانات على أنّها "مقيّدة".

4.5.6 الخطوة 6 – مراجعة مستوى التّصنيف

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

4.5.7 الخطوة 7 – 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 الانتهاء 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".

4.6 الأدواروالمسؤوليات 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:** هو الشّخص المسؤول عن المهام التالية:
  1. **تصنيف البيانات:** تصنيف البيانات التي تنتجها أو تجمعها إدارته والإدارات التابعة لها.
  2. **تجميع البيانات:** التأكّد من تصنيف البيانات المجمّعة من مصادرٍ متعدّدة على أعلى مستويات التّصنيف المستخدمة في تصنيف أي بيانات بشكل فردي.
  3. **تنسيق تصنيف البيانات:** التّأكّد من أنّ البيانات المتبادلة مصنّفة ومحميّة بصورة متّسقة.
  4. **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 مسؤول التصنيف، وعادة ما يكون في مستوى إداري عالٍ.
- **مختص بيانات الأعمال:** عادةً ما يكون مختص بيانات الأعمال من أعضاء إدارات تقنية المعلومات أو الأمن السيبراني أو كلهما، 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 (أو من يفوضه) من يراه من ذوي الاختصاص لأداء هذه الأدوار.

سياسة حماية البيانات الشخصية

5 سياسة حماية البيانات الشّخصيّة

5.1 نطاق السّياسة

تنطبق أحكام هذه السّياسة على جهة التحكم وجهة المعالجة التي تقوم كليّاً أو جزئياً بمعالجة البيانات الشّخصيّة.

يستثنى من ذلك جمع البيانات الشخصية من غير صاحبها مباشرةً، أو مُعالجتها لغرض آخر غير الذي جمعت من أجله، وذلك في الأحوال الآتية:

1. إذا وافق صاحب البيانات الشخصية على ذلك، وفقاً لأحكام نظام حماية البيانات الشخصية.
2. إذا كانت البيانات الشخصية متاحة للعموم، أو جرى جمعها من مصدر متاح للعموم.
3. إذا كان جمع البيانات الشخصية أو معالجتها؛ مطلوباً لأغراض المصلحة العامة أو لأغراض أمنية أو لتنفيذ نظام أخر أو لاستيفاء مُتطلبات قضائية.
4. إذا كان التقيد بهذا الحظر قد يُلحق ضرراً بصاحب البيانات الشخصية أو يؤثر على مصالحه الحيوية.
5. إذا كان جمع البيانات الشخصية أو معالجتها ضرورياً لحماية الصحة العامة أو السلامة العامة أو حماية حياة فرد أو أفراد معينين أو حماية صحتهم.
6. إذا كانت البيانات الشخصية لن تُسجل أو تُحفظ في صيغة تجعل من الممكن تحديد هوية صاحبها ومعرفته بصورة مباشرة أو غير مباشرة.
7. إذا كان جمع البيانات الشخصية أو معالجتها ضرورياً لتحقيق مصالح مشروعة، مالم يخل ذلك بحقوق صاحب البيانات الشخصية أو يتعارض مع مصالحه ولم تكن تلك البيانات بيانات حساسة.

5.2 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 والمو افقة

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

المبدأ الرّ ابع: 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 والاحتفاظ بها والتّخلّص منها

أن يتمّ تقييد معالجة البيانات الشّخصيّة بالأغراض المحدّدة في إشعار الخصوصيّة والتي من أجلها قدّم صاحب البيانات موافقته الصّريحة، والاحتفاظ 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 الصّريحة.

المبدأ الثامن: 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 الإدارة العامة للأمن السيبراني.

المبدأ التّاسع: جودة البيانات

أن يتمّ الاحتفاظ 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.

5.3 حقوق صاحب البيانات

أوّلاً: الحق في العلم، ويشمل ذلك إحاطته علماً بالمسوغ النظامي لجمع بياناته الشخصية والغرض من جمعها.

ثانياً الحق في وصوله إلى بياناته الشخصية المتوافرة لدى الوزارة، وفق الضوابط والإجراءات التي تحددها اللوائح.

ثالثاً: الحق في طلب الحصول على بياناته الشخصية المتوافرة لدى الوزارة بصيغة مقروءة وواضحة، وفق الضوابط والإجراءات التي تحددها اللوائح.

رابعاً: الحق في طلب تصحيح بياناته الشخصية المتوافرة لدى الوزارة، أو إتمامها، أو تحديثها.

خامساً: الحق في طلب إتلاف بياناته الشخصية المتوافرة لدى الوزارة مما انتهت الحاجة إليه منها.

5.4 التزامات الوزارة فيما يخص حماية البيانات الشخصية

1. تقوم الوزارة 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.
2. يقوم المكتب بإعداد وتطبيق السّياسات والإجراءات المتعلّقة بحماية البيانات الشّخصيّة، ويكون المسؤول الأوّل بالوزارة - أو من يفوّضه - مسؤولاً عن الموافقة عليها واعتمادها. ويكون المكتب هو المسؤول عن مراقبة الامتثال لهذه السّياسة بشكل دوري.
3. 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.
4. تقوم الجهة المختصة داخل الوزارة بمراجعة وتحديث العقود واتّفاقيات مستوى الخدمة والتّشغيل بما يتوافق مع سياسات وإجراءات الخصوصيّة المعتمدة من المسؤول الأوّل بالوزارة.
5. يقوم المكتب بإعداد وتوثيق الإجراءات اللّازمة 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.
6. يقوم المكتب بإعداد برامج توعوية لتعزيز ثقافة الخصوصيّة ورفع مستوى الوعي وفقاً لسياسات وإجراءات الخصوصيّة المعتمدة من المسؤول الأوّل بالوزارة.
7. يجب أن يتمّ إشعار صاحب البيانات - بطريقة ملائمة عند جمع البيانات - بالغرض والأساس النّظامي /الاحتياج الفعلي والوسائل والطّرق المستخدمة لجمع ومعالجة ومشاركة البيانات الشّخصيّة وكذلك التّدابير الأمنيّة لضمان حماية الخصوصيّة حسب نظام حماية البيانات الشخصية ولائحته التنفيذية.
8. يجب أن يتمّ إشعار صاحب البيانات عن المصادر الأخرى التي يتمّ استخدامها في حال تمّ جمع بيانات إضافيّة بطريقة غير مباشرة (من جهات أخرى).
9. يجب أن يتمّ أخذ موافقة صاحب البيانات عند معالجة البيانات الشّخصيّة وفقاً لنظام حماية البيانات الشخصية ولائحته التنفيذية.
10. 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) .
11. يقوم المكتب بالتأكّد من أنّ الغرض من جمع البيانات متوافقاً مع نظام حماية البيانات الشخصية ولائحته التنفيذية وذا علاقة مباشرة بنشاط الوزارة.
12. أن يكون محتوى البيانات مقتصراً على الحدّ الأدنى من البيانات اللّازمة لتحقيق الغرض من جمعها.

13. تقييد جمع البيانات على المحتوى المعدّ سلفاً (الموضح في القاعدة 12) ويكون بطريقة عادلة (مباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التّضليل) .
14. اقتصار استخدام البيانات على الغرض التي جُمعت من أجله.
15. يقوم المكتب بإعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات وفقاً للأغراض المحدّدة والأنظمة والتّشريعات ذات العلاقة.
16. يجب أن يتمّ تخزين البيانات الشّخصيّة ومعالجتها من قبل جهة التحكم داخل الحدود الجغرافيّة للمملكة لضمان المحافظة على السّيادة الوطنيّة الرقميّة لهذه البيانات، ولا تجوز معالجتها خارج المملكة إلا بعد موافقة صاحب الصلاحية داخل الوزارة، بعد تنسيق المكتب مع مكتب إدارة البيانات الوطنية.
17. 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 الإدارة العامة للأمن السّيبراني.
18. يجب تضمين أحكام سياستي الاحتفاظ والتّخلّص من البيانات الخاصّة بالوزارة في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.
19. تحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشّخصيّة وذلك لمراجعتها وتحديثها.
20. التّحقّق من هويّة الأفراد قبل منحهم الوصول إلى بياناتهم الشّخصيّة وفقاً للضّوابط المعتمدة من قبل الإدارة العامة للأمن السّيبراني.
21. يحظر مشاركة البيانات الشّخصيّة مع جهات أخرى إلا وفقاً للأغراض المحدّدة وبعد موافقة صاحب البيانات ووفقاً لنظام حماية البيانات الشخصية ولائحته التنفيذية على أن تُزوّد الجهات الأخرى بسياسات وإجراءات الخصوصيّة المتّبعة وتضمينها في العقود والاتّفاقيات.
22. إشعار أصحاب البيانات وأخذ الموافقة منهم في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الأغراض المحدّدة.
23. أخذ موافقة مكتب إدارة البيانات الوطنية قبل مشاركة البيانات الشّخصيّة مع جهات أخرى خارج المملكة.
24. أن يقوم المكتب بإعداد وتوثيق ومتابعة تطبيق الإجراءات اللّازمة لضمان دقّة البيانات الشّخصيّة واكتمالها وحداثتها وارتباطها بالغرض الذي جُمعت من أجله.
25. استخدام الضّوابط الإداريّة والتّدابير التّقنيّة المعتمدة في سياسات الوزارة للأمن السيبراني 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 الإدارة العامة للأمن السّيبراني.

26. 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.
27. تتولى الجهة المختصة داخل الوزارة مواءمة أحكام هذه السّياسة مع وثائق الوزارة التّنظيميّة وتعميمها على جميع الجهات التّابعة لها أو المرتبطة بها بما يحقّق التّكامل ويضمن تحقيق الهدف المنشود من إعداد هذه السّياسة.
28. أن يكون المكتب مسؤول عن مراقبة الامتثال لتنفيذ هذه السّياسات وفقاً للآليات والإجراءات التي تحدّدها الجهات التّنظيميّة.

29. على جهة التحكم إبلاغ الجهات التنظيمية فوراً ودون تأخير وبما لا يتجاوز 72 ساعة من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشّخصيّة أو تلفها أو وصول غير مشروع إليها، وفقاً للآليات والإجراءات التي تحدّدها الجهات التّنظيميّة.
30. يجب على الجهة المختصة داخل الوزارة عند تعاقدها مع جهات المعالجة أن تتحقّق من التزام جهات المعالجة لهذه السّياسة وفقاً للآليّات والإجراءات التي تحدّدها الجهات التّنظيميّة، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها جهات المعالجة.
31. يحقّ للوزارة وضع قواعد إضافيّة لمعالجة أنواع محدّدة من البيانات الشّخصيّة وفقاً لطبيعة وحساسيّة هذه البيانات بعد التّنسيق مع مكتب إدارة البيانات الوطنيّة.
32. يقوم المكتب بعد التّنسيق مع مكتب إدارة البيانات الوطنيّة - بإعداد الآليات والإجراءات التي تنظّم عمليّة معالجة الشّكاوى وفقاً لإطار زمني محدّد وحسب التّسلسل التّنظيمي للجهات.

سياسة مشاركة البيانات

6 سياسة مشاركة البيانات

6.1 نطاق السياسة

تنطبق أحكام هذه السّياسة على جهة التحكم وجهة المعالجة 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.

يستثنى من تطبيق أحكام هذه السياسة في الأحوال الآتية:

1. في حال كان مقدم الطلب جهة حكومية وكان الطلب لأغراض أمنية أو لاستيفاء متطلبات قضائية، أو تنفيذاً لاتفاقية دولية تكون المملكة طرفا فيها.
2. في حال كان مقدم الطلب جهة حكومية وكان طلب مشاركة البيانات لغرض ممارسة مهام رقابية أو متابعة أداء الجهات الحكومية وفقاً لأنظمتها أو تنظيماتها، على أن يتم الالتزام بما يأتي:
   أ. توثيق طلب مشاركة البيانات في سجل خاص بذلك من قبل المكتب.
   ب. أن يكون مقدم الطلب مسؤولا عن طلب البيانات بالحد الأدنى اللازم لتحقيق الغرض من جمعها والمحافظة عليها بما لا يخل بالأحكام النظامية أو المتطلبات التنظيمية الأخرى ذوات العلاقة.
   ج. أن تكون مشاركة البيانات بصورة آلية من خلال قناة التكامل الحكومية أو أي وسيلة آلية آمنة، وإن تعذر ذلك وكانت وسيلة المشاركة غير آلية فتتم مشاركة البيانات من خلال وسيلة آمنة وموثوقة، وفقاً لما يصدر من الجهات المختصة.
   د. إتلاف البيانات التي تمت مشاركتها بعد انتهاء الغرض من الحصول عليها، مع مراعاة الأحكام النظامية والمتطلبات التنظيمية ذوات العلاقة.

6.2 المبادئ الرئيسية لمشاركة البيانات

المبدأ الأول: تعزيز ثقافة المشاركة

على كل جهة مصدر مشاركة البيانات التي تصدرها وفقاً لأحكام هذه السياسة وذلك لتعزيز الاستفادة من هذه البيانات وتحقيق التكامل بين الجهات الحكومية.

المبدأ الثاني: مبدأ المرّة الواحدة

قيام وزارة التعليم بجمع البيانات -في سياق ممارسة اختصاصاتها المقررة نظاماً- لمرّة واحدة مع إمكانية مشاركتها وإعادة استخدامها بما لا يتعارض مع الأنظمة ذات العلاقة؛ وذلك للحد من ازدواجيتها وتعارضها وتعدد مصادرها وضمان تكاملها وحداثتها وجودتها.

المبدأ الثالث: مشروعية الغرض

تتم مشاركة البيانات لأغراض مبنية على أساس نظام أو احتياج عملي مبرر دون إلحاق أي ضرر بالمصالح الوطنية، أو أنشطة الجهات، أو خصوصية الأفراد، أو سلامة البيئة، وحصر استخدامها من قبل مقدم الطلب للأغراض المحددة في طلب مشاركة البيانات.

المبدأ الرابع: الاطلاع المصرّح به

أن يكون لدى جميع أطراف عملية مشاركة البيانات صلاحية الاطلاع على هذه البيانات والحصول عليها واستخدامها وذلك من خلال تحديد المخولين بالاطلاع على هذه البيانات بعد القيام بالإجراءات اللازمة للتأكد من موثوقيتهم (إن تطلب الأمر ذلك، حسب طبيعة ومستوى تصنيفها ودرجة حساسيتها وفقاً لسياسة تصنيف البيانات).

المبدأ الخامس: الشفافية

تتم إتاحة جميع المعلومات الضرورية المتعلقة بطلب مشاركة البيانات لجميع أطراف عملية مشاركة البيانات، وذلك من خلال إيضاح البيانات المطلوبة ومستويات تصنيفها -بحسب ما تنص عليه سياسة تصنيف البيانات- والغرض من طلبها، وطرق حفظها، والضوابط المستخدمة لحمايتها وآلية إتلافها.

المبدأ السادس: المسؤولية المشتركة

أن يكون جميع أطراف عملية مشاركة البيانات مسؤولين مسؤولية مشتركة عن قرارات مشاركة البيانات، وفقاً للأدوار والمسؤوليات في اتفاقية مشاركة البيانات أو الضوابط المناسبة -بحسب الأحوال- لضمان معالجتها وفقاً للأغراض المحددة.

المبدأ السابع: أمن البيانات

أن يقوم جميع أطراف عملية مشاركة البيانات بتطبيق الضوابط الأمنية المناسبة لحماية البيانات ومشاركتها في بيئة آمنة وموثوقة وفقاً للمتطلبات التنظيمية ذوات العلاقة، ووفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني.

المبدأ الثامن: الاستخدام الأخلاقي

أن يقوم جميع أطراف عملية مشاركة البيانات -إضافة إلى الالتزام بالمتطلبات التنظيمية ذوات العلاقة- بتطبيق الممارسات الأخلاقية لضمان استخدام البيانات في إطار من المسؤولية، والعدالة، والنزاهة، والأمانة.

6.3 القواعد العامة لمشاركة البيانات

مع مراعاة الخطوات اللازمة لإجراء عملية مشاركة البيانات الموضحة في البند (6.6)، تتمثل القواعد العامة التي يجب اتباعها عند مشاركة البيانات فيما يأتي:

1. في حال كان مقدم الطلب جهة حكومية، وكانت البيانات مطلوبة بصورة آلية تتم عملية مشاركة البيانات باستخدام قناة التكامل الحكومية.
2. في حال كانت مشاركة البيانات بين الجهات الحكومية بصورة آلية وتعذر استخدام قناة التكامل الحكومية أو كانت هناك أسباب مبررة لدى أطراف عملية مشاركة البيانات، فتقترح الأطراف وسيلة مشاركة آمنة ومناسبة ويتم أخذ موافقة مكتب إدارة البيانات الوطنية عليها.
3. في حال تعذر استخدام أي من الوسائل المشار إليها في الفقرة (1) والفقرة (2) وكانت البيانات مطلوبة من خلال وسيلة غير آلية، يجب على أطراف عملية مشاركة البيانات القيام بمشاركة البيانات من خلال وسيلة آمنة وموثوقة، وفقاً لما يصدر من الجهات المختصة.
4. تكون منصة سوق البيانات الوسيلة المعتمدة لطلبات مشاركة البيانات بين الجهات الحكومية، وللجهات الحكومية -في حال عدم إمكانية الحصول على البيانات من خلال سوق البيانات- تقديم الطلب إلى المكتب لنشر البيانات المطلوبة على قناة التكامل الحكومية وفقاً للآلية التي يحددها مكتب إدارة البيانات الوطنية.
5. في حال كان مقدم الطلب جهة غير حكومية يتم تقديم طلب مشاركة البيانات إلى المكتب وفقاً للآلية التي يتم تحددها.
6. يتم إرفاق البيانات الوصفية عند مشاركة البيانات، على أن يتم إيضاح مستويات تصنيف البيانات المطلوبة.
7. في حال كان مقدم الطلب جهة حكومية يتم تطبيق ضوابط مشاركة البيانات وفقاً لنموذج يتم إعداده من المكتب.
8. في حال كانت البيانات المطلوبة بيانات لأغراض تشغيلية ولم تكن الوزارة هي الجهة المصدر أو جهة مفوضة ولم يتم يتضمن الطلب موافقة الجهة المصدر، يقوم المكتب بإشعار مقدم الطلب خلال (5) أيام عمل من تاريخ استلام الطلب بالحصول على موافقة الجهة المصدر، وعلى الجهة المصدر الرد على الطلب بالموافقة أو الرفض كلياً أو جزئياً على أن يكون الرفض مسبباً وذلك خلال مدة لا تزيد عن (10) أيام عمل من تاريخ طلب الموافقة.

9. في حال عدم رد الجهة المصدر خلال المدة المحددة في الفقرة (8) من هذا البند فيعد ذلك رفضاً للطلب، ويمكن لمقدم الطلب -بحسب الأول المشار لها في الفقرة (8) من هذا البند- الرفع لمكتب إدارة البيانات الوطنية للنظر فيه وفق ما نصت عليه الفقرة (3) من البند (6.8) من هذه السياسة.
10. يمكن للوزارة القيام بمشاركة البيانات دون الحصول على موافقة الجهة المصدر في حال وجود تفويض بذلك، وفقاً لما ورد في البند (6.4).
11. على أطراف عملية المشاركة الالتزام بالأحكام المنظمة للمنافسة عند القيام بعملية مشاركة البيانات، وعدم الاتفاق على ما من شأنه الإخلال بالأحكام النظامية ذات الصلة.
12. مع مراعاة ما نصت عليه الفقرة (6) من البند (6.6)، يتم توقيع اتفاقية مشاركة البيانات من قبل المسؤول الأول أو من يفوضه في حال كانت البيانات المطلوبة مصنفة على مستوى سري أو سري للغاية، ويتم توقيعها من قبل مدير عام مكتب إدارة البيانات عند مشاركة البيانات المصنفة على مقيد.
13. في حال كانت البيانات المطلوبة مشاركتها لأغراض تحليلية، فيتم طلب البيانات من بنك البيانات الوطني بعد الحصول على موافقة الوزارة، وفي حال تعذر ذلك فيتم الحصول عليها مباشرة من الوزارة مع مراعاة الأحكام الواردة في الفقرة (1) و (2) و (3) من هذا البند.

6.4 طلب التفويض بمشاركة البيانات

1. يمكن للوزارة القيام بعملية مشاركة البيانات بناءً على تفويض من الجهة المصدر على أن يتضمن التفويض الآتي:
   أ. مدة التفويض وآلية التمديد.
   ب. نوع البيانات ومستوى تصنيفها.
   ج. وسيلة المشاركة مع مراعاة الأحكام المنصوص عليها في البند (6.3).
   د. المسؤوليات والأدوار لضمان أمن وحماية البيانات عند مشاركتها مع مقدم الطلب.
   هـ. آلية تسوية الخلافات الناشئة عن التفويض.
   و. آي بنود أخرى ترى الجهة المفوضة للبيانات (مُصدِرة التفويض) إضافتها في التفويض.
2. يجوز للجهة المفوضة للبيانات (مُصدِرة التفويض) متابعة التزام الوزارة بالمتطلبات الواردة في التفويض وطلب سجلات طلبات المشاركة والبيانات التي تمت مشاركتها.
3. على الوزارة اتخاذ الخطوات اللازمة لضمان حداثة البيانات قبل القيام بعملية مشاركة البيانات.

6.5 آلية تحديد ضوابط مشاركة البيانات

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

6.5.1 الأساس النظامي:

(المبادئ ذات العلاقة: المبدأ الأول: تعزيز ثقافة المشاركة، المبدأ الثاني: مبدأ المرة الواحدة، المبدأ الثالث: مشروعية الغرض، المبدأ السادس: المسؤولية المشتركة، المبدأ الثامن: الاستخدام الأخلاقي).

أ. أن يتم إيضاح الأساس النظام أو الاحتياج العملي المبرر لمشاركة البيانات، ومنها على سبيل المثال تنظيم الجهة أو الأوامر والقرارات ذوات الصلة التي تسمح للجهة بالحصول على بيانات الوزارة.
ب. أن تتم المحافظة على سرية البيانات وفقاً لمستوى تصنيفها وخصوصية أصحاب البيانات الشخصية وحماية حقوق الملكية الفكرية.

6.5.2 التفويض:

(المبادئ ذات العلاقة: المبدأ الرابع: الاطلاع المصرح به، المبدأ السابع: أمن البيانات).

أ. تحديد المخولين بطلب البيانات وتلقيها لدى أطراف عملية المشاركة وفقاً لضوابط الاستخدام والوصول إلى البيانات الموضحة في سياسة تصنيف البيانات، على أن يتم تعيين أو تفويض الشخص المناسب -حسب المؤهلات والتدريب المطلوب- لضمان التعامل مع البيانات بشكل مسؤول.

ب. يتم منح الصلاحيات بناءً على مبدأ الحاجة إلى المعرفة ومبدأ الحد الأدنى من الامتيازات بحسب ما هو منصوص عليه في سياسة تصنيف البيانات عند التعامل مع البيانات التي تمت مُشاركتها.

6.5.3 نوع البيانات:

(المبادئ ذات العلاقة: المبدأ الأول: تعزيز ثقافة المشاركة، المبدأ الثاني: مبدأ المرة الواحدة، المبدأ الثالث: مشروعية الغرض، المبدأ الخامس: الشفافية).

أ. أن يتم تحديد الحد الأدنى من البيانات المطلوبة لتحقيق الأغراض المحددة.

ب. أن يتم تحديد البيانات المطلوبة وصيغتها والمتطلبات المتعلقة بتعديلها أو تغييرها (مثل صيغة البيانات، دقة البيانات، مستوى التفاصيل، هيكلة البيانات، نوع البيانات).

ت. أن يتم تحديد آلية يتفق عليها أطراف عملية المشاركة لتحديث البيانات التي تمت مُشاركتها مسبقاً في حال الحاجة إلى ذلك.

6.5.4 المعالجة المسبقة للبيانات:

(المبادئ ذات العلاقة: المبدأ الثاني: مبدأ المرة الواحدة، المبدأ السابع: أمن البيانات).

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

ب. أن يتم تقييم جودة البيانات المطلوبة وصحتها وسلامتها وتحديد ما إذا كانت تتطلب إجراء تحسين قبل مشاركتها.

6.5.5 وسائل مشاركة البيانات:

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

أ. أن يتم التحقق من أمن وموثوقية قنوات مشاركة البيانات في حال عدم إمكانية استخدام الوسائل المنصوص عليها في الفقرة (1) من البند (6.3) للتقليل من المخاطر المحتملة، وفقاً للمتطلبات التنظيمية الصادرة عن الجهات ذوات الاختصاص.

ب. أن يتم الاتفاق على مدد الاحتفاظ وآلية إتلاف البيانات محل طلب مشاركة البيانات عند تحقيق الغرض من الحصول عليها مع مراعاة المتطلبات التنظيمية ذوات العلاقة.

6.5.6 استخدام البيانات والمحافظة عليها:

(المبادئ ذات العلاقة: المبدأ الثالث: مشروعية الغرض، المبدأ الخامس: الشفافية، المبدأ السابع: أمن البيانات، المبدأ الثامن: الاستخدام الأخلاقي).

أ. أن يتم تحديد متطلبات حماية البيانات التي ستتم مشاركتها، وتطبيق الضوابط المحددة لحمايتها بعد مشاركتها وفقاً لمستوى تصنيفها.

ب. أن يتم فرض قيود مناسبة على الاستخدام أو المعالجة المسموح بها للبيانات (إن وجُدت)، مثل قيود خاصة بالمعالجة، أو قيود مكانية، أو زمانية، أو حقوق حصرية، أو تجارية.

ج. أن يتم تحديد حقوق الجهة المطلوبة منها مشاركة البيانات سواءً كانت جهة مصدرة أو مفوضة في عملية مشاركة البيانات بإجراء عمليات التدقيق والمراجعة، بالإضافة إلى حقوقه اتجاه أي طرف ثالث مستفيد من البيانات.

د. أن يتم الاتفاق على إجراءات تسوية النزاعات.

هـ. أن يتم تحديد ما إذا كان هناك طرف ثالث للاستفادة من البيانات بعد مشاركتها والاتفاق على الآلية المنظمة لذلك.

6.5.7 مدة مشاركة البيانات وعدد مرات المشاركة وإلغاء المشاركة:

(المبادئ ذات العلاقة: المبدأ الثالث: مشروعية الغرض، المبدأ السابع: أمن البيانات).

أ. أن يتم تحديد مدة مشاركة البيانات والموعد النهائي للوصول إلى البيانات أو تخزينها.

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

ج. أن يتم تحديد الأطراف الذين يحق لهم إنهاء مشاركة البيانات قبل التاريخ المتفق عليه، والمستند النظامي، وفترة الإشعار المسموح بها.

6.5.8 أحكام المسؤولية:

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

أ. أن يتم الاتفاق على تحديد المسؤوليات في حال عدم الالتزام ببنود الاتفاقية، وغيرها من الالتزامات بين أطراف عملية مشاركة البيانات.

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

6.6 الخطوات اللازمة لإجراء عملية مشاركة البيانات

تتم معالجة طلبات مشاركة البيانات بحسب التسلسل الآتي:

1. مع مراعاة ما نصت عليه الفقرة رقم (4) و (5) من البند (6.3)، يقوم مقدّم المطلب بإرسال طلب مشاركة البيانات إلى المكتب، على أن يتم إرسال الطلب عن طريق مكتب الجهة في حال كان مقدم الطلب جهة حكومية.
2. التحقق من مستوى تصنيف البيانات المطلوبة، وفي حال عدم تحديد مستوى التصنيف، يجب على المكتب تصنيف البيانات المطلوبة وفقاً لسياسة تصنيف البيانات.
3. قيام المكتب بتقييم الطلب وفقاً لما يلي:
   أ- وجود غرض مشروع من مشاركة البيانات مبني على أساس نظامي أو احتياج عملي مبرر.
   ب- اقتصار البيانات المطلوبة وفق الحد الأدنى اللازم لتحقيق الغرض من طلب المشاركة.
   ج- موافقة الجهة المصدر في حال كان طلب مشاركة البيانات مقدماً إلى جهة غير الجهة المصدر أو الجهة المفوضة.
4. للمكتب في حال عدم استيفاء الطلب للمتطلبات المنصوص عليها في الفقرة (3) من هذا البند أن يرفض الطلب مع إيضاح مسببات الرفض وإتاحة الفرصة لمقدم الطلب لاستكمال المتطلبات وفقاً للفقرة (2) من الإطار الزمني لعملية مشاركة البيانات الواردة في البند (6.7).
5. عند استيفاء جميع متطلبات المشاركة يتم تحديد الضوابط المناسبة وفقاً للبند (6.5) وذلك لضمان الالتزام بمبادئ مشاركة البيانات وتحقيق الأهداف المحددة لكل منها.
6. يتم توقيع اتفاقية مشاركة البيانات في حال كان مقدم الطلب جهة غير حكومية، ويتم استيفاء الضوابط المشار إليها في الفقرة (2) من البند (6.8) في حال كان مقدم الطلب جهة حكومية.
7. عند استيفاء ما ورد في الفقرة (6) من هذا البند، تتم مشاركة البيانات المطلوبة مع مقدم الطلب وفقاً للمدة الزمنية المحددة في البند (6.7).
8. لا تنطبق الأحكام الواردة في الفقرة (3) و (6) من هذا البند في حال كانت البيانات التي سيتم مشاركتها بيانات مصنفة على مستوى عام.

6.7 الإطار الزمني لعملية مشاركة البيانات

1. يقوم المكتب بتقييم الطلب خلال فترة زمنية لا تتجاوز (10) أيام عمل من تاريخ استلام الطلب، وإشعار مقدم الطلب بالقرار على أن يكون القرار مكتوباً ومسبّباً.
2. في حال رفض طلب المشاركة، فيحق لمقدم الطلب استكمال المتطلبات وإعادة تقديم الطلب، وعلى المكتب إعادة تقييم الطلب وإصدار قراره خلال فترة زمنية لا تتجاوز (5) أيام عمل من تاريخ استلامه.
3. بعد الموافقة على عملية مشاركة البيانات، يقوم المكتب باستكمال ما نصت عليه الفقرة (6) من البند (6.6)؛ وذلك خلال (5) أيام عمل من تاريخ الموافقة، على أن تتم مشاركة البيانات المطلوبة مع مقدم الطلب خلال (10) أيام عمل من تاريخ الانتهاء من الإجراءات المنصوص عليها في الفقرة (6) من البند (6.6).
4. في حال كانت معالجة الطلب المقدم تتطلب جهداً غير عادي من الوزارة أو كانت طبيعة الطلب تقتضي مدداً أطول من المنصوص عليه في هذه السياسة، فيكون للوزارة تحديد مدد إضافية وإشعار مقدم الطلب بهذه المدة مع بيان السبب.
5. في حال عدم رد الوزارة خلال المدة المحددة المنصوص عليها في الفقرة رقم (1) من هذا البند، فيحق لمقدم الطلب تقديم إشعار خطي أو إلكتروني إلى المكتب، وعلى المكتب متابعة حالة الطلب ثم إشعار مقدم الطلب بمسببات التأخر بالرد وذلك خلال فترة زمنية لا تتجاوز (5) أيام عمل، وفي حال عدم رد الوزارة خلال هذه المدة فيكون لمقدم الطلب تقديم الإشعار إلى مكتب إدارة البيانات الوطنية للنظر فيه وفق ما نصت عليها الفقرة (3) من البند (6.8) من هذه السياسة.

6.8 الأدوار والمسؤوليات

1. يلتزم أطراف عملية مشاركة البيانات بأمن وحماية البيانات واستخدامها وفقاً للأغراض المحددة، بحسب ما نص عليه المبدأ (السابع) من هذه السياسة، ويحق للمكتب مراجعة مدى الالتزام بشكل دوري وفقاً للآليات التي يصدرها مكتب إدارة البيانات الوطنية.
2. يقوم المكتب بإعداد نماذج قياسية لكل من:
   أ. طلب مشاركة البيانات.
   ب. اتفاقية مشاركة البيانات.
   ت. الضوابط المشار إليها في الفقرة (7) من البند (6.3).
   ج. نموذج التفويض.
3. في حال وجود خلاف بين أطراف عملية مشاركة البيانات يتعلق بتنفيذ أحكام السياسة، يتم اللجوء لمكتب إدارة البيانات الوطنية لطلب بيان الرأي النظامي وفقا للآلية التي يحددها مكتب إدارة البيانات الوطنية..
4. في حال لم تتم معالجة الخلاف وفقاً للفقرة (3) من هذا البند، يقوم مكتب إدارة البيانات الوطنية باستكمال الإجراءات النظامية.
5. تلتزم أطراف عملية المشاركة بالمتطلبات النظامية والمتطلبات الأخرى ذوات الصلة المتعلقة بالإشعار عن حوادث تسرب البيانات.
6. في حال تضمن الطلب مشاركة بيانات شخصية فيتم مراعاة أحكام نظام حماية البيانات الشخصية ولوائحه التنفيذية وأحوال الإفصاح الواردة في النظام.
7. على الجهات الحكومية الاحتفاظ بسجلات خاصة بطلبات مشاركة البيانات والوثائق المرتبطة بها ولمدة خمس سنوات من انتهاء طلب المشاركة.
8. يجب على الوزارة إعداد ونشر سياسة لمشاركة البيانات الخاصة بها.
9. على الوزارة نشر بيانات التواصل المعتمدة للمكتب ولذلك لتمكين تقديم طلبات المشاركة من خلالها.
10. على الوزارة اتخاذ الوسائل الفنية والإدارية والتنظيمية اللازمة لضمان سرعة الاستجابة لطلبات مشاركة البيانات للالتزام بالإطار الزمني الموضح في البند (6.7)، على سبيل المثال إعداد أدلة إجرائية داخلية للاستجابة لطلبات مشاركة البيانات واتفاقيات مستوى الخدمة، ومصفوفة الصلاحيات.

11. يقوم المكتب بمتابعة الالتزام بأحكام هذه السياسة، وللمكتب الاستعانة بأي جهة خارجية لمتابعة الالتزام وفق الآلية التي يحددها.

سياسة حرية المعلومات

7 سياسة حرّية المعلومات

7.1 نطاق السّياسة

تنطبق هذه السّياسة على جميع طلبات الأفراد للاطّلاع أو الحصول على المعلومات العامّة - غير المحميّة - التي تنتجها جهة التحكم وجهة المعالجة.

لا تنطبق أحكام هذه السّياسة على المعلومات المحميّة التالية:

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

7.2 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.

7.3 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.

7.4 الخطوات الرّئيسيّة للاطلاع على المعلومات أو الحصول عليها

7.4.1 المتطلّبات الرّئيسيّة لطلبات الوصول إلى المعلومات العامّة أو الحصول عليها:

1. طلب خطّي أو الكتروني.

2. تعبئة "نموذج طلب معلومات عامّة" المعتمد من قبل الوزارة.
3. أن يكون الطّلب لأغراض الوصول إلى المعلومات العامّة أو الحصول عليها.
4. تضمين نموذج الطّلب على تفاصيل حول كيفيّة إرسال القرار النّهائي والإشعارات إلى الفرد (العنوان الوطني أو البريد الالكتروني أو الموقع... إلخ).
5. إرسال نموذج الطّلب مباشرة إلى الوزارة.

7.4.2 الخطوات الرّئيسية لطلب الاطّلاع أو الحصول على المعلومات العامّة:

أوّلاً: يتمّ تقديم الطّلبات عن طريق تعبئة "نموذج طلب معلومات عامّة" - إلكتروني أو ورقي – وتقديمه للمكتب 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 (30 يومًا) من استلام طلب الاطّلاع أو الحصول على المعلومات العامّة، باتخاذ أحد القرارات الآتية:

1. **الموافقة:** في حال تمّت موافقة الوزارة على طلب الوصول إلى المعلومات أو الحصول عليها كلّيًا أو جزئيًا؛ فيجب إشعار الفرد خطيّاً أو إلكترونياً بالرّسوم المطبّقة، ومن ثمّ إتاحة هذه المعلومات للفرد خلال فترة زمنيّة لا تتجاوز (10) أيام عمل من استلام المبلغ.
2. **الرّفض:** في حال تمّ رفض طلب الوصول إلى المعلومات أو الحصول عليها، فيجب أن يكون الرّفض خطيّاً أو إلكترونياً 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.
3. **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 (30) 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.
4. **الإشعار:** في حال كانت المعلومات المطلوبة متاحة على موقع الوزارة، أو ليست من اختصاصها، فيجب على المكتب إشعار الفرد بذلك خطيّاً أو إلكترونياً 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 إلكتروني بالتظلّم إلى المكتب خلال فترة زمنيّة لا تتجاوز (10) أيام عمل من استلامه قرار الرّفض، ويقوم المكتب (أو اللّجنة المشكّلة لهذا الغرض) بمراجعة الطّلب واتخاذ القرار المناسب وإشعار الفرد برسوم المراجعة - يتمّ استرجاعها في حال الموافقة على الطّلب - وقرار الاستئناف.

7.5 أحكام عامّة

1. على المكتب إعداد وتطبيق السّياسات والإجراءات المتعلّقة بممارسة حقّ الوصول إلى المعلومات العامّة أو الحصول عليها، ويكون المسؤول الاول بالوزارة -أو من يفوضه- مسؤول عن الموافقة عليها واعتمادها.
2. على المكتب تطوير وتوثيق ومراقبة تنفيذ السّياسات والإجراءات المعتمدة من المسؤول الأول بالوزارة -أو 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.
3. على المكتب مواءمة هذه السّياسة مع وثائق الوزارة التّنظيميّة - السّياسات والإجراءات - وتعميمها على جميع الجهات التّابعة لها أو المرتبطة بها بما يحقّق التّكامل ويضمن تحقيق الهدف المنشود من إعدادها.

4. على المكتب موازنة حقّ الاطّلاع والحصول على المعلومات مع المتطلّبات الضّرورية الأخرى كتحقيق الأمن الوطنيّ والمحافظة على خصوصيّة البيانات الشّخصيّة.
5. على المكتب متابعة وتوثيق الامتثال لهذه السّياسة بشكل دوري وفقاً للآليات والإجراءات التي تحدّدها الوزارة بعد التّنسيق مع مكتب إدارة البيانات الوطنيّة.
6. على المكتب - بعد التّنسيق مع مكتب إدارة البيانات الوطنيّة - إعداد الآليات والإجراءات والضّوابط المتعلّقة بمعالجة الشّكاوى وفقاً لإطار زمني محدّد وحسب التّسلسل التّنظيمي.
7. 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.
8. يجب على المكتب عند تعاقد الوزارة مع جهات أخرى - كالشّركات التي تقوم بمباشرة خدمات عامّة - أن يتحقّق من التزام الجهات الأخرى لهذه السّياسة وفقاً للآليّات والإجراءات التي تحدّدها الوزارة، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها الجهات الأخرى.
9. يحقّ للوزارة وضع قواعد إضافيّة لمعالجة الطّلبات المتعلّقة بأنواع محدّدة من المعلومات العامّة وفقاً لطبيعتها وحساسيّتها بعد التّنسيق مع مكتب إدارة البيانات الوطنيّة.
10. يقوم المكتب بالتّنسيق مع الجهات ذات العلاقة بالوزارة بإعداد نماذج للاطّلاع أو الحصول على المعلومات العامّة - سواء أكانت ورقيّة أو إلكترونية - يحدّد فيها المعلومات اللّازمة والوسائل الممكنة لتقديم المعلومات المطلوبة.
11. تحديد وتوفير الوسائل الممكنة (نموذج طلب المعلومات العامّة) - سواءً كانت ورقيّة أو إلكترونية - والتي من خلالها يمكن للفرد طلب الاطّلاع على المعلومات العامّة أو الحصول عليها.
12. التحقق من هويّة الأفراد قبل منحهم حقّ الاطّلاع على المعلومات العامّة أو الحصول عليها وفقاً للضّوابط المعتمدة من قبل الهيئة الوطنية للأمن السّيبراني والجهات ذات العلاقة.
13. 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 القيمة من البيانات.
14. 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.
15. على المكتب إعداد وتوثيق سياسات وإجراءات الاحتفاظ بسجلات الطّلبات والتّخلّص منها وفقاً للأنظمة والتّشريعات ذات العلاقة بأعمال وأنشطة الوزارة.
16. 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 أو مكتب إدارة البيانات الوطنيّة حسب التسلسل الإداري وفقاً للفترة الزمنيّة المحدّدة لمعالجة الطّلبات.
17. 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 (15) يوم من اتخاذ القرار.
18. على المكتب بالتّعاون مع الجهات ذات العلاقة بإعداد برامج توعوية لتعزيز ثقافة الشّفافيّة ورفع مستوى الوعي وفقاً لسياسات وإجراءات حريّة المعلومات المعتمدة من المسؤول الأول بالوزارة -أو من يفوضه-.
19. على المكتب مراقبة الامتثال لسياسات وإجراءات حريّة المعلومات بشكل دوري ويتمّ عرضها على المسؤول الأول بالوزارة -أو من يفوضه- كما يتمّ تحديد وتوثيق الإجراءات التّصحيحيّة التي سيتمّ اتخاذها في حال عدم الامتثال.

سياسة البيانات المفتوحة

8 سياسة البيانات المفتوحة

8.1 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.

8.2 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 التّميز

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 الثامن: 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.

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

8.4 القواعد العامّة للبيانات المفتوحة

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

1. التّخطيط للبيانات المفتوحة.
2. تحديد البيانات المفتوحة.
3. نشر البيانات المفتوحة.
4. تحديث البيانات المفتوحة.
5. متابعة أداء البيانات المفتوحة.

8.4.1 التّخطيط للبيانات المفتوحة

1. 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.
2. 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.
3. 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 وجودتها 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.

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

8.4.2 تحديد البيانات المفتوحة

1. تحديد جميع البيانات المصنّفة على أنّها بيانات عامّة بصفة منتظمة وتقييم مدى أولويّة كل مجموعة من مجموعات البيانات المحدّدة لنشرها كبيانات مفتوحة.
2. 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.
3. تسجيل البيانات الوصفيّة (Metadata) لمجموعات البيانات المفتوحة المحدّدة ونشرها.
4. 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.

8.4.3 نشر البيانات المفتوحة

1. نشر مجموعات البيانات المفتوحة على المنصّة الوطنيّة للبيانات المفتوحة.
2. 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.
3. توفير البيانات بعدّة صيغ كلما أمكن.

8.4.4 تحديث البيانات المفتوحة

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

8.4.5 متابعة أداء البيانات المفتوحة

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

8.5 الأدوار والمسؤوليّات

تحدّد سياسة البيانات المفتوحة الأدوار والمسؤوليّات التّالية على مستوى الوزارة مع الأخذ في الاعتبار أدوار ومسؤوليات مكتب إدارة البيانات الوطنيّة - التي نصّت عليها سياسات حوكمة البيانات الوطنيّة - بصفته 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.
تتحمل الجهات المختصة بالوزارة المسؤوليّة الأساسيّة المتعلّقة بأنشطة البيانات المفتوحة لدى الوزارة حسب الاختصاص.

- **المسؤول الأوّل بالوزارة (أو من يفوضه):** يعد المسؤول الأوّل بالوزارة - أو من يفوّضه - هو الشخص المسؤول عن الممارسات المتعلّقة بالبيانات المفتوحة داخل الوزارة، وتشمل مسؤولياته:
  1. **اعتماد خطّة البيانات المفتوحة:** الموافقة على تنفيذ خطّة البيانات المفتوحة لدى الوزارة والإشراف عليها.
  2. **تخصيص الأدوار المتعلّقة بالبيانات المفتوحة:** تخصيص الأدوار المختلفة المتعلّقة بالبيانات المفتوحة.
  3. **اعتماد التّقرير السنوي للبيانات المفتوحة:** اعتماد التّقرير السنوي للبيانات المفتوحة الذي يُعدّه المكتب.
- **مدير عام مكتب إدارة البيانات بالوزارة:** يعتبر المدير الاستراتيجي للعمليّات المتعلّقة بالبيانات المفتوحة في الوزارة، وتتضمّن مسؤولياته ما يلي:
  1. **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 خطة البيانات المفتوحة.
  2. **الإشراف على البيانات المفتوحة:** مراجعة أنشطة تحديد البيانات المفتوحة وترتيبها بحسب الأولويّة والموافقة على نشرها وضمان تنفيذ أنشطة تحديثها.
  3. **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.
  4. **التّنسيق مع مكتب إدارة البيانات الوطنيّة:** يُعدّ مدير عام 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:

1. **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 اعتماد المسؤول الأوّل بالوزارة (أو من يفوّضه).
2. **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.
3. **جمع طلبات البيانات المفتوحة:** مراجعة الملاحظات على البيانات المفتوحة ذات الصّلة بالوزارة وتسجيل وتحليل طلبات نشر البيانات المحدّدة كبيانات مفتوحة.
4. **التّثقيف والتّوعية بالبيانات المفتوحة:** تثقيف موظفي الوزارة وتوعيتهم بشأن البيانات المفتوحة ودعم حملات التّوعية الوطنيّة بالتّنسيق مع مدير عام المكتب.
5. **التّنسيق مع مكتب إدارة البيانات الوطنيّة (بشكل ثانوي):** يقوم مسؤول البيانات المفتوحة والمعلومات بالتّنسيق مع مكتب إدارة البيانات الوطنيّة عند الحاجة كمستوى ثانٍ.

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

1. **التّصديق على خطّة البيانات المفتوحة:** المساهمة في تطوير خطّة البيانات المفتوحة وإدارة الفرق المسؤولة عن تنفيذ الخطّة بالتّنسيق مع مسؤول البيانات المفتوحة.
2. **تحديد أولويّة البيانات المفتوحة:** تقديم المشورة إلى مسؤول البيانات المفتوحة بشأن قيمة مجموعات البيانات العامّة والاستثمارات المطلوبة لنشرها وتحديثها.
3. **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 :

1. **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.
2. **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.
3. **تحديث مجموعات البيانات المفتوحة:** تحديث مجموعات البيانات المفتوحة المنشورة والبيانات الوصفيّة ذات الصّلة.

8.6 الامتثال

يقوم المكتب بالوزارة بمراقبة الامتثال لسياسة البيانات المفتوحة.

8.6.1 شروط الامتثال

1. 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.
2. 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.

القواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية

9 القواعد العامة لنقل البيانات الشخصية خارج الحدود الجغر افية للمملكة

9.1 نطاق السّياسة

تنطبق أحكام هذه الوثيقة على جهة التحكم وجهة المعالجة والتي تقوم بنقل البيانات الشخصية إلى جهات أخرى خارج الحدود الجغرافية للمملكة بغرض معالجتها، ويستثنى من ذلك نقل البيانات الشخصية من وإلى الأفراد مباشرة.

9.2 حقوق أصحاب البيانات

إشارةً إلى سياسة حماية البيانات الشخصية، فإن المبادئ الأساسية للحماية تمنح الأفراد حقوقاً محددة فيما يتعلق بمعالجة بياناتهم الشخصية، بينما تحدد التزامات 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 إحاطته علماً بالمسوغ النظامي لجمع بياناته الشخصية والغرض من جمعها.

ثانياً: الحق في وصوله إلى بياناته الشخصية المتوافرة لدى الوزارة، وفق الضوابط والإجراءات التي تحددها اللوائح.

ثالثاً: الحق في طلب الحصول على بياناته الشخصية المتوافرة لدى الوزارة بصيغة مقروءة وواضحة، وفق الضوابط والإجراءات التي تحددها اللوائح.

رابعاً: الحق في طلب تصحيح بياناته الشخصية المتوافرة لدى الوزارة، أو إتمامها، أو تحديثها.

خامساً: الحق في طلب إتلاف بياناته الشخصية المتوافرة لدى الوزارة مما انتهت الحاجة إليه منها.

9.3 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:

1. 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 المكتب التنسيق مع مكتب إدارة البيانات الوطنية.
2. إذا كانت جهة المعالجة الخارجية في دولة ليست ضمن قائمة الاعتماد، فإن نقل البيانات الشخصية خارج الحدود الجغرافية للمملكة يتطلب مستوى كافٍ من الحماية – لا يقل عن مستوى الحماية الذي كفله نظام حماية البيانات الشخصية- بعد إجراء تقييم مستوى الحماية التي توفرها جهة المعالجة الخارجية.
3. إذا لم يكن هناك مستوى كافٍ من الحماية، فتقوم الوزارة بوضع ضمانات مناسبة لحماية حقوق أصحاب البيانات، ومنها على سبيل المثال، استخدام البنود القياسية، أو القواعد الملزمة.
4. إذا لم تتمكن الوزارة من توفير الضمانات الكافية، فيمكن الاعتماد على أحد الاستثناءات النظامية التي تتطلب نقل البيانات والموضحة في البند (ثالثاً) أدناه.

في جميع الحالات الواردة في الفقرات (2) و (3) و(4) أعلاه، يجب على جهة المعالجة الداخلية داخل الوزارة الحصول على موافقة كتابية من المسؤول الأول بالوزارة على نقل البيانات، وعلى المكتب 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 الحساسة يتطلب 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 الوزارة للأمن السيبراني 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 أو المنظمة الدولية – 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 أو المنظمة الدولية– 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 الجهة المختصة داخل الوزارة بالاستعانة بأطراف خارجية مستقلة تتولى إصدار شهادات اعتماد تؤكد وجود الضمانات المناسبة التي توفرها 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 هذه الاتفاقية بنوداً تعاقدية ملزمة تضمن المحافظة على خصوصية أصحاب البيانات وتحمي حقوقهم.

ثالثاً: الاستثناءات لحالات محددة

1- مع مراعاة ما ورد في الفقرة (2) يجوز للجهة المختصة داخل الوزارة نقل البيانات الشخصية إلى خارج المملكة أو الإفصاح عنها لجهة خارج المملكة، وذلك لتحقيق أي من الأغراض الآتية:
   أ- إذا كان ذلك تنفيذاً لالتزام بموجب اتفاقية تكون المملكة طرفاً فيه.
   ب- إذا كان ذلك لخدمة مصالح المملكة.
   ج- إذا كان ذلك تنفيذاً لالتزام يكون صاحب البيانات الشخصية طرفاً فيه.
   د- إذا كان ذلك تنفيذاً لأغراض أخرى وفق ما تحدده اللوائح.
2- تكون الشروط الواجب توافرها عند نقل البيانات الشخصية أو الإفصاح عنها –وفق ما ورد في الفقرة (1) من هذه المادة-على النحو الآتي:
   أ- ألا يترتب على النقل أو الإفصاح مساس بالأمن الوطني أو بمصالح المملكة الحيوية.
   ب- أن يتوافر مستوى مناسب لحماية البيانات الشخصية في خارج المملكة؛ بما لا يقل عن مستوى الحماية المقرر في النظام واللوائح، وفقاً لنتائج تقويم تجربة الجهة المختصة في هذا الشأن بالتنسيق مع من تراه من الجهات المعنية.
   ج- أن يقتصر النقل أو الإفصاح على الحد الأدنى من البيانات الشخصية الذي تدعو الحاجة إليه.
3- لا يسري ما ورد في الفقرة (2) على حالات الضرورة القصوى للمحافظة على حياة صاحب البيانات الشخصية أو مصالحه الحيوية أو الوقاية من عدوى مرضية أو فحصها أو معالجتها.
4- تحدد اللوائح والأحكام والمعايير والإجراءات المتعلقة بتطبيق ما ورد في هذه المادة، بما في ذلك تحديد حالات إعفاء جهات التحكم من الالتزام بأي من الشروط المشار إليها في الفقرتين الفرعيتين (ب) و (ج) من الفقرة (2)، وكذلك ضوابط وإجراءات ذلك الإعفاء والعدول عنه.

9.4 أحكام عامة

1. يتولى المكتب 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.
2. يقوم المكتب بمراقبة امتثال الجهات التابعة للوزارة أو المرتبطة بهذه القواعد بشكل دوري.
3. يجب على جهة التحكم وجهة المعالجة الامتثال لهذه القواعد وتوثيق الامتثال وفقاً للآليات والإجراءات التي يحددها المكتب.
4. يجب على جهة التحكم عند تعاقدها مع جهات المعالجة – داخل أو خارج المملكة – أن تتحقق من امتثال جهات المعالجة لهذه القواعد وفقاً للآليات والإجراءات التي يحددها المكتب، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها جهات المعالجة.
5. يحق للوزارة وضع قواعد إضافية لنقل أنواع محددة من البيانات الشخصية وفقاً لطبيعة وحساسية هذه البيانات بعد التنسيق مع مكتب إدارة البيانات الوطنية.

سياسة إدارة المحتوى والوثائق

10 سياسة إدارة المحتوى والوثائق

10.1 الهدف

تهدف سياسة إدارة المحتوى والوثائق الى ضمان أن المستندات التي تم إنشاؤها من قبل وزارة التعليم، وكل ما يتعلق بعملياتها، تتم إدارتها وصيانتها بشكل مناسب من خلال إدارة دورة حياة البيانات للمستندات والمحتوى داخل الوزارة والقطاعات التابعة لها.

- يجب أن تضمن السياسة صحة اصطلاحات تسمية المستندات، وأن تكون أسماء المستندات واضحة وخالية من الغموض.
- تلبية المتطلبات الداخلية للوزارة.

10.2 نطاق السياسة

تنطبق أحكام هذه السياسة على جميع القطاعات التابعة للوزارة التي تقوم بإنشاء المستندات والوثائق، أو الجهات التي تستلم الوثائق من مصادر خارجية، أو الجهات التي تقوم بمعالجة الوثائق.

10.3 بيان السياسة

تتضمن هذه السياسة العناصر الرئيسية لإدارة دورة حياة الوثائق والمحتوى، وهي كالتالي:

10.4 المبادئ الرئيسية لإدارة المحتوى والوثائق

المبدأ الأول: مشاركة خبراء إدارة الوثائق

يجب على الخبراء المسؤولين عن الوثائق أن يشاركوا مشاركة تامة وفعالة في تطوير السياسات والمعايير، وفي التخطيط لعمليات إدارة الوثائق والمحفوظات.

المبدأ الثاني: الملكية

تُحدد مرجعية الوثائق والمحفوظات بنفس طريقة تحديد مرجعية البيانات ويتم تعيين ممثلين لوثائق الإدارات والأقسام المختلفة في الوزارة.

المبدأ الثالث: المرونة وسهولة الوصول

ضمان كفاءة، وسهولة، وفعالية استرجاع واستخدام الوثائق المخزنة خارج قواعد بيانات الوزارة.

المبدأ الرابع: متابعة الامتثال

يقوم المكتب بمتابعة امتثال مركز الوثائق والمحفوظات لبنود سياسة إدارة المحتوى والوثائق وضوابط إدارة البيانات الوطنية في مجال إدارة المحتوى والوثائق.

المبدأ الخامس: موثوقية البيانات

تحقيق ثقة المستفيدين في البيانات بين مختلف الأطراف المشاركة من خلال رفع جودتها وصحتها.

10.5 الأدواروالمسؤوليات المتعلقة بإدارة المحتوى والوثائق

تُحدّد سياسة إدارة المحتوى والوثائق الأدوار والمسؤوليّات التّالية على مستوى الوزارة:

- **مدير عام مكتب إدارة البيانات:**

1. تسريع القرارات، ومعالجة الخلافات، وتصعيد المشكلات (متى ما أمكن ذلك) لتجنب حالات تعطل العمل.
2. الإشراف على أعمال حوكمة البيانات كأنشطة معتادة.

- **مالك الوثيقة:**

1. مسؤول عن إنشاء الوثيقة وتسميتها وتحديد مستوى تصنيف الوثيقة.
2. مسؤول عن عن تحديد الجهات المخول لها بالوصول إلى الوثيقة.

- **ممثل بيانات الأعمال:**

هو الشخص المسؤول عن إنشاء وتحديث البيانات الوصفية الضرورية للوثيقة في كل إدارة داخل الوزارة.

- **مسؤول الأرشفة:**

هو الشخص المسؤول عن عملية أرشفة البيانات بحسب معايير الجودة، وهو مسؤول عن استرجاع البيانات والتأكد من توفر النسخ الاحتياطية لها وتحديث الإصدارات عند الحاجة.

10.6 اصطلاحات تسمية الوثائق المستخدمة

1. يجب على مركز الوثائق والمحفوظات تحديد أسماء الوثائق في الوزارة والعمر الزمني لها، والمدة التي تكون فيها نشطة أو غير نشطة.
2. يضع مركز الوثائق والمحفوظات البيانات الوصفية المناسبة للوثائق والتي تستخدم في قوائم الوثائق وتتكون من الحقول التالية كحد أدنى:
   - اسم الوثيقة.
   - نسخة الوثيقة.
   - وصف الوثيقة.
   - فئة الحفظ.
   - مكان الحفظ.
   - بداية الحفظ.
   - مدة الحفظ.

يجب على مركز الوثائق والمحفوظات اتباع النسق المعياري التالي عند تسمية الوثيقة: <حالة الوثيقة>_<اسم الوثيقة>_<رقم نسخة الوثيقة>_الحروف الأولى من اسم المؤلف أو المراجع. مثال: مسودة_سياسة إدارة المحتوى والوثائق_نسخة 1.1 _ أ س.

10.7 تصنيف الوثائق

1. يجب على مركز الوثائق والمحفوظات اتباع التصانيف التالية عند تصنيف أنواع الوثائق من حيث مدد الحفظ:
   - وثائق دائمة الحفظ: وهي التي لا يستغنى عنها مع مرور الزمن لأهميتها وحاجتها.
   - وثائق مؤقتة الحفظ: وهي التي تتناقص قيمتها مع مرور الزمن حتى تنعدم.
2. يجب على مركز الوثائق والمحفوظات حفظ الوثائق التالية حفظاً دائماً:
   - الوثائق التي تثبت أملاك الوزارة الخاصة.
   - الوثائق التي تثبت أملاك الأشخاص الطبيعيين أو الاعتباريين.
   - الوثائق التي تحفظ حقوق الوزارة الطبيعية والقانونية الدائمة وحقوق الملكية الفكرية.
   - الوثائق التي تثبت حقوق الأشخاص تجاه الوزارة والغير.
   - الوثائق التي تؤرخ لوجود الوزارة وترصد تطورها الوظيفي والإداري، مثل:
     - الأنظمة واللوائح الداخلية.
     - القرارات التنظيمية.
     - السياسات والخطط والبرامج.
     - الميزانيات والحسابات الختامية.

- التنظيمات الإدارية والأدلة التنظيمية.
- التقارير المهمة كالتقرير السنوي وغيره.
- الإحصاءات.
- المخططات المعمارية والتصاميم الهندسية والمواصفات.
- مخططات ومواصفات المرافق.
- الأحكام القضائية.

- الوثائق الاخرى التي يرى مركز الوثائق والمحفوظات حفظها بشكل دائم بعد التنسيق مع ملاك الوثائق.

3. يجب على مركز الوثائق والمحفوظات حفظ الوثائق المؤقتة الحفظ (مثل: عقود العمل، عقود التجديد، صور شهادات الموظفين، التقارير الطبية، وغيرها) وفقاً للآتي:
   - الوثائق مؤقتة الحفظ يتم حفظها وإتلافها في الوزارة بعد انتهاء المدة الزمنية المقررة لحفظها.
   - تقدر أعمار الوثائق بالسنين، ويبدأ حساب السنة من بداية السنة التالية للواقعة التي تحدد بداية عمر الوثيقة.
   - يحتسب عمر الوثيقة بالسنة الميلادية التي تبدأ مع بداية شهر يناير وتنتهي بنهاية شهر ديسمبر.
   - إذا ألغي استخدام أي نوع من أنواع الوثائق، فلا يترتب على هذا الإلغاء إتلاف ما يوجد منه في الحفظ، وإنما يلتزم بالمدة الواردة في قوائم مدد الحفظ.
   - الوثيقة التي يتقرر إلغاء استخدامها من العمل وتزال من الملفات لانتهاء مدة حفظها، يتم حذفها من الطبعات الجديدة لقوائم مدد الحفظ (في حال الوثائق التخصصية).
   - تصور الوثائق مؤقتة الحفظ التي يزيد عمرها الزمني على عشرين عاماً باستخدام أحدث وسائل تصوير الوثائق كالتصوير الضوئي، وتربط هذه الصور بالحاسب الآلي.
4. يجب على مركز الوثائق والمحفوظات اتباع التصانيف الآتية عند تصنيف أنواع الوثائق من حيث درجة السرية إلى ثلاث أنواع:
   - وثائق سرية للغاية: الوثائق التي تؤدي معرفة بياناتها إلى الإضرار بأمن الدولة، ولا يجوز الاطلاع عليها عادة خلال مدة حظرها إلا من قبل المسؤولين المعنيين بمثل هذه الوثائق.
   - وثائق سرية جداً: الوثائق والمحفوظات التي يؤدي الاطلاع على بياناتها أو جزء منها إلى الإضرار بالمصالح العامة أو الخاصة.
   - وثائق سرية: الوثائق والمحفوظات التي تتعلق بمواضيع أو قضايا يترتب على الاطلاع عليها تأثيرات سلبية على الحياة الاجتماعية للجماعات أو الأفراد.

10.8 الوصول إلى الوثائق والمحتوى

1. يجب على مركز الوثائق والمحفوظات تقسيم الوثائق لأغراض الوصول والاطلاع عليها إلى فئتين:
   - **الفئة الأولى:** وثائق يجوز الاطلاع عليها وتداولها، وهي الوثائق التي تتعلق بموضوعات عامة غير مقيدة أو سرية تم نشرها أو تبليغها للجهات والأشخاص الاعتباريين أو الطبيعيين. ومن هذه الوثائق على سبيل المثال لا الحصر: الأنظمة واللوائح والسياسات والخطط والبرامج والميزانيات والإحصاءات والأبحاث والدراسات والتقارير الإحصائية.
   - **الفئة الثانية:** وثائق لا يجوز نشرها أو الاطلاع عليها أو تداولها لغير الموظفين المختصين إلا بموافقة صاحب الصلاحية بحكم سريتها أو حساسيتها أو أنه ليس من المصلحة الاطلاع عليها أو نشرها.
2. يجب على مركز الوثائق والمحفوظات اتباع الضوابط الآتية للموافقة على اطلاع الباحثين والدارسين على الوثائق المصنفة:
   - أن تكون هذه الوثائق والمحفوظات محتوية على بيانات أو معلومات صالحة للبحوث والدراسات في الموضوعات المراد بحثها.
   - إزالة أسماء الأشخاص الواردة في صور الوثائق والمحفوظات التي يزود بها الباحثين والدارسين قبل تمكينهم من الاطلاع عليها.
   - أن تكون مدة حظر الوثيقة قد انتهت.
   - أن يقدم الباحث أو الدارس خطاباً رسمياً من الجهة المشرفة على بحثه أو الجهة التي يتبع لها

- أن يشار في مصادر البحث إلى هذه الوثائق ومكان وجودها.
- أن يزود المركز الوطني للوثائق والمحفوظات بثلاث نسخ من هذا البحث ليتم إيداعها في مكتبته.

10.9 النسخ الاحتياطي واسترجاع الوثائق والمحتوى

1. يجب على تقنيّي وفنيّي البيانات إنشاء نسخ احتياطية كافية ومنتظمة لكافة الوثائق، بحيث تتضمن النسخ الاحتياطية:
   - إعداد نسخة احتياطية منعزلة: هي النسخة التي تشمل كافة الملفات والوثائق والمحفوظات، وتكون في مكان آمن وخارجي منعزل، وتكون شهرية.
   - إعداد نسخة احتياطية كاملة: هي النسخة التي تشمل كافة الملفات والوثائق والمحفوظات، وتكون محلية داخل الوزارة، وتكون أسبوعية.
   - إعداد نسخة احتياطية تزايديه: هي النسخة التي تشمل الوثائق والمحفوظات التي تم تخزينها بعد النسخة الاحتياطية الكاملة، وتحتوي على كافة الملفات والوثائق والمحفوظات التي تغيرت منذ إعداد النسخة الكاملة السابقة، وتكون محلية داخل الوزارة، وتكون يومية.
2. يجب على تقنيّي وفنيّي البيانات الاحتفاظ بسجلات لكافة عمليات النسخ الاحتياطي وتفاصيل الوثائق التي تم نسخها والمكان الذي تم إعداد النسخة الاحتياطية فيه.
3. يجب على تقنيّي وفنيّي البيانات اعتماد علامات مميزة لوثائق النسخة الاحتياطية.
4. يجب على تقنيّي وفنيّي البيانات القيام باختبارات استرجاع الوثائق والمحتويات من النسخ الاحتياطية، لضمان موثوقية النسخ الاحتياطية وإمكانية الاعتماد عليها عند الحاجة.

10.10 الاحتفاظ والتخلص من الوثائق والمحتوى

1. يجب على مركز الوثائق والمحفوظات إعداد قوائم مدد حفظ الوثائق الخاصة بالوزارة وذلك وفقاً للقوائم المنشورة من قبل المركز الوطني للوثائق والمحفوظات وذلك في "اللائحة الموحدة للوثائق والمحفوظات الإدارية"، و" لائحة الوثائق والمحفوظات المالية" و"تقويم الوثائق التخصصية".
2. يجب أن يأخذ ممثل بيانات الأعمال قوائم مدد حفظ الوثائق المعدّة من قبل مركز الوثائق والمحفوظات بعين الاعتبار أثناء إعداده للجدول الزمني الذي يحدد فترة الاحتفاظ الخاصة بالوثائق.
3. يتولى تقنيّو وفنيّو البيانات تنفيذ مبادرات التحول الرقمي للتحول من الوثائق الورقية في الوزارة إلى الوثائق الإلكترونية ولإدارة دورة حياة الوثائق من خلال نظام إلكتروني يدعم إدارة سير العمل.
4. يجب على مركز الوثائق والمحفوظات اتباع الضوابط الآتية عند التعامل مع الوثائق دائمة الحفظ:
   - وضع خطط للحفاظ على الوثائق واسترجاعها في مختلف الظروف والتوعية بشأن تداولها.
   - حفظ أصول الوثائق دائمة الحفظ في أوعية/حافظاتٍ خاصة مصممة لهذا الغرض وذلك لحمايتها من كل ما يعرضها للتلف.
   - ترميم هذه الأصول وتعقيمها قبل وضعها في أوعية الحفظ.
   - ترتيب هذه الأصول وتثبيتها وإيداعها في أوعية الحفظ دون حاجة لخرم أطرافها أو ما يعرض بعض أجزائها للتلف.
   - إيداع أوعية حفظ أصول الوثائق في خزائن أمنية مضادة للحريق وتوضع في أماكن آمنة، وتصور هذه الأصول بأحدث وسائل الحفظ المقاومة للتلف كالتصوير الضوئي على وسائط تخزين إلكترونية حديثة.
   - تجنب تداول أصول الوثائق دائمة الحفظ، وفي حال وُجدت الحاجة لذلك، يتم استخدام النسخ المصورة محل الوثائق الأصلية لضمان حفظها وسلامتها.
   - حفظ نسخ من صور أصول الوثائق دائمة الحفظ في أماكن مختلفة مناسبة لضمان سلامتها وحمايتها وسهولة استرجاعها.
5. يجب على مركز الوثائق والمحفوظات اتباع الضوابط الآتية عند الحفظ في ملفات الموضوعات:
   - يفتح ملف لكل موضوع حسب تصنيفه وفق التصنيف المعتمد لوثائق الوزارة، ويحدد تاريخ فتحه بتاريخ أول معاملة تحفظ فيه.
   - يوضع رمز الموضوع على أسفل الملف وعلى كل معاملة تحفظ بداخله.
   - يتم حصر الملف عند فتحه في سجل الملفات المفتوحة يدوياً والكترونياً.

- إذا كانت الموضوعات الفرعية للموضوع الأساسي قليلة الأوراق، توضع بملف واحد، ويفصل بين موضوعاتها بفواصل بلاستيكية، لكل فاصل منها بروز يوضع عليه رمز الموضوع الفرعي، كما تثبت رموز الموضوعات الفرعية على أسفل الملف.
- تحمى الأوراق داخل الملف ببطاقات مقواه تحت المعاملات وأعلاها.
- يحدد مقاس موحد لخرم الأوراق المسموح بخرمها.
- تخرم المعاملات بصورة تضمن المحافظة على كل الأوراق وسلامة محتوياتها.
- يتم الخرم من الناحية اليمنى من المعاملة في الهامش المخصص لهذا الغرض.
- ترتب المعاملات داخل الملف تصاعدياً حسب تواريخ وأرقام قيود الصادر والوارد، حيث يكون الأقدم أسفل والأحدث أعلى.
- لا يزيد عدد محتويات الملف من الوثائق عن القدر المناسب، ويحدد تاريخ قفل الملف على أسفله بتاريخ آخر معاملة حفظت فيه.
- لا يحفظ بالملف إلا المعاملات التي بت في موضوعها.
- يعمل فهرس لمحتويات كل ملف أو كل جزء من أجزاء الملف، إذا كان الملف يتكون من عدة أجزاء.
- ترقم المعاملات داخل الملف بذات الأرقام التي تعطى لها في فهرس الملف، ويوضع هذا الرقم في مكان محدد لا يؤثر على شكل المعاملة، ويكون واضحاً.
- يوضع دليل لتحديد أماكن الملفات، ويتحدد من خلاله مكان حفظ كل ملف ورقم الدولاب والرف الذي يحفظ فيه ورقم الملف، بحيث يمكن التعرف على مكان كل معاملة، ويكون ذلك يدوياً، كما يعمل إلكترونيا بالحاسب الآلي بعد تطوير البرنامج اللازم وإدخال المعلومات فيه.
- تتم حماية الملفات ومحتوياتها من كل ما قد يعرضها للتلف.
- يستخرج نسخ إضافية من هذه الصور وتحفظ في أماكن مختلفة مناسبة يتحقق فيها الأمن والسلامة لضمان سهولة الاسترجاع.

6. يجب على مركز الوثائق والمحفوظات اتباع الضوابط التالية عند حفظ ملفات الموظفين:
   - يفتح ملف لكل موظف حسب قواعد تصنيف ملفات الموظفين.
   - يوضع رقم ملف الموظف على الملف وعلى المعاملات التي تحفظ بداخله.
   - يحصر الملف عند فتحه في سجل الملفات المفتوحة يدوياً وآلياً.
   - يقسم ملف الموظف من الداخل إلى عدة أقسام تبعاً لاختلاف الموضوعات المحفوظة بداخله، ويكون على كل موضوع فاصل له بروز عليه اسم الموضوع.
   - ترتب ملفات الموظفين حسب ترتيب أرقامها، وتوضع في أرفف خاصة بها.
   - يوضع على كل رف رقم أول وآخر ملف فيه.
   - لا يتم حفظ المعاملة بالملف إلا بعد التأكد من استكمال الإجراءات الإدارية والفنية التي تسبق الحفظ.
7. يحفظ مركز الوثائق والمحفوظات الوثائق غير النشطة في وحدة للحفظ الوسيط بالوزارة وفق "لائحة الحفظ" الصادرة من المركز الوطني للوثائق والمحفوظات.
8. يقوم مركز الوثائق والمحفوظات بتعريف وتطبيق ضوابط أرشفة الوثائق والمحفوظات بالتوافق مع الضوابط الوطنية ذات العلاقة الصادرة عن المركز الوطني للوثائق والمحفوظات.
9. يجب على مركز الوثائق والمحفوظات تجهيز الوثائق أو المحفوظات للترحيل بحسب ما هو وارد في لوائح وتعليمات المركز الوطني للوثائق والمحفوظات والتعاميم الصادرة عنه في هذا الخصوص مع مراعاة الآتي:
   - يتم ترحيل الوثائق والمحفوظات وفقاً لقوائم مدد حفظها.
   - تبدأ عملية تجهيز الوثائق والمحفوظات للترحيل قبل نهاية العام الميلادي بشهرين.
   - تتم عملية الترحيل من الوزارة إلى المركز الوطني للوثائق والمحفوظات وفقاً لجدول زمني متفق عليه.
   - تشكيل لجان الترحيل من أربعة أعضاء؛ اثنان من الجهة المسلمة واثنان من الجهة المستلمة.
   - تقوم لجنة الترحيل بتطبيق الوثائق والمحفوظات والملفات والصناديق على بياناتها المكونة من نسختين والتوقيع عليها، مع احتفاظ كل جهة بنسختها.

- يكون الترحيل وفق النماذج المعدة لذلك من المركز الوطني للوثائق والمحفوظات.

10. يجب على مركز الوثائق والمحفوظات إتلاف الوثائق والأوراق الآتية:
    - الأوراق والوثائق التي انتهت مدة حفظها وفقاً لقوائم مدد الحفظ.
    - مخلفات المكاتب اليومية من الورق.
    - الأوراق والنسخ المكررة التي يتم الاستغناء عنها.
    - الصحف والمجلات والمطبوعات المكررة والتي يستغنى عنها.
11. يقوم مركز الوثائق والمحفوظات بتزويد المركز الوطني للوثائق والمحفوظات بنسخة من جداول الأوراق المتلفة ونسخة من بيان التسجيل والتسليم.
12. يحدد مركز الوثائق والمحفوظات مواعيد الإتلاف بحيث لا تتجاوز شهرين من بداية العام الميلادي الجديد.
13. يجب على مركز الوثائق والمحفوظات عند إتلاف الوثائق التي انتهت مدة حفظها القيام بالأمور الآتية:
    - استخراج الوثائق دائمة الحفظ التي قد تكون ضمن المرفقات كأصول الأوامر الملكية والأوامر السامية وصكوك الملكية ونحوها، وتسليمها للجهات المختصة بالطرق النظامية.
    - استخراج الأوراق التي عليها طوابع، أو أختام، أو تواقيع، أو شروحات مهمة لكبار المسؤولين، وتسليمها للمركز الوطني للوثائق والمحفوظات.
    - اختيار عينات من كل نوع من أنواع الوثائق المؤقتة الحفظ وتسليمها للمركز الوطني للوثائق والمحفوظات.
14. يجب على مركز الوثائق والمحفوظات إتلاف الوثائق التي انتهت مدة حفظها حسب اللوائح والأنظمة.
15. يضع مركز الوثائق والمحفوظات مخلفات الأوراق المتلفة لكل نوع من هذه الأنواع في أكياس بلاستيكية، وتوزن.
16. يسجل مركز الوثائق والمحفوظات أكياس الأوراق المتلفة في بيانات ذات تسلسل واحد من بداية العام حتى نهايته، وتستخدم هذه البيانات في عملية التسليم، وتشمل البيانات على الرقم المسلسل للكيس ونوع الأوراق المتلفة، ووزن الكيس، والفترة الزمنية التي تتعلق بها الأوراق، ويدون اسم المستلم وتوقيعه وتاريخ التسليم في أسفل البيان.
17. يتم إعداد جداول إحصائية شهرية عن الأوراق المتلفة، وتتضمن هذه الجداول أنواع الأوراق المتلفة ووزن كل نوع ومجموع هذه الأوزان ونسبة كل فئة من هذه الأنواع إلى المجموع العام.

10.11 إدارة تغيير الوثائق والرقابة على الإصدارات

يجب على مركز الوثائق والمحفوظات تطوير منهجية لإدارة تغيير الوثائق واتباعها للحفاظ على جودة الوثائق وتناسقها. وكما يجب عليه تحديد وتنفيذ ضوابط الرقابة على إصدارات وثائق وأدوات إدارة البيانات التي يتم إنشاؤها.

سياسة تحقيق القيمة من البيانات

11 سياسة تحقيق القيمة من البيانات

11.1 الهدف

تحقيق الإيرادات من البيانات، هو تمكّن الوزارة من الاستفادة من البيانات لكسب فوائد مالية واقتصادية واجتماعية قابلة للقياس، وذلك من خلال إنشاء منتجات أو خدمات بيانات حكومية ذات مردود يساعد في عملية اتخاذ القرار وتحقيق الطموحات، ومردود اقتصادي من خلال تحسين العمليات أو خفض التكاليف أو تنويع مصادر الدخل مما يسهم في النهضة التنموية.

ونظرًا لأن بيانات كل جهة فريدة عن نفسها، يجب أن يبدأ منهج تقييم البيانات توضيح فئات التكلفة والمزايا العامة التي يمكن تطبيقها باستمرار داخل الوزارة، تشمل فئات العينات ما يلي:

- تكلفة الحصول على البيانات وتخزينها.
- تكلفة استبدال البيانات في حالة فقدانها.
- التأثير على الوزارة إذا كانت البيانات مفقودة.
- تكلفة تخفيف المخاطر والتكلفة المحتملة للمخاطر المرتبطة بالبيانات.
- تكلفة تجويد البيانات وتحسين آليات عرضها وتقديمها.
- ما الذي يقدمه طالبوا البيانات مقابل البيانات.
- ما هي البيانات التي يمكن بيعها.
- الإيرادات المتوقعة من الاستخدامات المبتكرة للبيانات.

11.2 نطاق السياسة

تنطبق أحكام هذه السياسة على أي تسويق للبيانات التي تصدرها وزارة التعليم أو المنتجات المبنية على هذه البيانات المعالجة جزئياً أو كلياً، وتندرج تحتها كافة التطبيقات والبرامج والخدمات التابعة للوزارة.

11.3 المبادئ الرئيسية لتحقيق القيمة من البيانات

المبدأ الأول: البيانات أصول وطنية

تعتبر البيانات التي تنتجها الوزارة أحد الأصول الوطنية التي ينبغي أن تديرها الوزارة بما يحقق المصلحة العامة، تعد المعلومات والبيانات الحكومية ثروة وطنية يجب على الوزارة تنميتها، وضمان المحافظة عليها بصفتها أصول وطنية، وتحتفظ الوزارة بحقوق الملكية الفكرية الخاصة بالبيانات ولا يجوز استخدامها من قبل أي جهة أخرى إلا بموجب اتفاقية مشاركة البيانات بين الجهتين.

أما ما يتعلق بمنتجات البيانات، فيتوجب على الجهات الخارجية التي ترغب بتطوير منتجاً مبنياً على البيانات الاتفاق مع الوزارة بشأن تقاسم حقوق الملكية بين الأطراف أو احتفاظ الوزارة بكامل حقوق الملكية على هذه المنتجات.

المبدأ الثاني: تنمية الإيرادات

تعتبر البيانات أصولاً قيمة يمكن الاستفادة منها في رفع كفاءة الإنفاق وتنمية الإيرادات المتعلقة بالبيانات لضمان استدامة الخدمات التي تقدمها الوزارة.

المبدأ الثالث: الخصوصية بالتصميم

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

المبدأ الرابع: الأصل في البيانات الإتاحة

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

المبدأ الخامس: تعزيز ثقافة المشاركة

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

المبدأ السادس: منع الممارسات الاحتكارية

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

المبدأ السابع: الشفافية

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

المبدأ الثامن: استرداد التكاليف

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

11.4 الأدوار والمسؤوليات

- **إدارة دعم القرار وذكاء الأعمال (الإدارة العامة لقياس الأداء)**

1. تطوير متجر إلكتروني أو دليل يتضمن البيانات ومنتجات البيانات التي ترغب في تزويدها أو تقديمها.
2. تحديد نموذج التسعير التفصيلي لكل خدمة أو منتج وفقا للمسارات الموضحة أعلاه وإرسالها إلى صاحب الصلاحية بالوزارة.
3. إدارة محفظة حالات استخدام تحقيق القيمة من البيانات.

- **مكتب إدارة البيانات**

1. يقوم بمراجعة الخدمات والمنتجات المعروضة في المتجر او الدليل للتأكد من أن البيانات المراد تزويدها أو المستخدمة لتطوير منتجات البيانات مصنفة على مستوى مقيد او عام.
2. التحقق من استيفاء متطلبات الخصوصية وفقا لسياسة حماية البيانات الشخصية.
3. تحديد نماذج التسعير التفصيلية وفق المسارات الموضحة في هذه السياسة.
4. توثيق جميع طلبات مشاركة البيانات والقرارات المتعلقة بها في سجلات خاصة.

- **ممثل بيانات الأعمال**

1. تطوير الأعمال وتحقيق الإيرادات بالوزارة من خلال المشاركة بتطوير متجر إلكتروني أو دليل يتضمن البيانات ومنتجات البيانات التي ترغب الوزارة بتزويدها أو تقديمها وتحديد نموذج التسعير التفصيلي لكل خدمة أو منتج وفقاً للمسارات الموضحة في النماذج.
2. مراجعة الخدمات والمنتجات المعروضة في المتجر أو الدليل للتأكد من أن البيانات المراد تزويدها أو المستخدمة لتطوير منتجات البيانات مصنفة على مستوى مقيد أو عام، والتحقق من استيفاء متطلبات الخصوصية وفقاً لسياسة حماية البيانات الشخصية، وأن نماذج التسعير التفصيلية تم تحديدها وفقاً للمسارات الموضحة في هذه السياسة.
3. توثيق جميع طلبات مشاركة البيانات والقرارات المتعلقة بها في سجلات خاصة.

- **أمين البيانات**

1. يتحمل أمين البيانات المسؤولية عن تحديد المخاطر المحتملة المتعلقة بالبيانات بشكل مستمر ضمن مجموعة بيانات معينة تتم مشاركتها مع مقدم الطلب.
2. مسؤولية تنفيذ الإجراءات لضمان استخدام البيانات بفعّالية لتلبية احتياجات العمل الخاصة بالإدارة.
3. التحقق من الالتزام بأحكام سياسة مشاركة البيانات والقواعد العامة المنصوص عليها في سياسة تحقيق القيمة من البيانات.
4. يتولى أمين البيانات مسؤولية استخراج البيانات.

- **الجهات الحكومية والأفراد**

1. تقديم الطلبات للمكتب مثل مشاركة البيانات وفقاً للخطوات الموضحة في سياسة مشاركة البيانات.
2. يقوم المكتب بالتحقق من الالتزام بأحكام سياسة حوكمة البيانات وبالقواعد العامة المنصوص عليها في سياسة تحقيق القيمة من البيانات.

11.5 سياسة تحقيق القيمة من البيانات – القواعد العامة

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

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

11.6 نماذج تحقيق الإيرادات

نموذج تحقيق الإيرادات (Revenue Model) هو الهيكل الذي ينص على كسب الإيرادات الخاصة بنموذج العمل (Business Model) ويشمل المنتج أو الخدمة ذات القيمة المضافة والمستهلكين. هناك عدة نماذج شائعة، لكل نموذج منها يعتمد على استخدامات المستهدفين. بناءً على طبيعة المنتج أو الخدمة، منها على سبيل المثال لا الحصر: الإعانات، والميزة التنافسية، والتراخيص، والعمولة، وغيرها من النماذج الأخرى.

11.7 نماذج التسعير

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

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

ولتحقيق الهدف المقصود من هذه السياسة، يعتبر النموذجان المشار إليها في الفقرة (3) والفقرة (4) أعلاه هما نموذجا التسعير المعتمدان من مكتب إدارة البيانات الوطنية عند قيام الوزارة بتحقيق الإيرادات من البيانات أو منتجات البيانات.

11.8 إطارتحقيق الايرادات

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

- إتاحة أكبر قدر ممكن من البيانات المصنفة (على مستوى: عام) ونشرها على أنها بيانات مفتوحة –مجاناً وبدون مقابل– وفقاً لسياسة البيانات المفتوحة المعتمدة في الوزارة.
- تبادل البيانات التابعة لها وإتاحة البيانات المشتركة منها إلكترونياً مجاناً (دون مقابل) للجهات الحكومية الأخرى المستفيدة تنفيذاً للتنظيمات الصادرة من الجهات التنظيمية.

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

	البيانات غير المعالجة	منتجات البيانات
البيانات المفتوحة	مجاناً	استرداد التكاليف
البيانات المصنفة (مقيد، عام)	مجاناً	استرداد التكاليف

القواعد العامة المتعلقة بالمسار الأول:

- لا تفرض الوزارة رسوماً على البيانات غير المعالجة، سواء عند إتاحة البيانات المفتوحة أو عند مشاركة البيانات المصنفة (علّى مستوى: مقيد أو عام) مع الجهات الحكومية الأخرى لتنفيذ المهام والاختصاصات المنوطة بها. كما تضمن هذه القاعدة الالتزام بالأوامر من الجهات التنظيمية-

1. يمكن للوزارة أن تحقق إيرادات من منتجات البيانات المطورة من البيانات المفتوحة أو البيانات المصنفة (على مستوى: مقيد أو عام)، على أن تُقدم هذه المنتجات عن طريق الوزارة ويكون التسعير وفقاً لنموذج استرداد التكاليف المنصوص عليه في هذه السياسة.
2. تلتزم الوزارة بأحكام سياسة مشاركة البيانات ومتطلبات حماية البيانات الشخصية عند تطوير منتجات البيانات، ومنها على سبيل المثال إجراء المعالجة المسبقة للبيانات الشخصية قبل مشاركتها مثل: التعتيم (Data Masking) أو المزج (Data Scrambling) أو التعمية (Data Anonymization).
3. يجب على الوزارة أن تقدم –وفقا للمبدأ السادس– وصولاً متساويا لأي بيانات أو منتج بيانات يُستخدم لتحقيق القيمة من البيانات من قبل الجهات الخاصة وذلك لتحقيق المنافسة العادلة ومنع الممارسات الاحتكارية.

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

	البيانات غير المعالجة	منتجات البيانات
البيانات المفتوحة	مجاناً	استرداد التكاليف
البيانات المصنفة (مقيد، عام)	استرداد التكاليف	استرداد التكاليف (بلس)

القواعد العامة المتعلقة بالمسار الثاني:

1. لا تفرض الوزارة رسوماً على البيانات المفتوحة (غير المعالجة) التي تُتاح للعموم (الجهات الخاصة والأفراد).
2. يمكن للوزارة تحقيق إيرادات من منتجات البيانات المطّورة من البيانات المفتوحة، على أن تُقدم هذه المنتجات عن طريق الوزارة أو الجهات التابعة لها ويكون التسعير وفقاً لنموذج استرداد التكاليف المنصوص عليه في هذه السياسة.

3. يمكن الوزارة تحقيق إيرادات من البيانات غير المعالجة المصنفة (على مستوى: مقيد أو عام)، على أن تزود هذه البيانات عن طريق الوزارة أو الجهات التابعة لها ويكون التسعير وفقاً لنموذج استرداد التكاليف المنصوص عليه في هذه السياسة
4. يمكن للوزارة تحقيق قيمة من منتجات البيانات (البيانات المعالجة) المصنفة (على مسّتوى: مقيد أو عام)، على أن تقدم هذه المنتجات عن طريق الوزارة أو الجهات التابعة لها ويكون التسعير وفقاً لنموذج استرداد التكاليف (بلس) المنصوص عليه في هذه السياسة.
5. تلتزم الوزارة بأحكام سياسة مشاركة البيانات ومتطلبات نظام حماية البيانات الشخصية عند مشاركة البيانات غير المعالجة أو تطوير منتجات البيانات، ومنها على سبيل المثال إجراء المعالجة المسبقة للبيانات الشخصية قبل مشاركتها مع الجهات الخاصة أو الأفراد مثل التعتيم (Data Masking) أو المزج (Data Scrambling) أو التعمية (Data anonymization).
6. يجب على الوزارة أن تقدم –وفقا للمبدأ السادس– وصولاً متساويا لأي بيانات أو منتج بيانات يستخدم لتحقيق الإيرادات من قبل الجهات الخاصة أو الأفراد وذلك لتحقيق المنافسة العادلة ومنع الممارسات الاحتكارية.

المسار الثالث: الجدول أدناه يوضح التزامات الجهات الخاصة تجاه الوزارة والجهات الخاصة والأفراد (B2I/B2B/B2G)

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

القواعد العامة المتعلقة بالمسار الثالث:

1. يمكن للجهات الخاصة أن تحقق قيمة من منتجات البيانات المطورة من البيانات المفتوحة، علماً أنه لا يخضع تسعير منتجات البيانات لأحكام هذه السياسة، وإنما يخضع لنماذج التسعير الموصى بها.
2. لا يجوز للجهات الخاصة –في حال تم منحها ترخيص لاستخدام البيانات من قبل جهة حكومية– إعادة استخدام البيانات الحكومية غير المعالجة لأغراض غير الأغراض المحددة في اتفاقيات مشاركة البيانات أو مشاركتها مع الجهات أخرى سواء بمقابل مالي أو بدون مقابل. تنطبق هذه القاعدة على جميع الجهات الخاصة، بما في ذلك الاتفاقيات التجارية التي تحكم العلاقة بين الجهة الخاصة والوزارة.
3. يمكن للجهات الخاصة أن تحقق قيمة من البيانات غير المعالجة التي يتم الحصول عليها من الوزارة والمصنفة (على مستوى: مقيد أو عام) من خلال تطوير منتجات بيانات عليها (بعد الاتفاق مع الوزارة) ومشاركتها مع جهات حكومية أخرى والاتفاق على تقاسم الأرباح (إن وجد)، على أن يكون التسعير وفقاً لنموذج استرداد التكاليف المنصوص عليه في هذه السياسة.

4. يمكن للجهات الخاصة أن تحقق قيمة من منتجات البيانات التي يتم الحصول عليها من الوزارة المصنفة (مستوى: مقيد أو عام) عند تقديمها إلى جهات خاصة أخرى أو أفراد، على أن يكون التسعير وفقاً لنموذج استرداد التكاليف (بلس) المنصوص عليه في هذه السياسة والاتفاق على تقاسم الأرباح (إن وجد).

11.9 نموذج التسعير (استرداد التكاليف)

- **معايير تسعير البيانات**

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

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

- **آلية تسعير استرداد التكاليف**

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

1. يجب على الوزارة أخذ العوامل التالية بعين الاعتبار عند تسعير استرداد التكاليف (تحصيل):

السعر = تكاليف جمع البيانات + تكاليف التطوير

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

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

2. تتمتع الوزارة بالسلطة التقديرية لتسعير البيانات أو منتجات البيانات بأقل من استرداد التكلفة المقدّرة.
3. إذا رأت الوزارة دراسة إضافة هامش ربح أعلى من استرداد التكلفة، بناء على ذلك، يجب أخذ الموافقة من مكتب إدارة البيانات الوطنية بعد تزويده بالمبررات الكافية.
4. تحدد الوزارة سعر البيانات أو منتجات البيانات بشكل موحد بين المستفيدين من البيانات، كما يجب رفع أي استثناء إلى مكتب إدارة البيانات الوطنية للموافقة عليه.

11.10 أحكام عامة

أولاً: يتولى المكتب مواءمة أحكام هذه الوثيقة مع وثائقها التنظيمية- السياسات والإجراءات_ وتعميمها على جميع الجهات التابعة لها أو المرتبطة بها بما يحقق التكامل ويضمن تحقيق الهدف المنشود من إعدادها.

ثانياً: تلتزم الوزارة بتحديد أدوات المتابعة لتحصيل الإيرادات من البيانات –بما لا يتعارض مع نظام إيرادات الدولة– ومراقبة الامتثال لهذه السياسة وتزويد مكتب إدارة البيانات الوطنية بتقارير الامتثال بشكل دوري.

ثالثاً: يجب على الوزارة تحصيل جميع إيراداتها من البيانات الحكومية –سواء كانت بيانات غير معالجة أو منتجات بيانات– وتسجيلها في سجل مفصل بما لا يتعارض مع نظام إيرادات الدولة واللوائح التنفيذية.

رابعاً: تلتزم الوزارة بالحصول على موافقة رسمية وموثقة على أي إيراد يتعلق بالبيانات غير المعالجة أو منتجات البيانات من مسؤول الجهة أو من يفوضه.

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

سادساً: يحق للوزارة –بعد موافقة مكتب إدارة البيانات الوطنية– اقتراح إضافة بعض نماذج تحقيق الإيرادات ووضع معايير إضافية لتطوير نماذج التسعير وفقاً لطبيعة أنشطة الجهات التابعة لها أو المرتبطة بها.

سابعاً: تقوم الوزارة –بعد التنسيق مع مكتب إدارة البيانات الوطنية– بإعداد الآليات والإجراءات التي تنظم عملية معالجة الشكاوى والنزاعات المتعلقة بتحقيق الإيرادات وفقاً لإطار زمني محدد وحسب التسلسل التنظيمي.

سياسة ذكاء الأعمال

12 سياسة ذكاء الأعمال

12.1 الهدف

تهدف سياسة ذكاء الأعمال إلى تحسين اتخاذ القرارات حول توافر البيانات ومعالجتها وتقديمها بشكل مناسب لقطاع الأعمال وبشكل ملائم لبيئة العمل وذلك عن طريق إظهار البيانات التاريخية والحالية. ويعد ذكاء الأعمال مثالياً في تطوير وخلق فرص جديدة للمساعدة في توسيع الأعمال وخفض التكاليف إن أمكن.

12.2 نطاق السياسة

تنطبق أحكام هذه السياسة على وزارة التعليم وجميع الإدارات المرتبطة بها، والتي تقوم بجمع ومعالجة البيانات بشكل كلي أو جزئي وبأي وسيلة سواء كانت يدوية أو إلكترونية.

12.3 المبادئ الرئيسية لذكاء الأعمال

المبدأ الأول: البيانات أصل وطني

اعتبار البيانات أصلاً وطنياً يساهم في بناء تصور شمولي لجميع أصحاب المصلحة مع القدرة على ربط المعطيات من البيانات القيمة من جميع قطاعات الأعمال والنتيجة هي تحسين كفاءة الوزارة والجهات الحكومية الأخرى.

المبدأ الثاني: ثقافة البيانات

رفع ثقافة ووعي المجتمع حول إدارة البيانات وحماية البيانات الشخصية. وتعزيز القدرات الوطنية في الجهات.

المبدأ الثالث: موثوقية البيانات

أن تكون البيانات المعروضة ذات جودة وكفاءة يمكن الاعتماد عليها في عرض مؤشرات الأداء وموثوقة لمتخذي القرار وهي أيضا مسؤولية مشتركة من كل الأطراف المشاركين في مبادرات ذكاء الأعمال.

المبدأ الرابع: الاستخدام الأخلاقي للبيانات

أن تقوم جميع الأطراف المشاركة في مبادرات ذكاء الأعمال بتطبيق الممارسات الأخلاقية أثناء عملية تحميل البيانات ومعالجتها وتطوير المؤشرات لضمان استخدامها في إطار من العدالة والنزاهة والأمانة والاحترام، وعدم الاكتفاء بالالتزام بسياسات حماية البيانات أو الالتزام بالمتطلبات التنظيمية والتشريعية ذات العلاقة.

المبدأ الخامس: القرارات المبنية على البيانات

توفير البيانات وتحليلها لدعم متخذي القرار لاتخاذ قرارات فعالة على المستويات الاستراتيجية والتشغيلية وكافة الأصعدة.

المبدأ السادس: ضمان الاستمرار

العمل على تحديث البيانات ومؤشرات الأداء والوثائق الخاصة بنماذج البيانات ووصف المؤشرات والتغيرات الطارئة عليهم بشكل مستمر من أجل ضمان الوصول إلى الفائدة المطلوبة للمستخدمين.

12.4 الأدوار والمسؤوليات

- **مدير عام مكتب إدارة البيانات:**

1. تسريع القرارات، ومعالجة الخلافات، وتصعيد المشكلات (متى ما أمكن ذلك) لتجنب حالات تعطل العمل.
2. الإشراف على أعمال حوكمة البيانات كأنشطة معتادة.

- **مالك البيانات:**

1. يتحمل المسؤولية عن تحديث تفاصيل هيكلة البيانات فيما يتعلق بنطاقات البيانات الخاصة به.
2. يحدد نطاق وأنواع نماذج البيانات المفاهيمية المقرر إنشاؤها استنادًا إلى متطلبات العمل.

- **ممثل بيانات الأعمال:**

يتولى ممثل بيانات الأعمال المسؤولية عن وضع مسودة لنماذج البيانات بغرض مراجعتها واعتمادها من جانب المكتب للتأكد من اكتمالها وإمكانية إعادة استخدامها.

- **أمين البيانات:**

1. يتحمل أمين البيانات المسؤولية عن تنفيذ نماذج البيانات المادية على قواعد البيانات.
2. يتحمل أمين البيانات المسؤولية عن صيانة مخازن أنظمة البيانات، وإدارتها.

- **مختص بيانات الأعمال**

1. التأكد من تناسق النهج المتبع من جانب ممثل بيانات الأعمال وأمين البيانات في مختلف نطاقات البيانات.
2. إنشاء أو تعديل نظام أو خدمة.
3. رسم تخطيطي يشمل نماذج البيانات الثلاث (نموذج البيانات المفاهيمية، نموذج البيانات المنطقية، نموذج البيانات المادية).
4. إدخال وتوثيق البيانات الوصفية داخل نماذِج البيانات.
5. تعيين أبعاد جودة البيانات.
6. إنشاء قاعدة جودة البيانات في مستودع البيانات الوصفية.
7. وضع قواعد تنميط جودة البيانات وتحديثها.
8. إعداد تقرير تنميط البيانات، بالإضافة إلى تقرير تقييم جودة البيانات.

- **مسؤول إتاحة البيانات:**

مسؤول عن استقبال الطلبات من الأفراد والمؤسسات الخاصة بتطوير مؤشرات الأداء؛ ومن ثم إرسالها إلى ممثل بيانات الأعمال بعد الموافقة عليها.

- **مختص هيكلة البيانات**

1. وضع هيكل البيانات وتحديد احتياج بيئات العمل المختلفة من حيث المواصفات والممكنات المطلوبة.
2. تحديد أنواع النماذج المُراد إنشاؤها ومنها: (نماذج البيانات المفاهيمية، نماذج البيانات المنطقية، ونماذج البيانات المادية).
3. إنشاء نماذج البيانات المفاهيمية ومراجعة واعتماد كل نماذج البيانات المنطقية ونماذج البيانات المادية بعد إنشائها من قبل مختص نمذجة البيانات ثم إرسالها.
4. مراجعة واعتماد البيانات الوصفية لاعتمادها بعد توثيقها داخل النظام من قبل مختص بيانات الأعمال.

- **مختص نمذجة البيانات:**

الشخص المسؤول عن إنشاء نماذج البيانات المنطقية والمادية والمفاهيمية وإرسالها لمختص هيكلة البيانات لمراجعة النماذج واعتمادها.

- **مطورذكاء الأعمال**:

الشخص المسؤول عن تحليل متطلبات مستخدمي ذكاء الأعمال وتوثيقها، ويقوم بتطوير لوحات معلوماتية لمؤشرات الأداء المطلوبة وعمل تصور مبدئي لشكل المؤشرات.

- **مصمم جرافيك**:

الشخص المسؤول عن وضع تصميم للوحات المعلومات وما يخص الألوان والأشكال البيانية وعرضها على المستخدمين من قطاع الأعمال لمراجعتها واعتمادها.

- **محلل بيانات:**

تحليل مصادر البيانات ومعرفة الروابط، ويعطي تحليلاً مبدئياً عن جودة البيانات، ويقوم بتحميل البيانات ومعالجتها وتخزينها في نموذج البيانات المتفق عليه من قبل مختص نمذجة البيانات، ويقوم بتحليل مقترحات جودة البيانات من قبل ممثل بيانات الأعمال.

12.5 إرشادات عملية ذكاء الأعمال

1. يتم رفع طلبات ذكاء الأعمال داخل الوزارة إلكترونيا من خلال منصة طلبات البيانات.
2. يقوم (مسؤول طلبات تحليل البيانات) في إدارة دعم القرار وذكاء الأعمال باستقبال ودراسة طلبات لوحات البيانات ومؤشرات الأداء، وإحالتها لمحلل بيانات الأعمال المختص بقطاع الأعمال الذي قام برفع الطلب.
3. تقوم إدارة دعم القرار وذكاء الأعمال بإعداد خطط لتطوير لوحات ذكاء الأعمال واعتمادها من المكتب.
4. يتم توجيه نسخة من كل الطلبات ذكاء الأعمال إلى المكتب.
5. يقوم محلل بيانات الأعمال بالرجوع إلى مختص بيانات الأعمال وممثل بيانات الأعمال للوصول إلى البيانات المطلوبة لتطوير منتجات ذكاء الأعمال.
6. يقوم مهندسو ذكاء الأعمال بالمواءمة مع مختصي جودة البيانات للتأكد من جودة البيانات المستخدمة في تطوير منتجات ذكاء الأعمال.
7. في حال تم استحداث أو طلب تعديل على لوحة رقمية بعينها أو مؤشر أداء من قطاع الأعمال، يلزم ذلك التنسيق المباشر من قبل قطاع الأعمال مع مسؤول طلبات تحليل البيانات داخل إدارة دعم القرار وذكاء الأعمال.
8. يقوم مختص هيكلة البيانات بدراسة وتحليل أي متطلبات باستحداث أو تعديل نماذج بيانات مستودع البيانات.
9. يقوم محلل البيانات بتطوير عمليات سحب البيانات ومعالجتها وهو المسؤول عن إظهار مشاكل البيانات وأي مخاطر يمكن تواجدها في البيانات والتي يمكن أن تؤثر على مخرجات المؤشرات.
10. يتحمل مختص هيكلة البيانات مسؤولية وضع نماذج البيانات المفاهيمية لدعم طلب البيانات الخاصة بالتحليلات، كما يمكن وضع النموذج المفاهيمي من قبل مختص نمذجة البيانات ولكن يلزم ذلك مراجعتها من قبل مختص هيكلة البيانات.
11. يتحمل مختص هيكلة البيانات مسؤولية وضع نماذج البيانات المفاهيمية لدعم طلب البيانات الخاصة بالتحليلات.
12. يتحمل مختص نمذجة البيانات مسؤولية وضع نماذج البيانات المنطقية والمادية.
13. تقوم إدارة البنية المؤسسية بتعديل أو إنشاء هيكلة البيانات بمشاركة إدارة دعم القرار وذكاء الأعمال.
14. يتحمل مطور ذكاء الأعمال المسؤولية عن تطوير لوحة المعلومات الرقمية أو تعديلها بناءً على متطلبات قطاع الأعمال.
15. يتحمل مصمم اللوحات (مصمم جرافيك) المسؤولية عن وضع تصميم اللوحة المبدئي (Mockups) والتصميم النهائي، والاستجابة لأي تعديل على التصميم يتم طرحه من جهة قطاع الأعمال.
16. يجب اتباع قالب موحد في تصميم اللوحات من حيث الألوان ونوع الخطوط والمتفق عليها من قبل إدارة دعم القرار وذكاء الأعمال.

17. يتم عرض جميع اللوحات الرقمية ومؤشرات الأداء داخل الوزارة من خلال منصة موحدة لذكاء الأعمال.
18. إدارة دعم القرار وذكاء الأعمال هي الجهة المسؤولة عن إنشاء وتعديل مصفوفة صلاحيات الوصول إلى منتجات ذكاء الأعمال.
19. يتم الرجوع إلى سجلات تصنيف البيانات لتحديد الأشخاص المصرح لهم بالاطلاع على البيانات المعروضة من خلال منتجات ذكاء الأعمال.
20. لا يجب عرض أي بيانات من خلال اللوحات تفصح عن البيانات الشخصية أو تضر بالجهات الحكومية أو الخاصة أو الأفراد.
21. تتحمل أي جهة تقوم بإصدار لوحات رقمية دون الرجوع إلى إدارة دعم القرار وذكاء الأعمال المسؤولية الكاملة تجاه تسرب أي بيانات شخصية أو الإفشاء عنها.
22. لا يتم عرض بيانات ذات جودة منخفضة حسب توجيه إدارة دعم القرار وذكاء الأعمال.
23. ترتيب وتقسيم الملفات في منصة ذكاء الأعمال يجب أن يكون وفقاً لمعايير إطار عمل ذكاء الأعمال والتحليلات الموحد.
24. مسميات الملفات واللوحات في منصة ذكاء الأعمال يجب أن تكون وفقاً لمعايير إطار عمل ذكاء الأعمال والتحليلات الموحد.
25. يجب أن يتم الوصول إلى لوحات المعلومات حسب إرشادات الإدارة العامة للأمن السيبراني ووفقاً لمصفوفة الصلاحيات الصادرة من إدارة دعم القرار وذكاء الأعمال.
26. يجب تعيين صلاحيات للمستخدمين المصرح لهم على مستوى كل من الملفات/ التقارير/ كل عنصر من عناصر البيانات.
27. يجب اتباع وتقديم حالات اختبار لكل لوحة يتم تقديمها كالتالي:
    - اختبار صحة البيانات وذلك بتقديم حالات اختبار وكيفية تقديم أدلة وإثباتات عن صحة البيانات المقدمة.
    - اختبار تكامل البيانات، إذا كان هناك تكامل بيانات بين مصادر بيانات لوحة المعلومات.
    - اختبار اللوحات والمؤشرات الوظيفية للتأكد من صحة تشغيل كل اللوحات وعناصرها المختلفة.
28. يجب تقديم وثيقة تقنية تشمل كل الجوانب المطلوبة كالتالي:
    - مصادر البيانات (IP / Port).
    - الهدف من اللوحات.
    - الجهة المسؤولة أو الطالبة.
29. ضمان وجود دعم تنفيذي لإطار عمل ذكاء الأعمال والتحليلات الموحد من داخل وخارج إدارة دعم القرار وذكاء الأعمال لاستدامة مخرجات ذكاء الأعمال وتنميتها.
30. يجب اتباع نماذج وقوالب ثابتة في أي عملية توثيق للمتطلبات وفي تنفيذ اللوحات والمؤشرات.
31. يجب إنشاء وثيقة تعريف باللوحة والغرض منها وتقديمها لإدارة دعم القرار وذكاء الأعمال.
32. يجب عقد ورش عمل تعريفية وتدريبية لجهات الوزارة المختلفة للتعرف على مجال ذكاء الأعمال وكيفية التعامل مع المنصات ولوحات المعلومات.

12.6 حوكمة عملية ذكاء الأعمال

تطبيق حوكمة ذكاء الأعمال عملية تحتاج إلى مجهود وذلك لوجود مؤشرات ولوحات عديدة وأدوات متنوعة لتطويرها، ولذا لا يمكن تطبيق الحوكمة فقط على الأدوات المستخدمة لذكاء الأعمال وإنما لا بد من وجود نهج موحد يتم اتباعه ويجمع بين عناصر ذكاء الأعمال ويضعهم في إطار موحد.

- **الوصول المحكم للوحات والمؤشرات**

- يجب وضع مصفوفة مستخدمي البيانات وتحديد أدوارهم والصلاحيات المنسوبة لهم فعلى سبيل المثال يجب طرح الأسئلة التالية: هل يمكن لذلك المستخدم الوصول لهذه البيانات؟ هل يحق له تحميل البيانات؟ هل يحق له مشاركتها مع مستخدمين آخرين؟ هل يحق له تعديلها ورفعها مرة أخرى؟
- يجب وضع صلاحيات للمستخدمين طبقا لمصفوفة البيانات على مستوى اللوحات الرقمية وعناصر البيانات وأيضا على مستوى مجموعة البيانات.
- وجود البيانات بشكل مركزي أو محوري يضمن للمستخدمين سهولة الوصول الآمن وذلك باستخدام منصة واحدة لعرض اللوحات والمؤشرات.
- اتباع آلية موحدة ومحكمة في توثيق البيانات المرجعية عن التقارير واللوحات وسهولة الرجوع لها والتعديل عليها.

- مرور اللوحات والمؤشرات بمرحلة اختبار قبل العرض على المستخدم النهائي لضمان كسب ثقة المستفيد من عملية ذكاء الأعمال.

- **تحسين كفاءة موارد ذكاء الأعمال**

- يجب انتقاء فريق ذكاء الأعمال بدقة وحرص من أجل تحقيق المستهدفات الاستراتيجية والتشغيلية لذكاء الأعمال.
- لا بد من اتباع دورة حياة محكمة لطلبات ذكاء الأعمال وتحليلات البيانات الجديدة والتعديلات، وذلك بوضع وثائق مرجعية للمؤشرات ولوحات تم تنفيذها بوصفها وتفاصيل بياناتها وأيضا هدف كل مؤشر والقطاع المسؤول عنها ومن خلال ذلك يمكن أيضا حذف ما هو غير مفيد لقطاع الأعمال وذلك بالرجوع لمختص بيانات قطاع الأعمال.
- استخدام التراخيص يحتاج إلى الحصر والمراجعة الدورية، من تجديد أو تخفيض أو إلغاء الرخص التقنية حسب الحاجة.
- متابعة نشاط استخدام اللوحات، وتقييمه بشكل دوري ومؤتمت حسب حاجة قطاع الأعمال.

- **موثوقية مخرجات ذكاء الأعمال**

من أهم عوامل نجاح ذكاء الأعمال هي ضمان ثقة المستخدمين وضمان مشاركتهم في بناء لوحات المؤشرات التي تخدم متطلبات الأعمال الخاصة بهم، وذلك من خلال اتباع بعض الإجراءات ومنها:

- الحفاظ على قنوات تواصل مع قطاع الأعمال عند حدوث مشكلات تقنية أو فنية.
- مشاركة فريق ذكاء الأعمال بمستويات جودة البيانات، ويفضل أن تتم هذه العملية عن طريق إرسال تنبيهات آلية بشكل مؤتمت من أنظمة جودة البيانات وبشكل استباقي قبل حدوث المشاكل والبحث في حلها من قبل مختصي جودة البيانات دون التأثير على اللوحات والمعلومات المعروضة لمستخدمي قطاع الأعمال ومتخذي القرار.

- **مرحلة التجهيزوالإعداد والتخطيط**

- وجود مؤشرات أداء واضحة ورئيسية لقياس أداء وكفاءة حلول ذكاء الأعمال.
- وضع آلية للتواصل وجمع متطلبات المؤشرات من قطاع الأعمال.
- تصميم نموذج موحد للبيانات (مفاهيمية ومنطقية ومادية) بناء على إرشادات متبعة من قبل الفريق ويتم مراجعتها من قبل مختص هيكلة البيانات.
- مع التطوير وطلب الاستفسارات سيواجه الفريق مشاكل تحتاج إلى اتباع طريقة موحدة لتصعيدها وحلها، ويجب وضع مصفوفة للتصعيد بشكل هرمي.
- موافقة قطاع الأعمال على المتطلبات قبل البدء في أي تطوير أو تخطيط وتوثيق محاضر الاجتماعات، واستخدام قالب موحد تدون فيه محاضر الاجتماعات ويمكن الوصول له بسهولة.
- الوصول السهل والسريع للوثائق التي تخص أي متطلب بشكل مرجعي أو أي وثيقة تفيد قطاع الأعمال أو قطاع التقنية والتطوير.
- عند اختيار الأدوات الخاصة بذكاء الأعمال فيجب تحديد المتطلبات ومعرفة حجم المستخدمين والبيانات المطلوبة وأيضا اختيار أدوات سهلة الاستخدام وغير معقدة لمستخدمي قطاع الأعمال.
- الأخذ في الاعتبار القواعد التي تخص قطاع الأعمال ومتخذي القرار وهذا يساعد على فهم المتطلبات وأيضاً لإنتاج مخرج يضمن الاستخدام الأمثل للوحات والمؤشرات.
- الأخذ في عين الاعتبار قواعد الامتثال لمتطلبات مكتب إدارة البيانات الوطنية عند جمع البيانات وعرضها.

- **مرحلة الإنتاج**

- يمكن الاطلاع على سياسة مشاركة البيانات لمعرفة ما يجب اتباعه في مرحلة جمع البيانات وتخزينها وإنتاجها قبل استخدامها في مختلف التقارير واللوحات
- ما يخص اللوحات والمؤشرات في طور الإنتاج فيجب اتباع الآتي:
  - اتباع مصفوفة المستخدمين لإعطاء صلاحية البيانات.
  - الالتزام بسياسة حماية البيانات الشخصية.
  - الالتزام بسياسات الأمن السيبراني الصادرة من الإدارة العامة للأمن السيبراني.

- **مرحلة المتابعة**

- وضع آلية دعم لتشغيل منصة ذكاء الأعمال وتحديد فريق تشغيل للدعم الأولي وفريق فني للدعم ثانوي وذلك بحسب التنسيق مع فرق التشغيل بالإدارة العامة للتطبيقات والخدمات الإلكترونية بالإدارة العامة للتحول الرقمي، وتحديد الأدوار والصلاحيات ونطاق عمل كل فريق لضمان استمرارية المنصة والتقارير المنبثقة عنها.
- تسجيل المشاكل ومتابعتها من خلال نظام لرفع المتطلبات ومشاكل التقارير واللوحات للرجوع له ومعرفة السبب الرئيسي وحل هذه المشاكل بشكل جذري لضمان عدم التكرارية.

وزارة التعليم

Ministry of Education