PDF Public

وزارة التعليم
Ministry of Education

سياسات حوكمة البيانات

مساعد الوزير للتطوير والتحول

مكتب إدارة البيانات



تصنيف الوثيقة : عام
الإصدار: 1.1
2025

PDF Public

الفهرس

١التّعريفات ----------٥
٢الأهداف ----------١٠
٣حاكميّة سياسات حوكمة البيانات ----------١٢
٣,١ مالك الوثيقة ١٢
٣,٢ مراجعة وتعديل وتغيير السّياسات ١٢
٣,٣ الامتثال للسّياسات ١٢
3.4 التعامل مع حالات عدم الامتثال ١٢
٣,٥ استثناءات على السّياسات ١٢
٤سياسة تصنيف البيانات ----------١٤
٤,١ نطاق السّياسة ١٤
٤,٢ المبادئ الرّئيسيّة لتصنيف البيانات ١٤
٤,٣ مستويات تصنيف البيانات ١٤
٤,٤ ضوابط تصنيف البيانات ٢٠
٤,٥ الخطوات اللّازمة لتصنيف البيانات ٢١
٤,٦ الأدوار والمسؤوليات داخل الوزارة ٢٣
5سياسة حماية البيانات الشّخصيّة ----------٢٥
٥,١ نطاق السّياسة ٢٥
٥,٢ المبادئ الرّئيسيّة لحماية البيانات الشّخصيّة ٢٥
٥,٣ حقوق صاحب البيانات ٢٦
5.4 التزامات الوزارة فيما يخص حماية البيانات الشخصية ٢٦
6سياسة مشاركة البيانات ----------٣٠
٦,١ نطاق السياسة ٣٠
٦,٢ المبادئ الرئيسية لمشاركة البيانات ٣٠
٦,٣ القواعد العامة لمشاركة البيانات ٣١
٦,٤ طلب التفويض بمشاركة البيانات ٣٢
6.5 آلية تحديد ضوابط مشاركة البيانات ٣٢
٦,٦ الخطوات اللازمة لإجراء عملية مشاركة البيانات ٣٤
٦,٧ الإطار الزمني لعملية مشاركة البيانات ٣٥
٦,٨ الأدوار والمسؤوليات ٣٥
7سياسة حرّية المعلومات----------٣٧
٧,١ نطاق السّياسة ٣٧
٧,٢ المبادئ الرّئيسيّة لحرّية المعلومات ٣٧
٧,٣ حقوق الأفراد فيما يتعلّق بالاطّلاع على المعلومات العامّة أو الحصول عليها ٣٧
٧,٤ الخطوات الرّئيسيّة للاطلاع على المعلومات أو الحصول عليها ٣٧
٧,٥ أحكام عامّة ٣٨
8سياسة البيانات المفتوحة ----------٤١

PDF Public

٨,١ نطاق السّياسة	٤١
٨,٢ المبادئ الرّئيسيّة للبيانات المفتوحة	٤١
٨,٣ تقييم قيمة البيانات العامّة لتحديد مجموعات البيانات المفتوحة	٤١
٨,٤ القواعد العامّة للبيانات المفتوحة	٤٢
٨,٥ الأدوار والمسؤوليّات	٤٤
8.6 الامتثال	٤٥

PDF Public

التعريفات

PDF Public

١ التّعريفات

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

الوزارة: وزارة التّعليم.

المكتب: مكتب إدارة البيانات في الوزارة.

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

الوصول إلى البيانات: القدرة على الوصول 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.

PDF Public

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 ضوابط 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.

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

الطّفل: كل شخص لم يتجاوز الثامنة عشرة من عمره.

PDF Public

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).

PDF Public

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.

PDF Public

الأهداف

PDF Public

٢ 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:

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

PDF Public

حاكمية سياسات حوكمة البيانات

PDF Public

٣ حاكميّة سياسات حوكمة البيانات

٣,١ مالك الوثيقة

مكتب إدارة البيانات في وزارة التّعليم.

٣,٢ مراجعة وتعديل وتغيير السّياسات

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

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

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

٣,٣ الامتثال للسّياسات

١. 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.

٢. المكتب في وزارة التّعليم المسؤول عن مراقبة الامتثال لبنود هذه السّياسات.

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

٣,٤ التعامل مع حالات عدم الامتثال

١. 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:

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

٣. 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.

٤. 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.

٣,٥ 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.

PDF Public

سياسة تصنيف البيانات

PDF Public

٤ سياسة تصنيف البيانات

٤,١ نطاق السّياسة

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

٤,٢ المبادئ الرّئيسيّة لتصنيف البيانات

المبدأ الأوّل: الأصل في البيانات الإتاحة

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

المبدأ الثّاني: الضّرورة والتّناسب

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

المبدأ الثّالث: التّصنيف في الوقت المناسب

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

المبدأ الرّابع: المستوى الأعلى من الحماية

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

المبدأ الخامس: فصل المهام

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

المبدأ السّادس: الحاجة إلى المعرفة

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

المبدأ السّابع: الحدّ الأدنى من الامتيازات

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

٤,٣ مستويات تصنيف البيانات

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

PDF Public

سياسة تصنيف البيانات

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.

PDF Public

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 (٢)

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؟

PDF Public

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.	-

PDF Public

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؟

PDF Public

مستوى الاثر			
سرّي للغاية	سرّي	مقيّد	عام
عالي	متوسّط	منخفض	لا يوجد أثر
تأثير كارثي لا يمكن تداركه على البيئة أو الموارد الطبيعيّة.	تأثير طويل المدى على البيئة أو الموارد الطبيعيّة.	تأثير قصير المدى أو محدود على البيئة أو الموارد الطبيعيّة.	لا يوجد تأثير على البيئة.

٤,٤ ضوابط تصنيف البيانات

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

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

٤,٤,١ علامات الحماية

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

٤,٤,٢ الوصول

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

٤,٤,٣ الاستخدام

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

٤,٤,٤ التخزين

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

٤,٤,٥ مشاركة البيانات

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

٤,٤,٦ الاحتفاظ بالبيانات

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

PDF Public

٤,٤,٧ التّخلّص من البيانات

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

٤,٤,٨ الأرشفة

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

٤,٤,٩ إلغاء التّصنيف (رفع السرّيّة)

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

٤,٥ الخطوات اللّازمة لتصنيف البيانات

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

جرد وتحديد جميع البيانات التي تمتلكها الوزارة.

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

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

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

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

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

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

PDF Public

٤,٥,٣,١ الخطوة أ-٣ - تحديد فئة الأثر:

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

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

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

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

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

تحدّد هذه المعايير مستويات الأثر الأربعة:

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

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

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

١. عالٍ: تُصنّف البيانات باعتبارها "سرّية للغاية".
٢. متوسّط: تُصنف البيانات على أنّها "سرّية".
٣. منخفض: يلزم إجراء مزيدٍ من التقييمات (يرجى الاطّلاع على الخطوة ٤ و٥).
٤. لا يوجد أثر: تُصنّف البيانات على أنّها بياناتٍ "عامّة".

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

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

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

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

يجب على مسؤول التصنيف في هذا الصدد، دراسة ما إذا كان الإفصاح عن هذه البيانات يتعارض مع أنظمة المملكة العربيّة السعوديّة مثل نظام 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 ٥.

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

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

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

PDF Public

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

٤,٥,٦ الخطوة ٦ – مراجعة مستوى التّصنيف

يجب فحص جميع البيانات المصنّفة 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.

٤,٥,٧ الخطوة ٧ – تطبيق الضّوابط المناسبة

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

٤,٦ 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:
  ١. **تصنيف البيانات:** تصنيف البيانات التي تنتجها أو تجمعها إدارته والإدارات التابعة لها.
  ٢. **تجميع البيانات:** التأكّد من تصنيف البيانات المجمّعة من مصادرٍ متعدّدة على أعلى مستويات التّصنيف المستخدمة في تصنيف أي بيانات بشكل فردي.
  ٣. **تنسيق تصنيف البيانات:** التّأكّد من أنّ البيانات المتبادلة مصنّفة ومحميّة بصورة متّسقة.
  ٤. **الامتثال لتصنيف البيانات (بالتّنسيق مع مختصّي بيانات الأعمال):** التأكد من أنّ البيانات محميّة وفقاً للضّوابط المحدّدة.
- **مراجع تصنيف البيانات:** الشّخص المسؤول عن مراجعة واعتماد مستويات تصنيف البيانات التي يحدّدها 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.

PDF Public

سياسة حماية البيانات الشخصية

PDF Public

٥ سياسة حماية البيانات الشّخصيّة

٥,١ 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:

١. إذا وافق صاحب البيانات الشخصية على ذلك، وفقاً لأحكام نظام حماية البيانات الشخصية.
٢. إذا كانت البيانات الشخصية متاحة للعموم، أو جرى جمعها من مصدر متاح للعموم.
٣. إذا كان جمع البيانات الشخصية أو معالجتها؛ مطلوباً لأغراض المصلحة العامة، أو لأغراض أمنية ،أو لتنفيذ نظام أخر ،أو لاستيفاء مُتطلبات قضائية.
٤. إذا كان التقيد بهذا الحظر قد يُلحق ضرراً بصاحب البيانات الشخصية أو يؤثر على مصالحه الحيوية.
٥. إذا كان جمع البيانات الشخصية أو معالجتها ضرورياً لحماية الصحة العامة، أو السلامة العامة ،أو حماية حياة فرد ،أو أفراد معينين ،أو حماية صحتهم.
٦. إذا كانت البيانات الشخصية لن تُسجل أو تُحفظ في صيغة تجعل من الممكن تحديد هوية صاحبها ومعرفته بصورة مباشرة أو غير مباشرة.
٧. 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.

٥,٢ المبادئ الرّئيسيّة لحماية البيانات الشّخصيّة

المبدأ الأوّل: المسؤوليّة

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

المبدأ الثّاني: الشّفافيّة

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

المبدأ الثّالث: الاختيار 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.

PDF Public

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.

٥,٣ 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.

٥,٤ التزامات الوزارة فيما يخص حماية البيانات الشخصية

١. 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.

٢. 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.

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

٤. تقوم الجهة المختصة داخل الوزارة بمراجعة وتحديث العقود واتّفاقيات مستوى الخدمة والتّشغيل بما يتوافق مع سياسات وإجراءات الخصوصيّة المعتمدة من المسؤول الأوّل بالوزارة.

٥. 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.

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

٧. يجب أن يتمّ إشعار صاحب البيانات - بطريقة ملائمة 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.

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

٩. يجب أن يتمّ أخذ موافقة صاحب البيانات عند معالجة البيانات الشّخصيّة وفقاً لنظام حماية البيانات الشخصية ولائحته التنفيذية.

١٠. 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) .

١١. يقوم المكتب بالتأكّد من أنّ الغرض من جمع البيانات متوافقاً مع نظام حماية البيانات الشخصية ولائحته التنفيذية وذا علاقة مباشرة بنشاط الوزارة.

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

PDF Public

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

١٤. اقتصار استخدام البيانات على الغرض التي جُمعت من أجله.

١٥. يقوم المكتب بإعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات وفقاً للأغراض المحدّدة والأنظمة والتّشريعات ذات العلاقة.

١٦. 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.

١٧. يقوم المكتب بإعداد وتوثيق سياسة وإجراءات التّخلّص من البيانات لإتلاف البيانات بطريقة آمنة تمنع فقدانها أو إساءة استخدامها أو الوصول غير المصرّح به إليها - وتشمل البيانات التشغيليّة، المؤرشفة، والنّسخ الاحتياطيّة - وذلك وفقاً لما يصدر من الإدارة العامة للأمن السّيبراني.

١٨. يجب تضمين أحكام سياستي الاحتفاظ والتّخلّص من البيانات الخاصّة بالوزارة في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.

١٩. تحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشّخصيّة وذلك لمراجعتها وتحديثها.

٢٠. التّحقّق من هويّة الأفراد قبل منحهم الوصول إلى بياناتهم الشّخصيّة وفقاً للضّوابط المعتمدة من قبل الإدارة العامة للأمن السّيبراني.

٢١. 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.

٢٢. إشعار أصحاب البيانات وأخذ الموافقة منهم في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الأغراض المحدّدة.

٢٣. أخذ موافقة مكتب إدارة البيانات الوطنية قبل مشاركة البيانات الشّخصيّة مع جهات أخرى خارج المملكة.

٢٤. أن يقوم المكتب بإعداد وتوثيق ومتابعة تطبيق الإجراءات اللّازمة لضمان دقّة البيانات الشّخصيّة واكتمالها وحداثتها وارتباطها بالغرض الذي جُمعت من أجله.

٢٥. استخدام الضّوابط الإداريّة والتّدابير التّقنيّة المعتمدة في سياسات الوزارة 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.

٢٦. يقوم المكتب بمراقبة الامتثال لسياسات وإجراءات الخصوصيّة بشكل دوري ويتمّ عرضها على المسؤول الأوّل بالوزارة - أو من يفوّضه - كما يتمّ تحديد وتوثيق الإجراءات التّصحيحيّة التي سيتمّ اتخاذها في حال عدم الامتثال.

٢٧. 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.

٢٨. أن يكون المكتب مسؤول عن مراقبة الامتثال لتنفيذ هذه السّياسات وفقاً للآليات والإجراءات التي تحدّدها الجهات التّنظيميّة.

PDF Public

٢٩. على جهة التحكم إبلاغ الجهات التنظيمية فوراً ودون تأخير وبما لا يتجاوز ٧٢ ساعة من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشّخصيّة أو تلفها أو وصول غير مشروع إليها، وفقاً للآليات والإجراءات التي تحدّدها الجهات التّنظيميّة.

٣٠. 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.

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

٣٢. 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.

PDF Public

سياسة مشاركة البيانات

PDF Public

٦ سياسة مشاركة البيانات

٦,١ 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:

١. في حال كان مقدم الطلب جهة حكومية وكان الطلب لأغراض أمنية أو لاستيفاء متطلبات قضائية، أو تنفيذاً لاتفاقية دولية تكون المملكة طرفا فيها.
٢. 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.

٦,٢ 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).

PDF Public

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.

٦,٣ القواعد العامة لمشاركة البيانات

مع مراعاة الخطوات اللازمة لإجراء عملية مشاركة البيانات الموضحة في البند (٦,٦)، تتمثل القواعد العامة التي يجب اتباعها عند مشاركة البيانات فيما يأتي:

١. في حال كان مقدم الطلب جهة حكومية، وكانت البيانات مطلوبة بصورة آلية تتم عملية مشاركة البيانات باستخدام قناة التكامل الحكومية.
٢. 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.
٣. في حال تعذر استخدام أي من الوسائل المشار إليها في الفقرة (١) والفقرة (٢) 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.
٤. 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.
٥. في حال كان مقدم الطلب جهة غير حكومية يتم تقديم طلب مشاركة البيانات إلى المكتب وفقاً للآلية التي يتم تحددها.
٦. يتم إرفاق البيانات الوصفية عند مشاركة البيانات، على أن يتم إيضاح مستويات تصنيف البيانات المطلوبة.
٧. في حال كان مقدم الطلب جهة حكومية يتم تطبيق ضوابط مشاركة البيانات وفقاً لنموذج يتم إعداده من المكتب.
٨. 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 (٥) 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 (١٠) أيام عمل من تاريخ طلب الموافقة.

PDF Public

٩. في حال عدم رد الجهة المصدر خلال المدة المحددة في الفقرة (٨) من هذا البند فيعد ذلك رفضاً للطلب، ويمكن لمقدم الطلب -بحسب الأول المشار لها في الفقرة (٨) من هذا البند- الرفع لمكتب إدارة البيانات الوطنية للنظر فيه وفق ما نصت عليه الفقرة (٣) من البند (٦,٨) من هذه السياسة.

١٠. يمكن للوزارة القيام بمشاركة البيانات دون الحصول على موافقة الجهة المصدر في حال وجود تفويض بذلك، وفقاً لما ورد في البند (٦,٤).

١١. على أطراف عملية المشاركة الالتزام بالأحكام المنظمة للمنافسة عند القيام بعملية مشاركة البيانات، وعدم الاتفاق على ما من شأنه الإخلال بالأحكام النظامية ذات الصلة.

١٢. مع مراعاة ما نصت عليه الفقرة (٦) من البند (٦,٦)، 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.

١٣. 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 (١) و (٢) و (٣) من هذا البند.

٦,٤ طلب التفويض بمشاركة البيانات

١. 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 (٦,٣).

د. المسؤوليات والأدوار لضمان أمن وحماية البيانات عند مشاركتها مع مقدم الطلب.

هـ. آلية تسوية الخلافات الناشئة عن التفويض.

و. أي بنود أخرى ترى الجهة المفوضة للبيانات (مُصدِرة التفويض) إضافتها في التفويض.

٢. يجوز للجهة المفوضة للبيانات (مُصدِرة التفويض) متابعة التزام الوزارة بالمتطلبات الواردة في التفويض وطلب سجلات طلبات المشاركة والبيانات التي تمت مشاركتها.

٣. على الوزارة اتخاذ الخطوات اللازمة لضمان حداثة البيانات قبل القيام بعملية مشاركة البيانات.

٦,٥ آلية تحديد ضوابط مشاركة البيانات

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

٦,٥,١ 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.

٦,٥,٢ التفويض:

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

PDF Public

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.

٦,٥,٣ 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.

٦,٥,٤ 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.

٦,٥,٥ 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 (١) من البند (٦,٣) 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.

٦,٥,٦ 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.

PDF Public

٦,٥,٧ 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.

٦,٥,٨ 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.

٦,٦ الخطوات اللازمة لإجراء عملية مشاركة البيانات

تتم معالجة طلبات مشاركة البيانات بحسب التسلسل الآتي:

١. مع مراعاة ما نصت عليه الفقرة رقم (٤) و (٥) من البند (٦,٣)، 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.

٢. التحقق من مستوى تصنيف البيانات المطلوبة، وفي حال عدم تحديد مستوى التصنيف، يجب على المكتب تصنيف البيانات المطلوبة وفقاً لسياسة تصنيف البيانات.

٣. 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.

٤. للمكتب في حال عدم استيفاء الطلب للمتطلبات المنصوص عليها في الفقرة (٣) من هذا البند أن يرفض الطلب مع إيضاح مسببات الرفض وإتاحة الفرصة لمقدم الطلب لاستكمال المتطلبات وفقاً للفقرة (٢) من الإطار الزمني لعملية مشاركة البيانات الواردة في البند (٦,٧).

٥. عند استيفاء جميع متطلبات المشاركة يتم تحديد الضوابط المناسبة وفقاً للبند (٦,٥) وذلك لضمان الالتزام بمبادئ مشاركة البيانات وتحقيق الأهداف المحددة لكل منها.

٦. يتم توقيع اتفاقية مشاركة البيانات في حال كان مقدم الطلب جهة غير حكومية، ويتم استيفاء الضوابط المشار إليها في الفقرة (٢) من البند (٦,٨) في حال كان مقدم الطلب جهة حكومية.

٧. عند استيفاء ما ورد في الفقرة (٦) من هذا البند، تتم مشاركة البيانات المطلوبة مع مقدم الطلب وفقاً للمدة الزمنية المحددة في البند (٦,٧).

٨. لا تنطبق الأحكام الواردة في الفقرة (٣) و (٦) من هذا البند في حال كانت البيانات التي سيتم مشاركتها بيانات مصنفة على مستوى عام.

PDF Public

٦,٧ الإطار الزمني لعملية مشاركة البيانات

١. يقوم المكتب بتقييم الطلب خلال فترة زمنية لا تتجاوز (١٠) أيام عمل من تاريخ استلام الطلب، وإشعار مقدم الطلب بالقرار على أن يكون القرار مكتوباً ومسبّباً.

٢. 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 (٥) أيام عمل من تاريخ استلامه.

٣. بعد الموافقة على عملية مشاركة البيانات، يقوم المكتب باستكمال ما نصت عليه الفقرة (٦) من البند (٦,٦)؛ وذلك خلال (٥) أيام عمل من تاريخ الموافقة، على أن تتم مشاركة البيانات المطلوبة مع مقدم الطلب خلال (١٠) أيام عمل من تاريخ الانتهاء من الإجراءات المنصوص عليها في الفقرة (٦) من البند (٦,٦).

٤. 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.

٥. في حال عدم رد الوزارة خلال المدة المحددة المنصوص عليها في الفقرة رقم (١) 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 (٥) 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 (٣) من البند (٦,٨) من هذه السياسة.

٦,٨ الأدوار والمسؤوليات

١. 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.

٢. يقوم المكتب بإعداد نماذج قياسية لكل من:

أ. طلب مشاركة البيانات.

ب. اتفاقية مشاركة البيانات.

ت. الضوابط المشار إليها في الفقرة (٧) من البند (٦,٣).

ج. نموذج التفويض.

٣. 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..

٤. في حال لم تتم معالجة الخلاف وفقاً للفقرة (٣) من هذا البند، يقوم مكتب إدارة البيانات الوطنية باستكمال الإجراءات النظامية.

٥. تلتزم أطراف عملية المشاركة بالمتطلبات النظامية والمتطلبات الأخرى ذوات الصلة المتعلقة بالإشعار عن حوادث تسرب البيانات.

٦. في حال تضمن الطلب مشاركة بيانات شخصية فيتم مراعاة أحكام نظام حماية البيانات الشخصية ولوائحه التنفيذية وأحوال الإفصاح الواردة في النظام.

٧. على الجهات الحكومية الاحتفاظ بسجلات خاصة بطلبات مشاركة البيانات والوثائق المرتبطة بها ولمدة خمس سنوات من انتهاء طلب المشاركة.

٨. يجب على الوزارة إعداد ونشر سياسة لمشاركة البيانات الخاصة بها.

٩. على الوزارة نشر بيانات التواصل المعتمدة للمكتب ولذلك لتمكين تقديم طلبات المشاركة من خلالها.

١٠. على الوزارة اتخاذ الوسائل الفنية والإدارية والتنظيمية اللازمة لضمان سرعة الاستجابة لطلبات مشاركة البيانات للالتزام بالإطار الزمني الموضح في البند (٦,٧)، على سبيل المثال إعداد أدلة إجرائية داخلية للاستجابة لطلبات مشاركة البيانات واتفاقيات مستوى الخدمة، ومصفوفة الصلاحيات.

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

PDF Public

سياسة حرية المعلومات

PDF Public

٧ سياسة حرّية المعلومات

٧,١ نطاق السّياسة

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

لا تنطبق أحكام هذه السّياسة على المعلومات المحميّة التالية:

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

٧,٢ المبادئ الرّئيسيّة لحرّية المعلومات

المبدأ الأوّل: الشّفافيّة

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

المبدأ الثّاني: الضرورة والتناسب

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

المبدأ الثّالث: الأصل في المعلومات العامّة الإفصاح

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

المبدأ الرّابع: المساواة

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

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

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

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

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

٧,٤ الخطوات الرّئيسيّة للاطلاع على المعلومات أو الحصول عليها

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

١. طلب خطّي أو الكتروني.

PDF Public

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

٧,٤,٢ الخطوات 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 (٣٠ يومًا) من استلام طلب الاطّلاع أو الحصول على المعلومات العامّة، باتخاذ أحد القرارات الآتية:

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

٧,٥ أحكام عامّة

١. 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.
٢. 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.
٣. 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.

PDF Public

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

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

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

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

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

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

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

١١. 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.

١٢. 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.

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

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

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

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

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

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

١٩. 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.

PDF Public

سياسة البيانات المفتوحة

PDF Public

٨ سياسة البيانات المفتوحة

٨,١ نطاق السّياسة

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

٨,٢ المبادئ الرّئيسيّة للبيانات المفتوحة

المبدأ الأوّل: الأصل في البيانات الإتاحة

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

المبدأ الثّاني: الصّيغة المفتوحة وإمكانيّة القراءة آلياً

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

المبدأ الثّالث: حداثة البيانات

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

المبدأ الرّابع: الشّمولية

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

المبدأ الخامس: عدم التّمييز

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

المبدأ السّادس: بدون مقابل مالي

يجب إتاحة البيانات المفتوحة للجميع مجاناً.

المبدأ السّابع: ترخيص البيانات المفتوحة في المملكة

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

المبدأ 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.

٨,٣ تقييم قيمة البيانات العامّة لتحديد مجموعات البيانات المفتوحة

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

PDF Public

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.

٨,٤ القواعد العامّة للبيانات المفتوحة

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

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

٨,٤,١ التّخطيط للبيانات المفتوحة

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

PDF Public

- 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.

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

٨,٤,٢ تحديد البيانات المفتوحة

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

٨,٤,٣ نشر البيانات المفتوحة

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

٨,٤,٤ تحديث البيانات المفتوحة

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

٨,٤,٥ متابعة أداء البيانات المفتوحة

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

PDF Public

٨,٥ 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:
  ١. **اعتماد خطّة البيانات المفتوحة:** الموافقة على تنفيذ خطّة البيانات المفتوحة لدى الوزارة والإشراف عليها.
  ٢. **تخصيص الأدوار المتعلّقة بالبيانات المفتوحة:** تخصيص الأدوار المختلفة المتعلّقة بالبيانات المفتوحة.
  ٣. **اعتماد التّقرير السنوي للبيانات المفتوحة:** اعتماد التّقرير السنوي للبيانات المفتوحة الذي يُعدّه المكتب.
- **مدير عام مكتب إدارة البيانات بالوزارة:** يعتبر المدير الاستراتيجي للعمليّات المتعلّقة بالبيانات المفتوحة في الوزارة، وتتضمّن مسؤولياته ما يلي:
  ١. **التّخطيط الاستراتيجي للبيانات المفتوحة:** الإشراف على وضع خطّة البيانات المفتوحة وتقديمها إلى المسؤول الأوّل بالوزارة (أو من يفوّضه). كما يتولى مراجعة أداء البيانات المفتوحة وتحديد فرص التّحسين والاسترشاد بذلك في خطة البيانات المفتوحة.
  ٢. **الإشراف على البيانات المفتوحة:** مراجعة أنشطة تحديد البيانات المفتوحة وترتيبها بحسب الأولويّة والموافقة على نشرها وضمان تنفيذ أنشطة تحديثها.
  ٣. **الامتثال لسياسة البيانات المفتوحة:** ضمان امتثال أنشطة البيانات المفتوحة لدى الوزارة للسّياسات الوطنيّة المتعلّقة بالبيانات، ويشمل ذلك على سبيل المثال لا الحصر، تصنيف البيانات وحماية خصوصيّة البيانات الشّخصيّة وحرّية المعلومات.
  ٤. **التّنسيق مع مكتب إدارة البيانات الوطنيّة:** يُعدّ مدير 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:

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

PDF Public

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

١. **التّصديق على خطّة البيانات المفتوحة:** المساهمة في تطوير خطّة البيانات المفتوحة وإدارة الفرق المسؤولة عن تنفيذ الخطّة بالتّنسيق مع مسؤول البيانات المفتوحة.

٢. **تحديد أولويّة البيانات المفتوحة:** تقديم المشورة إلى مسؤول البيانات المفتوحة بشأن قيمة مجموعات البيانات العامّة والاستثمارات المطلوبة لنشرها وتحديثها.

٣. **مراجعة مجموعات البيانات واعتمادها:** مراجعة مجموعات البيانات واعتمادها للتّأكّد من استيفائها للمواصفات المحدّدة في اللائحة من حيث الجودة والكمال وتوثيق البيانات الوصفيّة قبل تقديمها للنشر.

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

١. **تحديد مجموعات البيانات المفتوحة:** يتولى مختصّ بيانات الأعمال مراجعة وتحديد البيانات التي يتمّ إنشاؤها ومعالجتها من قبل الإدارة التي يعمل فيها بصفة منتظمة وتصنيفها بصفتها بيانات عامّة إذا لزم الأمر.

٢. **إعداد مجموعات البيانات المفتوحة:** إعداد مجموعات البيانات المفتوحة التي سيتمّ نشرها لضمان استيفائها للمواصفات المحدّدة في السّياسة من حيث الجودة والكمال وتوثيق البيانات الوصفيّة قبل تقديمها للنّشر.

٣. **تحديث مجموعات البيانات المفتوحة:** تحديث مجموعات البيانات المفتوحة المنشورة والبيانات الوصفيّة ذات الصّلة.

٨,٦ الامتثال

يقوم المكتب بالوزارة بمراقبة الامتثال لسياسة البيانات المفتوحة.

٨,٦,١ شروط الامتثال

١. على الوزارة الالتزام بسياسة البيانات المفتوحة وتقديم تقرير سنوي إلى مكتب إدارة البيانات الوطنيّة يشمل، على سبيل المثال لا الحصر، ما يلي:

- التّقدم ومستوى الإنجاز الذي حقّقته الوزارة في خطّتها المحدّدة.
- الأهداف ومؤشّرات الأداء الرّئيسيّة المحدّدة في خطّة البيانات المفتوحة.
- عدد مجموعات البيانات المفتوحة المحدّدة.
- عدد مجموعات البيانات المفتوحة المنشورة.

٢. تقوم الوزارة - بعد التّنسيق مع مكتب إدارة البيانات الوطنيّة - بإعداد الآليات والإجراءات والضّوابط المتعلّقة بتسوية النّزاعات المتعلّقة بالبيانات المفتوحة وفقاً لإطار زمني محدّد وحسب التّسلسل التّنظيمي.

PDF Public

وزارة التعليم
Ministry of Education

