وزارة الاتصالات وتكنولوجيا المعلومات
Ministry of Information and Communications Technology

سياسة إدارة البيانات

وزارة الاتصالات وتكنولوجيا المعلومات

أبريل 2015

جدول المحتويات

تعريفات ومختصرات

"**الجهة**": تعني جهة حكومية ما لم يتم استخدام المصطلح أو تتم الإشارة إليه في سياق مختلف

"**الجمعية البريطانية للكمبيوتر** أو **BCS**": هي هيئة مهنية دولية وجمعية ذات دراية علمية تهدف إلى تشجيع دراسة وتطبيق تكنولوجيا الاتصالات وتكنولوجيا الحوسبة ونشر المعرفة في مجال تكنولوجيا المعلومات والاتصالات (ICT) لفائدة الممارسين المهنيين والجمهور العام. وتعتبر الجمعية الكيان المهني الوحيد بالمملكة المتحدة التي تمنح مؤهلات قانونية للمتخصصين في تكنولوجيا المعلومات في إطار ميثاقها الملكي.

"**DAMA (جمعية إدارة البيانات):** هي جمعية دولية غير ربحية ومستقلة تضم فنيين ومتخصصين في مجال الأعمال، وتكرس أعمالها في مجال تطوير مفاهيم وممارسات إدارة مصادر المعلومات (IRM) وإدارة مصادر البيانات (DRM)

"**البيانات":** وإدارتها تشير، لأغراض هذه الوثيقة، إلى كل البيانات والمعلومات في صيغة إلكترونية والتي تجمعها أو تسترجعها أو تتقاسمها أو تعالجها الجهات الحكومية لأغراض تقديم الخدمات الإلكترونية للجمهور و للزوار وللأعمال التجارية.

"**معالجة البيانات**": وتعني لأغراض هذه الوثيقة إجراء أي عملية أو مجموعة عمليات على البيانات بما في ذلك جمع وتلقي وتدوين وتنظيم وتخزين وأقلمة وتعديل واسترجاع، والتشاور حول، واستخدام وكشف ونشر وبث وحظر ومحو أو تدمير مثل تلك المعلومات

"**تداول البيانات**": يعني إفشاء البيانات من جهة/كيان أو جهات إلى جهة أو كيان آخر أو جهات أو كيانات أخرى، أو تداول البيانات بين وحدات جهة أو كيان

"**الجهة المصدرة للبيانات**": تعني الجهة التي يتم فيها تدوين وحفظ وصون البيانات باعتبارها صاحبة الحق في هذه البيانات، والتي تقوم بتوفير / تبادل البيانات مع الجهات الأخرى

"**الجهة المستخدمة للبيانات**": تعني الجهة التي تطلب / تتلقى البيانات

"**البيانات الإلكترونية**": جميع البيانات الصادرة في صيغة إلكترونية، منظمة كانت أو غير منظمة

"**الجهة الحكومية**": تشير إلى جميع الوزارات والمؤسسات العامة التي تتبع مباشرة للوزارات أو مجلس الوزراء في دولة قطر

"ictQATAR ": تشير إلى وزارة الاتصالات وتكنولوجيا المعلومات لدولة قطر، المجلس الأعلى للاتصالات وتكنولوجيا المعلومات لدولة قطر سابقًا

"البيانات الشخصية": تشير إلى (1) أي معلومات عن شخص معروف الهوية أو يمكن التأكد من هويته، إلى حد معقول، عن طريق تلك المعلومات أو تركيبة منها ومن معلومات أخرى و / أو (2) أي معلومات، بما فيها بيانات الموقع التي يمكن، إلى حد معقول، ربطها بشخص معين بصرف النظر عما إذا كانت هوية الشخص ظاهرة من خلال تلك المعلومات أو تركيبة منها ومن معلومات أخرى

"الطرف الثالث": تعني العبارة لأغراض هذه الوثيقة أي شخص أو كيان بخلاف الجهة المصدرة للبيانات أو الجهات المستخدمة للبيانات، يقوم بمعالجة البيانات نيابةً عن الجهة، وتشمل العبارة أي شخص أو كيان آخر يتم تعيينه من قبل طرف ثالث للغرض المشار إليه

1. التفويض القانوني

تنص المادة 14 من القرار الأميري رقم 16 لعام 2014 بشأن تحديد اختصاصات وزارة الاتصالات وتكنولوجيا المعلومات (يشار إليها فيما يلي باسم "الوزارة") على تفويض الوزارة بسلطة الإشراف على، وتنظيم وتطوير قطاعات تكنولوجيا المعلومات والاتصالات في دولة قطر بطريقة تتفق مع متطلبات استراتيجية التنمية الوطنية، وبأهداف تهيئة بيئة مناسبة للمنافسة العادلة، ودعم التنمية وتحفيز الاستثمار في هذه القطاعات؛ لتحقيق ورفع كفاءة المعلومات والبنية التحتية التكنولوجية، إضافة إلى تنفيذ ومتابعة برامج الحكومة الإلكترونية وتعزيز الوعي المجتمعي بأهمية تكنولوجيا المعلومات والاتصالات، وصولاً إلى تحسين حياة الفرد والمجتمع وبناء مجتمع قائم على المعرفة والاقتصاد الرقمي.

كما تنص المادة 12 (9) من القرار الأميري رقم 27 لعام 2014 بشأن وضع الهيكل التنظيمي للوزارة على منحها سلطة صياغة التشريعات والسياسات والمعايير ذات الصلة بأنظمة تكنولوجيا المعلومات والمعاملات الإلكترونية وخدمات الحكومة الإلكترونية، بهدف تحقيق التحول التكنولوجي للجهات الحكومية في دولة قطر.

وقد وضعت الحكومة رؤية تقضي بضمان تقاسم المعلومات لتقديم خدمات عامة أفضل من خلال زيادة التنسيق بين الجهات المعنية. وتتضمن استراتيجية التنمية الوطنية لدولة قطر 2011-2016 ضرورة استخدام تكنولوجيا المعلومات والاتصالات لتحقيق "التكامل المؤسسي" من خلال زيادة تكامل العمليات، وإنشاء مستودعات مركزية للبيانات لتقديم خدمات عامة موجهة للمواطنين، ذلك أن زيادة التنسيق من خلال تداول المعلومات من شأنه التقليل من تجزئة عملية صنع القرار من قبل الجهات الحكومية.

لقد تم إعداد هذه الوثيقة مع مراعاة القوانين المعمول بها حاليا في دولة قطر. وفي حال نشوء تعارض بين هذه الوثيقة وقوانين دولة قطر، تكون الأسبقية للقوانين، ويتعين حذف أي جزء من ذلك القبيل من الوثيقة، إلى الحد الذي يزيل ذلك التعارض، على أن تظل الوثيقة قائمة بعد تعديلها دون التأثير على بقية الأحكام. وفي هذه الحالة، لا بد من إدخال التعديلات المطلوبة لضمان الامتثال للقوانين السارية ذات الصلة في دولة قطر.

2. مقدمة

يتمثل الهدف الرئيسي من إدارة البيانات، في دعم احتياجات أي منظمة من معلومات الأعمال[1]. ويمكن تعريف إدارة البيانات[2] باعتبارها الممارسات والتقنيات والأساليب والأدوات المعمارية اللازمة لتحقيق الوصول إلى وتوفير البيانات بصورة ثابتة عبر مختلف أطياف البيانات وأنواع هياكل البيانات في المؤسسة، لتلبية متطلبات استهلاك البيانات بمختلف تطبيقاتها وعملياتها في مجال الأعمال. ومن منظور الخدمات، تعتبر إدارة البيانات[3] خدمة مؤسسية تساعد في تقديم خدمات المعلومات من خلال التحكم في أو تنسيق التعريفات أو استخدام البيانات الموثوق بها والملائمة. وتشمل المجالات الرئيسية لإدارة البيانات ما يلي:[4]

- تطوير سياسة البيانات
- ملكية البيانات
- تجميع البيانات الوصفية
- التحكم في دورة حياة البيانات
- جودة البيانات
- النفاذ إلى البيانات ونشرها

تأخذ هذه الوثيقة في الاعتبار كلاً من إدارة البيانات والوظائف الخدمية لعمليات إدارة البيانات عند تحديد أحكام السياسة، لدعم معلومات الأعمال المطلوبة لتقديم الخدمات الحكومية للجمهور على نحو سلس.

2.1 الخلفية

ونحن نمضي قدمًا نحو اقتصاد المعرفة، تصبح المعلومات أحد الأصول الثمينة التي يجب على الحكومة إدارتها باعتبارها أمانة عامة نيابة عن المواطنين. إن استخدام البيانات داخل وعبر الجهات الحكومية بفعالية أمر بالغ الأهمية لتعزيز قدرة الجهات الحكومية على وضع سياسات وتقديم خدمات أكثر ملاءمة للجمهور.

1 لماذا نحتاج إلى إدارة ألمعلومات، الجمعية الدولية لإدارة البيانات
2 تعريف إدارة وتكامل البيانات، مسرد تكنولوجيا المعلومات، غارتنر
3 مبادىء إدارة البيانات، تسهيل عملية تداول المعلومات، الجمعية البريطانية للكمبيوتر
4 مبادىء إدارة البيانات المتميزة، مكتب نائب رئيس الوزراء، لندن

تعتمد الجهات الحكومية، في تقديم الخدمات العامة لجمهورها، على معلومات قد تكون مملوكة لجهات متعددة. والواقع إنها تقوم بجمع واستخدام وتخزين مجموعة واسعة من المعلومات الشخصية، مثل سجلات تاريخ الميلاد، معلومات الهوية الوطنية وتفاصيل الوضع السكاني وعناوين الاتصال، وذلك ضمن أداء مهامها. وتستخدم المعلومات للتحقق من الهوية وتأكيد الأهلية وكشف ومنع الاحتيال.

لذلك، من المهم أن تتم إدارة البيانات باعتبارها ثروة وطنية، لأن ذلك من شأنه زيادة الكفاءة التشغيلية وخفض التكاليف، وتحسين الخدمات وتعزيز أسس الحوكمة. وتهدف هذه الوثيقة إلى وضع عمليات للحوكمة والمعايير لكافة الجهات الحكومية في دولة قطر لإدارة وتداول البيانات.

2.2 الوضع الراهن

تعمل بعض الجهات الحكومية حاليا على تداول المعلومات لتتمكن من توفير خدماتها للجمهور على نحو فعال. على سبيل المثال، وضعت كل من وزارة الداخلية، المجلس الأعلى للصحة، وزارة العمل والشؤون الاجتماعية، وزارة الاقتصاد والتجارة ووزارة التخطيط التنموي والاحصاء، ترتيبات مباشرة لتداول مثل هذه البيانات عبر مختلف الوسائل الإلكترونية وغير الإلكترونية. ومع ذلك، يجري حاليا تداول هذه البيانات على أساس محدود وثنائي فقط.

هناك جهات لا تعرف بوجود البيانات في القطاع العام، وحتى إذا عرفت بوجود تلك البيانات، فإنها قد لا تعرف مكان وجودها أو كيفية الحصول عليها. في بعض الأحيان، يمكن الحصول على بيانات من جهة أخرى، غير أن هذه الجهة لا يمكنها أن تسمح لعملائها بمعرفة حقيقة أنها موجودة في الأصل (أي أنها محظورة من قبل الجهة الموردة للبيانات). وقد تتخوف بعض الجهات من إطلاق / تداول البيانات تحت الانطباع بأن أي تداول لتلك المعلومات قد يفسر على أنه إفشاء غير صحيح للبيانات، أو ربما مخالفة.

وحتى لو افترضنا استعداد الجهات لتداول البيانات مع بعضها البعض، فقد لا تكون البيانات متاحة في شكل إلكتروني، أو قد لا تتوفر عمليات مناسبة لإدارة البيانات مثل حماية البيانات ومعايير البيانات، أو قناة أو منصة مناسبة يتم من خلالها تداول البيانات إلكترونيا. وبالمثل، قد تحجم بعض الجهات الحكومية عن اتباع مبادرات جديدة لتداول البيانات بسبب الشكوك حول صلاحياتها القانونية التي تسمح لها بذلك. وتصبح هذه المشكلات أكثر وضوحا عند الحاجة إلى الحصول على بيانات من جهات متعددة من أجل تقديم خدمة.

في الوقت نفسه، وطبقا لمسح ميداني[5]، عبر مستخدمو الإنترنت في دول مجلس التعاون الخليجي عن مخاوف من استخدام بياناتهم الشخصية لأغراض غير تلك التي تم تقديم البيانات من أجلها.

[5] تقرير وزارة الاتصالات وتكنولوجيا المعلومات في يوليو 2014 حول: مواقف مستخدمي الإنترنت بمنطقة الشرق الأوسط تجاه الأمن الإلكتروني وخصوصية البيانات (صفحة 29 ، مخاوف من سوء استخدام البيانات الشخصية)

2.3 الحاجة إلى إدارة وتداول البيانات

إن من أكبر المشكلات المتعلقة بإدارة وتداول المعلومات، هي أن معظم البيانات الحكومية محفوظة في "صوامع"، أو، بعبارة أخرى، داخل إدارات منفصلة. وبينما أن إدارة البيانات قد تكون فعالة على مستوى كل جهة على حدة، إلا أن تبني نهج موحد لإدارة البيانات من شأنه أن يؤدي إلى مستوى أكبر من التعامل المشترك وبالتالي تبادل البيانات على النطاق الحكومي بطريقة أكثر فعالية.

لقد أدركت الحكومات في جميع أنحاء العالم أهمية إدارة وتبادل البيانات، وأنشأت التشريعات والممارسات والعمليات لتسهيل هذا الجانب. وفي هذا الصدد، وجه المكتب التنفيذي لرئيس الولايات المتحدة[6] رؤساء الإدارات والجهات التنفيذية إلى إدارة المعلومات كثروة، ووضع إطاراً للمساعدة في إضفاء الطابع المؤسسي على مبادئ الإدارة الفعالة للمعلومات في كل مرحلة من مراحل دورة حياة المعلومات، لتعزيز التعامل المشترك والانفتاح. وتشجع سياسة كندا[7] في مجال إدارة المعلومات، عملية إدارة المعلومات والسجلات باستخدام نهج موحد عبر جميع الجهات الحكومية. وقد سنت فنلندا[8] قانونا حول حوكمة إدارة المعلومات يتضمن أحكاماً بشأن التزامات هيئات معينة في الإدارة العامة عند إجراء مهام إدارة المعلومات بما في ذلك توافر المعلومات في شكل إلكتروني، ونظام التعامل المشترك، وتداول المعلومات. في نفس السياق، عدل برلمان نيوزيلندا[9] قانون الخصوصية للسماح بعقد اتفاقيات تداول المعلومات المعتمدة لتمكين استخدام وتداول المعلومات بين وداخل الجهات المقدمة للخدمات العامة عن طريق تعديل أو توضيح أسس تطبيق مبادئ خصوصية المعلومات. ووضعت أستراليا[10] استراتيجية وطنية بهدف إدارة المعلومات الحكومية باعتبارها ثروة استراتيجية لضمان استخدام أكثر كفاءة وفعالية. وقدمت اللجنة القانونية في المملكة المتحدة[11]، التي أنشئت لتشجيع الإصلاح القانوني، تقريراً للبرلمان عن تداول البيانات بين الجهات الحكومية، يتضمن التوصية بإصلاح قانوني شامل من أجل إنشاء هيكل قانوني مبدئي وواضح لتداول البيانات يضمن كفاءة وفعالية الحكومة، وتقديم الخدمات العامة وحماية الخصوصية، وكذلك وضع قواعد لممارسات إدارة وتداول المعلومات بين الجهات الحكومية.

ضمانا للتوصل إلى استخدام أكثر فعالية للبيانات في القطاع العام في دولة قطر، ضمن نطاق التشريعات الحالية، ومن أجل الحفاظ على الحماية الأساسية لخصوصية البيانات، فقد أخذت وزارة الاتصالات وتكنولوجيا المعلومات زمام المبادرة لتطوير سياسة من شأنها قيادة وتوجيه الجهات في مجال إدارة وتداول البيانات على مستوى القطاع العام. وتسعى هذه الوثيقة إلى تمكين وتوجيه الجهات الحكومية في دولة قطر نحو إدارة وتداول

[6] مذكرة لرؤساء الادارات والجهات التنفيذية: سياسة إدارة البيانات المفتوحة كثروة، 9 مايو 2013 مكتب الادارة والميزانية ، المكتب التنفيذي لرئيس الولايات المتحدة الامريكية
[7] سياسة إدارة المعلومات، 1 يوليو 2007، مجلس الخزانة لأمانة كندا، حكومة كندا
[8] قانون حوكمة إدارة المعلومات في الادارة العامة، 1 سبتمبر 2010، وزارة المالية ، حكومة فنلندا
[9] تعديلات حول تداول المعلومات في قانون الخصوصية لعام 1993، فبراير 2013 ، حكومة بيوزيلندا
[10] الاستراتيجية الوطنية لتداول المعلومات الحكومية، يوليو 2007، مكتب إدارة المعلومات ، حكومة استراليا
[11] تداول البيانات بين الجهات الحكومية، تقرير تشخيصي، 10 يوليو 2014، اللجنة القانونية، وزارة العدل، المملكة المتحدة

البيانات ضمن القوانين السائدة من أجل تسهيل توفير الخدمات الحكومية على نحو فعال، مع ضمان حماية المعلومات والخصوصية.

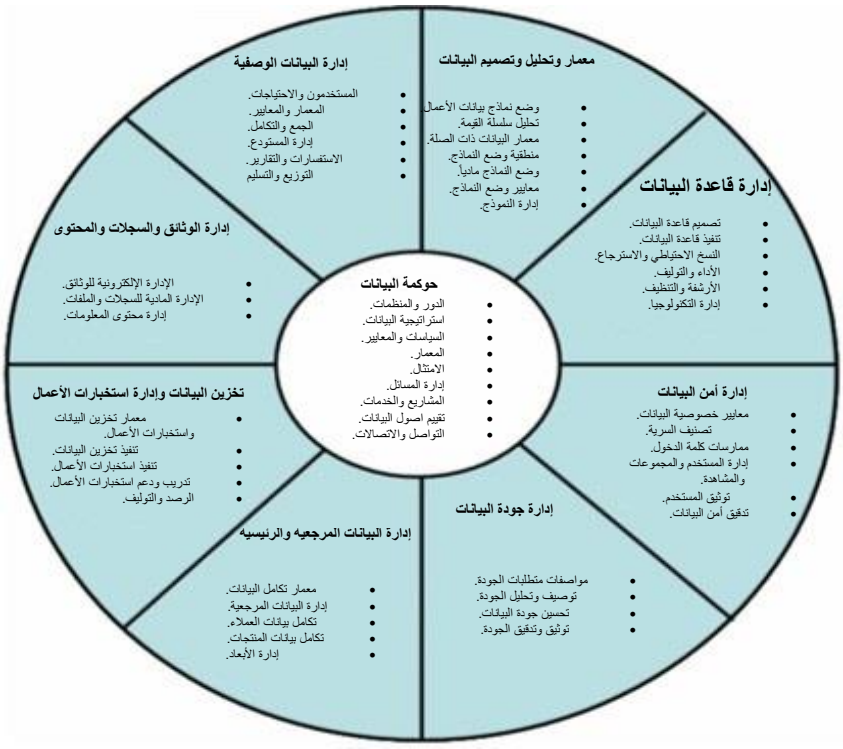
وكخطوة متقدمة أخرى، تخطط الوزارة أيضا لتطوير منصة للتطبيق تسهيلاً لتداول البيانات عبر الجهات.

2.4 المبادئ التوجيهية

تهدف هذه الوثيقة إلى توفير أساس يضمن أن أي بيانات يتم تداولها ستستخدم فقط لأغراض مشروعة، ووضع أساس لإدارة البيانات على نحو فعال. ويتعين على الحكومة وهي تتولى عملية جمع وحفظ واستخدام معلومات شخصية، أن تتصرف بوصفها راعية لتلك البيانات وصيانة وحماية أمن المعلومات وفقا لأحكام القوانين والتشريعات والسياسات ذات الصلة. كما يتعين عليها تحديد قواعد للجهات لتسهيل تداول البيانات داخل تلك الجهات وفيما بينها بطريقة فعالة.

فيما يلي المبادئ التوجيهية الرئيسية المطبقة في صياغة هذه السياسة:

i. ينبغي أن تدار البيانات كمورد استراتيجي يدعم السياسات واتخاذ القرار، علاوة على مبادىء المساءلة والتنفيذ الفعال للبرامج والخدمات الحكومية.



ii. يجب أن لا ينظر إلى البيانات التي يتم جمعها أو استحداثها من قبل كل جهة على أنها ملك لتلك الجهة وحدها، بل باعتبارها متاحة للتداول مع جهات أخرى ، ضمن حدود الخصوصية وحقوق المؤلف والاعتبارات القانونية والأمنية.

iii. حيثما كان ذلك ممكنا، يجب الحصول على البيانات مرة واحدة واستخدامها لأغراض متعددة و / أو عامة، وتجنب الازدواجية في الحصول على البيانات.

يحدد مجمل معارف إدارة البيانات لجمعية إدارة البيانات[12] الوظائف العشر لإدارة البيانات على النحو الموضح في الشكل أعلاه، وتستمد هذه الوثيقة معلوماتها من هذا الاطار فيما يتعلق ببعض الوظائف ذات الصلة في صياغة السياسة.

[12] مصدر معارف إدارة البيانات، مطبوعة تصدر عن جمعية ادارة البيانات (DAMA) - (www.dama.org)

3. النطاق والتطبيق

3.1 تنظم هذه السياسة كيفية إدارة وتداول البيانات في الجهات الحكومية

3.2 تتضمن سياسة إدارة البيانات هذه المجالات الرئيسية التالية:

- حوكمة البيانات
- إدارة البيانات
- حماية البيانات
- تداول البيانات

3.3 تنطبق هذه السياسة على جميع البيانات الصادرة في صيغة إلكترونية (منظمة كانت أو غير منظمة) والتي يتم جمعها أو استحداثها وحفظها من قبل الجهات كجزء من أعمالها الرسمية ويتم استخدامها أو تقاسمها لأغراض تقديم الخدمات العامة. ومن أمثلة البيانات المنظمة، بيانات تتعلق بالعملاء (مثل البيانات الشخصية والبيانات المؤسسية)، وبيانات لا صلة لها بالعملاء (مثل البيانات البيئية)، وبيانات مؤسسية (مثل البيانات المتعلقة بالموارد البشرية، التمويل، الأصول، والمشتريات). أما البيانات غير المنظمة (مثل مستندات معالجة الكلمات، شرائح العرض، الصور، وأشرطة الفيديو والتسجيلات الصوتية) فإنها تشمل البيانات القائمة على النص وعلى أساس الصورة النقطية.

3.4 تخضع هذه السياسة الخاصة بإدارة البيانات لاعتبارات الخصوصية وحقوق المؤلف إضافة للاعتبارات القانونية والأمنية. ويجب على الجهات ضمان الامتثال للتشريعات[13] ذات الصلة المعمول بها في دولة قطر.

[13] تشمل التشريعات المراسيم والتوجيهات والقوانين والسياسات الصادرة من السلطات المختصة بدولة قطر

4. أحكام السياسة

يضع هذا القسم للجهات الحكومية في دولة قطر الأحكام التي تضمن حسن إدارة البيانات وحمايتها وأيضا تداولها فيما بينهما من أجل توفير خدمات متميزة للجمهور.

وتتطلب سياسة إدارة البيانات هذه من جميع الجهات الحكومية في دولة قطر اتخاذ الخطوات التالية:

4.1 حوكمة البيانات

i. على الجهات تعيين أحد كبار الموظفين لتحمل مسؤولية الإشراف على إدارة ومراقبة بيانات الجهة والعمليات ذات الصلة.

ii. يجب أن يكون من يتولى هذه المسؤولية في درجة عليا مناسبة نظراً لاختصاصاته الإشرافية وتمثيل الجهة في جميع المسائل المتعلقة بإدارة البيانات وتداول البيانات عبر مختلف الجهات.

iii. يتعين على الموظف المعين التأكد من وجود عمليات وإجراءات فعالة لإدارة دورة حياة المعلومات[14] لضمان استحداث وتخزين وإدارة ومعالجة البيانات على نحو دقيق وآني ومكتمل. يتولى الموظف أيضا مسؤولية ضمان الامتثال للتشريعات ذات الصلة في هذا الشأن.

iv. يجب تصعيد جميع القضايا المشتركة بين الجهات فيما يخص إدارة وتداول البيانات إلى اللجنة التوجيهية للحكومة الإلكترونية. وتختص اللجنة التوجيهية للحكومة الإلكترونية بمراقبة البيانات وضمان مواءمتها وتقديم التوجيه العام والمشورة بشأن قضايا إدارة البيانات لتسهيل تداول البيانات عبر الجهات داخل الإطار التشريعي القائم.

4.2 إدارة البيانات

4.2.1 ملكية البيانات

i. البيانات التي يتم جمعها من قبل أي جهة هي في النهاية ملك لحكومة قطر، وبهذا الفهم يجب أن تكون متاحة للتداول مع جهات أخرى في حدود القوانين والسياسات والأنظمة القائمة.

[14] يرجى الرجوع إلى الملحق رقم 1 حول المباديء التوجيهية

ii. يتعين على الجهات المصدرة للبيانات وضع تدابير من شأنها صيانة البيانات بما في ذلك التعامل مع أية تحديثات لاحقة للبيانات ونشرها بين الجهات المستخدمة.

iii. لضمان سلامة البيانات على المستوى الحكومي، يجب على الجهات أن تطلب البيانات التي تحتاجها لاستكمال معاملات الخدمة أولاً من الجهات المصدرة للبيانات، في حالة وجودها. إما إذا لم تكن هناك جهة مصدرة للبيانات المطلوبة، فيمكن للجهات جمع بيانات من مصادر أخرى مناسبة.

4.2.2 جمع البيانات

i. على الجهات التأكد من أن جميع المعلومات أو السجلات مخزنة إلكترونيا في أنظمتها، ومصنفة ومؤمنة تمشيا مع سياسة تأمين المعلومات الوطنية (الإصدار الثاني). يجب على الجهات أيضا إنشاء وصيانة سجل لهذه البيانات والمعلومات بالغة الأهمية.

ii. على الجهات التأكد من أن البيانات يتم جمعها عن طريق الوسائل المشروعة والنزيهة، ويجب أن يقتصر الجمع على ما هو ضروري لتلبية متطلباتها القانونية أو المتصلة بنشاطها العملي. يجب تطبيق أحكام السياسة رقم 4.2.1 (iii) الواردة في هذه الوثيقة عند تحديد ما إذا كان للجهة أن تحصل على البيانات من جهة أخرى (جهة مصدرة للبيانات) أو جمعها من مصادر مناسبة أخرى.

iii. ينبغي على الجهات طلب الحصول على معلومات أو مستندات داعمة من أفراد أو شركات لاستكمال معاملات الخدمة، فقط في حالة عدم توفر هذه المعلومات إلكترونيا لديها أو عدم توفرها لأغراض التداول إلكترونيا لدى أي جهة حكومية أخرى.

iv. يجب على الجهات التأكد من أن الفرد المعني بالمعلومات الشخصية لديه معرفة وأبدى موافقته على جمع واستخدام أو الإفصاح عن بياناته الشخصية إلى طرف ثالث أو جهة أخرى لغرض استكمال معاملات الخدمة.

v. على الجهات إجراء مراجعات لتحديد الخدمات التي يمكن فيها التخلص من أو تقليل المستندات أو تعبئة الاستمارات المطلوبة من قبل الأفراد والشركات إلى أدنى حد ممكن:

أ) إجراء مراجعات لتحديد ما إذا كانت المعلومات أو المستندات ضرورية فعلاً لاستكمال خدمة أو معاملة معينة.

ب) النظر في طرق بديلة للحصول على المعلومات من خلال:

- الحصول على المعلومات المطلوبة داخليا من المستودعات وقواعد البيانات.

- طلب الإثباتات و / أو البيانات المطلوبة خارجياً من الجهات المصدرة للبيانات.
- أتمتة العمليات المشار إليها أعلاه والمتعلقة بالحصول على المعلومات من مصادر داخلية أو خارجية.

4.2.3 معايير البيانات

تعتبر معايير البيانات حجر الزاوية في عملية الاستخدام المشترك، ومن شأن اعتماد مجموعة من معايير البيانات للاستخدام في كافة الجهات الحكومية أن يفضي في النهاية إلى إزالة الغموض والتضارب في استخدام البيانات وتحقيق أساليب أكثر فعالية من حيث استخدام وتداول البيانات.

i. تتحمل كل جهة مسؤولية إنشاء وصيانة كتالوج[15] لمعايير البيانات الذي يجب أن يشمل المعلومات الوصفية والمعايير المتعلقة بالبيانات الخاصة بها في شكل موحد. من شأن كتالوج معايير البيانات أن يساعد أيضا في تحديد المسئول الرئيسي عن العمل أو الجهة المصدرة للبيانات فيما يتعلق ببيانات معينة.

ii. على الجهات نشر كتالوج معايير البيانات للموظفين المخولين في الجهات الحكومية الأخرى لكي يحددوا مدي توافر البيانات وكذلك معايير المعلومات الوصفية.

iii. على الجهات المستخدمة للبيانات اعتماد معايير البيانات الخاصة بالجهات المصدرة للبيانات بالنسبة لعناصر بيانات بعينها.

iv. تتحمل الجهة المصدرة للبيانات المسؤولية عن تحديث كتالوج معايير البيانات لديها بإضافة سمات جديدة أو محدثة، وإخطار الأطراف ذات المصلحة على مستوى الدولة بكل هذه المراجعات.

4.2.4 النفاذ إلى البيانات

يقتصر منح حق النفاذ إلى البيانات فقط على الأفراد والجهات التي لديها أسباب مشروعة ومبررة للوصول إليها، وذلك في حدود القوانين والسياسات واللوائح ذات الصلة

[15] يرجى الرجوع إلى الملحق 2 – نموذج معايير البيانات

i. على الجهات أن تميز بوضوح بين عناصر البيانات ذات النفاذ المقيد، وتلك البيانات ذات النفاذ المفتوح والتي يتم تصنيفها على أساس أنها بيانات عامة تمشيا مع سياسة تأمين المعلومات الوطنية (الإصدار الثاني).

ii. يتعين على الجهات وضع ضوابط تضمن أن فرصة الوصول إلى البيانات ذات النفاذ المقيد مقصور فقط على الأفراد والجهات التي لديها أسباب مشروعة ومبررة للوصول إليها، وكذلك الموافقات اللازمة لذلك.

4.3 حماية البيانات

4.3.1 حماية المعلومات والبيانات

كل جهة مسؤولة عن حماية جميع البيانات بما فيها البيانات الشخصية المودعة في عهدتها.

i. يجب على الجهات حماية جميع ما في حوزتها من المعلومات والبيانات (بما في ذلك البيانات الواردة من جهات أخرى)، أو عند الكشف عن البيانات لطرف ثالث أو جهة أخرى. كما يجب وضع ضمانات أمنية لحماية البيانات من أي نوع من النفاذ أو الإفشاء أو التعديل غير المصرح به.

ii. على الجهات الالتزام بـ سياسة تأمين المعلومات الوطنية (الإصدار الثاني) الصادرة من الوزارة فيما يتعلق بوجود احتياطات كافية لضمان حماية جميع أنظمة ووسائط التخزين الإلكتروني المعنية بالتعامل مع البيانات لمنع أي نوع من النفاذ أو التعديل للبيانات غير المصرح به.

iii. على الجهات إجراء مراجعات دورية لسياساتها وعملياتها لضمان وجود احتياطات كافية لحماية البيانات، وأيضا إجراء عمليات تدقيق دورية للتأكد من أن التدابير الرامية إلى حماية البيانات تتوافق مع هذه السياسات.

iv. على الجهات أن تضمن وجود إجراءات تكفل حماية سرية وسلامة البيانات التي يتم الحصول عليها من جهات أخرى.

v. على الجهات التأكد من أن تصنيف وتخزين جميع أصول المعلومات والبيانات يتم وفق مستويات السلامة الموضوعة لكل منها (يرجى الرجوع إلى سياسة تأمين المعلومات الوطنية - الإصدار الثاني - الصادرة من الوزارة).

4.3.2 حماية المعلومات الشخصية

i. يجب على الجهات الالتزام بمبادئ خصوصية المعلومات وكذلك القوانين المعمول بها في دولة قطر بشأن جمع ومعالجة وتداول البيانات الشخصية. كما يتعين عليها التأكد من أن السياسات والعمليات المطبقة لديها لحماية البيانات الشخصية حديثة ويتم التقيد بها في جميع عمليات معالجة البيانات داخل الجهة وعند نقل أو تداول البيانات مع جهة أخرى أو إلى طرف ثالث.

ii. على الجهات التأكد من أن سياساتها وعملياتها المتعلقة بمعالجة البيانات الشخصية تشمل المجالات التالية:

أ) البيانات الشخصية التي هي في حوزة الجهة أو التي تتاح لجهات أخرى والتي تعتبر ضرورية لأغراض الوفاء بشرط قانوني أو تنظيمي، أو لأغراض تقديم خدمة عامة،

ب) الإجراءات التي تمكن الفرد من الحصول على مزيد من المعلومات أو الوصول إلى البيانات الشخصية التي قدمها في وقت سابق للجهة، وكذلك الإجراءات ذات الصلة باستخدام وإفشاء تلك البيانات الشخصية من قبل الجهة.

ت) تفاصيل الاتصال بالموظف المسؤول المكلف باستقبال الاستفسارات والملاحظات المتعلقة بالبيانات الشخصية.

iii يجب على الجهات نشر بيان بشأن الخصوصية على مواقعها الإلكترونية. يرجى الرجوع إلى الملحق 3 المتضمن نسخة من عينة بيان الخصوصية.

iv يجب على الجهات تطبيق عمليات تكفل التخلص من أو تدمير البيانات الشخصية بشكل آمن وذلك لمنع الأطراف غير المصرح لها من الوصول إلى تلك البيانات.

4.4 تداول واستخدام البيانات

4.4.1 تداول البيانات

ينبغي على الجهات عدم جمع بيانات من الجمهور إذا كانت تلك البيانات متوفرة لدى جهات حكومية أخرى. ومن شأن هذا أن يكفل أن الجمهور سيقدم البيانات مرة واحدة فقط للجهات الحكومية من أجل الحصول على خدمات متعددة؛ وبالتالي ضمان مصدر وحيد للحقيقة، ودقة وسلامة البيانات.

i. يجب على الجهات المصدرة للبيانات تداول البيانات المكتسبة أو المستحدثة مع الجهات الأخرى وفق الالتزامات القانونية واعتبارات الخصوصية، ما دام هناك غرض واضح وسليم للتداول.

ii. على الجهات الحصول على موافقة الأفراد، وذلك على النماذج الورقية أو الإلكترونية لطلب الخدمة، للسماح بإعادة استخدام وتداول البيانات الشخصية لغرض توفير الخدمات الحكومية لهم. قد تكون هذه الموافقة في شكل بيان مفاده أنه بتقديم الطلب للحصول على الخدمة المطلوبة، فإن الشخص يوافق على تداول وإعادة استخدام بياناته الشخصية من قبل الجهات الحكومية في دولة قطر لأغراض تلبية طلباته الحالية والمستقبلية من الخدمات الحكومية.

iii. بالنسبة لإعادة استخدام أو تداول تلك البيانات لأي غرض بخلاف توفير الخدمات، يجب على الجهات الحصول على موافقة الأفراد فيما يتعلق بتلك الأغراض تحديداً.

iv. على الجهات المصدرة للبيانات تسهيل وتمكين تداول البيانات مع الجهات المستخدمة حتى يتمكن القطاع العام من:

أ) تحقيق أكبر قدر من الراحة للأفراد والكيانات (بمعنى أنهم سيقدمون البيانات مرة واحدة لحكومة قطر للحصول على العديد من الخدمات العامة بدلاً من الاضطرار لتقديمها لجهات مختلفة عند الحاجة لمعاملات مختلفة).

ب) توفير الخدمات الكاملة من البداية إلى النهاية (المنصوص عليها في تمشيا مع سياسة تأمين المعلومات الوطنية - الإصدار الثاني - الصادرة من الوزارة).

ت) تطوير سياسات أكثر وعياً وتركيزاً من خلال النفاذ إلى بيانات أكثر وأفضل من حيث النوعية.

ث) تعزيز الكفاءة وخفض التكلفة من خلال زيادة تداول البيانات.

4.4.2 الغرض من تداول البيانات

ينبغي على الجهات تداول البيانات مع بعضها البعض فقط لأغراض واضحة وسليمة.

i. يجب على الجهة المستخدمة للبيانات تحديد غرض واضح للجهة المصدرة للبيانات، ما لم تكن هناك موافقة مسبقة على استخدام البيانات لجميع الأغراض، من قبل الجهة المصدرة للبيانات.

ii. على الجهة المستخدمة للبيانات استخدام البيانات فقط للأغراض المحددة.

iii. يجب وضع اتفاقيات لتداول البيانات، متى ما كان ذلك مناسباً، لإلزام جميع الأطراف المشاركة في مبادرة التداول، على أن يتضمن مثل هذا الاتفاق لتداول البيانات: الغرض من تداول البيانات والمنظمات المعنية، مجموعات / عناصر البيانات التي سيتم تداولها، والقواعد المحددة لاستبقاء وحفظ وحذف عناصر البيانات المتداولة، وإجراءات التعامل مع انتهاء/إنهاء اتفاقيات تداول البيانات.

4.4.3 التداول داخل الجهات الحكومية

i. يجب تداول البيانات التي يتم جمعها أو استحداثها من قبل أي جهة مع الجهات الأخرى، وذلك في حدود القوانين المعمول بها ومبادئ خصوصية البيانات، لتمكين الجهات الحكومية من تحقيق الأهداف التالية:
أ) توفير خدمات موجهة للعملاء
ب) تحقيق مبدأ الجودة في صياغة السياسات
ت) تسهيل عمليات التحليل والبحث

ii. فيما يتعلق بالبيانات الحساسة، يجب على الجهات المصدرة للبيانات العمل مع الجهات المستخدمة للبيانات لتحديد الحد الأدنى من البيانات اللازمة لتلبية احتياجات المستخدمين، مع التأكد من وجود احتياطات كافية لضمان حماية البيانات، على سبيل المثال، بتحديد ما إذا كان في الإمكان تحقيق الهدف دون ذكر المصدر.

iii. يجب أن تقتصر البيانات التي سيتم تداولها على ما يلبي أغراض الطلب. على سبيل المثال، إذا كان الغرض من البيانات المطلوبة هو التحقق مما إذا كان مقدم الطلب يكسب أقل من 10000 ريال قطري لكي يتأهل لبعض الفوائد الاجتماعية، فينبغي على مستخدمي البيانات السؤال عن مؤشرات الدخل، أي الإجابة بـ"نعم" إذا كان الدخل أكثر من 10000 ريال قطري أو بـ"لا " إذا كان الدخل أقل من 10000 ريال قطري، بدلاً من السؤال عن دخل الفرد كمبلغ محدد.

iv. يجب على الجهات المستخدمة للبيانات الامتثال، حيثما أمكن، لمعايير البيانات الموضوعة من قبل الجهات المصدرة للبيانات لضمان سهولة الحصول على تلك البيانات.

v. إذا اعتبرت معايير بيانات الجهات المصدرة غير مناسبة من قبل الجهات المستخدمة للبيانات، لأغراض التداول أو لتقديم الخدمات، استناداً إلى أسباب مشروعة ومبررة، فيجب على الأولى تحديث معايير البيانات القائمة وجعل البيانات متاحة في الشكل المتفق عليه وخلال إطار زمني معقول.

vi. يجب على الجهات التي تعمل في مجال تداول البيانات وضع تدابير للتعامل مع التحديثات والملاحظات المتعلقة بجودة البيانات.

vii. على الجهات تضمين نصوص واضحة بشروط استخدام ومعاملة والتخلص من البيانات، بما في ذلك فترات الاستبقاء والترتيبات اللازمة لحذف البيانات المرسلة أو المستلمة، قبل تحويل البيانات إلى الجهات المستخدمة.

viii. على الجهات المستخدمة للبيانات عدم تداول البيانات مع جهات أخرى دون موافقة صريحة من الجهة المصدرة للبيانات، ما لم يكن ذلك مخولاً أو مطلوباً وفقاً لقانون أو مرسوم، أو إذا كانت البيانات متاحة للاستخدام لجميع الأغراض بموافقة مسبقة من الجهة المصدرة للبيانات.

ix. على الجهة المصدرة للبيانات تداول جميع البيانات المصنفة "معتمدة مسبقاً للاستخدام لجميع الأغراض" من خلال المنصة المركزية لتكنولوجيا المعلومات (راجع الفقرة 4.5 أدناه) الخاصة بخدمات تداول البيانات لأغراض إعادة استخدامها من قبل الجهات الحكومية .

4.4.4 التداول مع الجمهور

i. على الجهات تبادل البيانات غير الشخصية فقط مع الجمهور وذلك في حدود القوانين والسياسات واللوائح التنظيمية ذات الصلة.

ii. إن لم تكن البيانات ملكاً للجهة، فيجب عليها الحصول على موافقة الجهة المصدرة للبيانات قبل إطلاق تلك البيانات للجمهور، ما لم يكن ذلك مخولاً أو مطلوباً وفقاً لقانون أو مرسوم.

4.5 منصة مركزية لتكنولوجيا المعلومات لدعم عملية تداول البيانات الحكومية

i. على وزارة الاتصالات وتكنولوجيا المعلومات إنشاء وصيانة منصة لتبادل البيانات الحكومية يكون بوسعها أن تتيح للجهات تبادل وتصفح البيانات المتاحة لأغراض تقديم الخدمات العامة، ويمكن اللمنصة أن تتضمن المكونات الرئيسية التالية:

أ) بنية تحتية لتكنولوجيا المعلومات - منصة إلكترونية مؤمنة لتبادل البيانات الحكومية يكون من شأنها أن تتيح للجهات المصدرة للبيانات أن تتداول البيانات بينما يكون بوسع الجهات المستخدمة للبيانات أن تبحث في وأن تطلب البيانات المتاحة.

ب) دليل معايير البيانات – قواميس بالبيانات المتوفرة لدى جميع الجهات الحكومية بعد حصرها وتحديثها على النحو المبين في الفقرة 4.2.3 (i) تتضمن المعلومات الوصفية ومعايير البيانات.

ت) حوكمة وإدارة المنصة - إنشاء هيكل وإجراءات الإدارة بغرض الإشراف على فعالية وكفاءة استخدام البيانات بين الجهات الحكومية بما في ذلك شروط الاستخدام، النفاذ، اتفاقيات مستوى الخدمة...إلخ.

ii. على جميع الجهات تداول وتبادل البيانات مع الجهات الحكومية الأخرى في دولة قطر من خلال منصة تبادل البيانات الحكومية عند اكتمال تشغيلها، والالتزام بالإجراءات والمعايير المنظمة.

4.6 متابعة ومراجعة مراحل التطبيق

ستعمل الوزارة بوصفها صاحبة سياسة إدارة البيانات، على مراقبة تنفيذ الجهات وامتثالها لهذه السياسة وكذلك النفاذ إلى المنصة المركزية لتبادل البيانات عند اكتمال تطويرها.

i. على الجهات بذل أقصى جهد لتداول البيانات بين كافة الجهات الحكومية لأغراض توفير خدمات حكومة إلكترونية كاملة من البداية إلى النهاية وصولاً إلى خدمة القطريين على أفضل نحو ممكن.

ii. يجوز لوزارة الاتصالات وتكنولوجيا المعلومات إصدار أي إجراءات أو مبادئ توجيهية إضافية أو تكميلية أو نماذج لأفضل الممارسات من وقت لآخر لدعم سياسة إدارة البيانات.

الملاحق

الملحق 1: إدارة دورة حياة المعلومات

الملحق 2: نموذج معايير البيانات

الملحق 3: عينة لبيان الخصوصية

الملحق 1: إدارة دورة حياة البيانات

يعرض هذا القسم دليلًا موجزاً لفهم مختلف الخطوات المتبعة في عملية إدارة دورة حياة المعلومات للجهات بغرض وضع سياسات وإجراءات تشغيلية مناسبة لإدارة البيانات على نحو فعال.

وتمثل إدارة دورة حياة المعلومات نهجاً لإدارة السجلات والبيانات والمعلومات المؤسسية (ويشار إليها فيما يلي باسم "البيانات" في هذا القسم لسهولة الرجوع إليها)، خلال كامل دورة حياتها، أي من منشئها حتى التخلص منها. وهي تستند إلى فرضية أن قيمة البيانات تتغير مع مرور الوقت ويجب إدارتها وفقا لهذه التغيرات.

تتضمن إدارة دورة حياة المعلومات ثلاث مراحل أساسية: (i) مرحلة الإنشاء والالتقاط (ii) مرحلة التخزين والإدارة (iii) مرحلة التوزيع والتعامل:

i. الإنشاء والالتقاط

تتضمن المرحلة الأولى إنشاء أو التقاط البيانات في شكل رقمي. قد تكون بعض البيانات موجودة أصلاً في شكل رقمي، مثل ملفات XML المستخرجة من نظام الكمبيوتر أو البيانات المتاحة في شكل رقمي مثل جداول البيانات الواردة من مصادر أخرى. بينما يمكن رقمنة البيانات غير الرقمية من مصادر أخرى مثل المستندات الورقية من خلال الإدخال اليدوي إلى النظام أو عن طريق المسح الضوئي.

وتعتبر عملية التقاط وتخزين البيانات من مصادر رقمية، أسهل نسبياً بالمقارنة مع إنشاء بيانات رقمية من مصادر غير رقمية. وتشمل الحلول التقنية التي تساعد في عملية إنشاء والتقاط البيانات، النماذج الرقمية، حلول إدارة الوثائق، المسح الضوئي والتصوير، وحلول تكامل الأنظمة.

على الجهات تطوير عمليات وإجراءات تتوافق مع قانون دولة قطر رقم (2) لسنة 2011 بشأن الإحصاءات الرسمية، عند الاقتضاء، لتغطية جميع جوانب إنشاء والتقاط البيانات، وبقدر الإمكان أتمتة خطوات العملية.

ii التخزين والإدارة

بمجرد اكتمال عملية جمع وإنشاء البيانات، لابد من تخزينها على نحو يمكن من دعم الأعمال بأفضل طريقة ممكنة. وتتضمن المرحلة الثانية إدارة البيانات التي تم التقاطها وتخزينها في البنية التحتية لتكنولوجيا المعلومات في المنظمة، وفقاً لسياساتها التشغيلية. وتشمل العناصر الرئيسية في هذه المرحلة من إدارة دورة حياة المعلومات ما يلي:

أ) تصنيف البيانات

إن الغرض الأساسي من تصنيف المعلومات إلى درجات، هو التحقق من وجود تقييم صحيح لبنود المعلومات، وتحديد مخاطرها، وإجراءات الحماية المناسبة الواجب تطبيقها. ويجب تصنيف جميع البيانات التي تم إنشاؤها والتقاطها وفقاً لـسياسة تأمين المعلومات الوطنية - الإصدار الثاني.

ب) أمن البيانات وإمكانية الوصول إليها

لابد من مراعاة الأمن المادي، وأمن الشبكات، وأمن أنظمة الكمبيوتر والملفات، لضمان سلامة البيانات ومنع النفاذ غير المصرح به، أو أي تغييرات على البيانات أو الكشف عنها أو إتلافها. ويجب أن تكون الترتيبات الأمنية متناسبة مع طبيعة البيانات والمخاطر التي قد تتعرض لها.

من ضمن أهم الخطوات الأخرى في هذه العملية للمساعدة في اكتشاف طبيعة البيانات وسهولة الوصول إليها، فهرسة البيانات والكشف عن البيانات الوصفية من خلال واجهة قابلة للبحث.

أدناه بعض الممارسات التأمينية للبيانات:

- يتطلب الأمن المادي للبيانات ما يلي:

- التحكم في دخول الغرف والمباني التي توضع فيها البيانات وأجهزة الكمبيوتر أو الوسائط.
- تسجيل جميع حالات إزالة أو الوصول إلى الوسائط أو المواد المطبوعة داخل غرف التخزين.
- مراعاة عدم نقل البيانات الحساسة إلا في حالات استثنائية، حتى لو كان النقل لأغراض التصليح. على سبيل المثال، قد يشكل إعطاء محرك أقراص صلبة به خلل ويحتوي على بيانات حساسة إلى شركة مصنعة لأجهزة كمبيوتر خرقاً لإجراءات التأمين والسلامة.

- أمن الشبكات يعني:

- عدم تخزين بيانات سرية مثل تلك التي تحتوي على معلومات شخصية على الخوادم أو أجهزة الكمبيوتر المتصلة بشبكة خارجية، خاصة الخوادم التي تستضيف خدمات الإنترنت.

- نظام جدار الحماية (Firewall) والتحديثات المتعلقة بالأمن ووضع رقع واقية على أنظمة التشغيل لتجنب الفيروسات والشفرات الخبيثة.

- قد يشمل أمن أنظمة الكمبيوتر والملفات ما يلي:

- إغلاق نظام الكمبيوتر باستخدام كلمة مرور وتركيب نظام جدار الحماية.

- حماية الخوادم بأنظمة الحماية من طفرات الطاقة من خلال تركيب أنظمة إمدادات الطاقة غير المتقطعة (UPS).

- تطبيق إجراءات الحماية لملفات البيانات من خلال كلمة المرور والتحكم بالدخول، على سبيل المثال، حظر الدخول، للقراءة فقط، للقراءة والكتابة، فقط بإذن من الشخص المسؤول.

- التحكم في الوصول إلى المواد المحظورة، عن طريق التشفير.

- إلزام المديرين أو مستخدمي البيانات السرية باتفاقيات الحفاظ على السرية وعدم الإفشاء.

- عدم إرسال بيانات شخصية أو سرية عبر البريد الإلكتروني أو أي وسائل أخرى لتحويل الملفات بدون تشفيرها أولاً.

- تدمير البيانات بطريقة منتظمة عند الحاجة.

- عدم استخدام خدمات تداول الملفات مثل مستندات جوجل أو برنامج دروبوكس (Dropbox) وغيرها من الوسائل غير الآمنة.

- تفعيل نظام تعقب للمراجعة ونظام التحكم في الإصدار لتعقب التعديلات على الأنظمة وقواعد البيانات.

- أمن البيانات الشخصية:

يجب معاملة البيانات التي تحتوي على معلومات شخصية بمستويات أعلى من الأمن مقارنة بغيرها. ومن الممكن جعل التأمين أسهل عن طريق:

- إخفاء مصدر البيانات أو تجميع البيانات.

- إزالة المعلومات الشخصية مثل الاسماء والعناوين من ملفات البيانات، وتخزينها على نحو منفصل.

- تشفير البيانات التي تحوي معلومات شخصية قبل تخزينها – ومن المعلوم بالضرورة أن يتم التشفير قبل البث.

على الجهات تحديد عمليات وإجراءات أمن المعلومات بما يتماشى مع سياسة تأمين المعلومات الوطنية - الإصدار الثاني.

جـ) جودة البيانات

تعتبر البيانات ذات نوعية جيدة إذا كانت مكتملة ودقيقة ومتاحة في الوقت المناسب. ومن الأخطاء الشائعة التي تؤثر على جودة البيانات السجلات الرئيسية المكررة، وعدم وجود معايير مشتركة وغياب الروابط بين عناصر المعاملات.

وتشمل الخطوات الرئيسية في عملية جودة البيانات الآتي:

- تقييم البيانات:

تتألف مرحلة تقييم البيانات من تحليل هياكل البيانات ورسم مخطط يتضمن كل التفاصيل بين أنظمة المصدر وأنظمة الوجهة. وتعنى هذه المرحلة بتحديد متطلبات تنقية البيانات ووضع الأولويات

- ضبط جودة البيانات:

تركز هذه المرحلة على تصحيح وتوحيد البيانات لمراقبة سلامة البيانات على مر الزمن، وتشمل أساساً ثلاث خطوات: مقايسة البيانات، تنقية البيانات وتجميع البيانات. وبينما تضمن مقايسة البيانات اتساق البيانات في كافة الأنظمة، تتم تنقية البيانات لضمان سلامة البيانات وإعدادها لتلبية احتياجات نقل محددة. أما تجميع البيانات فهو يحد ويقلل من المعلومات المكررة وغير الضرورية في مستودع البيانات.

- التحقق من جودة البيانات

يجب إجراء اختبارات دورية للتحري عن أي أخطاء في البيانات. إن التحقق من البيانات يوفر القدرة على اكتشاف الأخطاء وأسباب ذلك والإجراءات التصحيحية الممكنة.

على الجهات إنشاء إطار جودة معلومات يتميز بالاستمرارية والاتساق لضبط جودة البيانات.

د) النسخ الاحتياطي للبيانات

الغرض الرئيسي من النسخ الاحتياطي هو استعادة البيانات بعد فقدانها، سواء كان ذلك بسبب حذف البيانات أو تلفها. ويشكل النسخ الاحتياطي عموماً جزءً من خطط مجابهة الكوارث في المؤسسة. على الجهات وضع

عمليات للنسخ الاحتياطي بما يتفق مع سياسة تأمين المعلومات الوطنية - الإصدار الثاني - وسياسات وإجراءات التعافي من الكوارث.

هـ) التخلص من البيانات وأرشفتها

التخلص من البيانات يعني محو البيانات التي أصبحت بالية أو زائدة عن الحاجة ولا داعي لحفظها أو أرشفتها بشكل آمن، بينما تعني الأرشفة فرز ونقل البيانات الخاملة من أنظمة الإنتاج الحالية إلى أنظمة متخصصة لتخزين المحفوظات لمدد طويلة.

تتضمن هذه العملية خطوة أساسية هي تحديد سياسات حفظ ببيانات المؤسسة. وفيما يلي بعض الأحكام القانونية والتنظيمية المعمول بها في دولة قطر بشأن حفظ السجلات[16]:

- حفظ السجلات المتعلقة بتحديد هوية العملاء لمدة 6 سنوات من نهاية العلاقة (هيئة مركز قطر للمال – لوائح مكافحة غسيل الأموال، المادة 10).
- حفظ الدفاتر المحاسبية الخاصة بجميع التجار (بما في ذلك الشركات) والمؤسسات لمدة 10 سنوات، ويجب الحفاظ على الوثائق الأساسية لمدة 5 سنوات (القانون التجاري، المادة 28).
- على دافعي الضرائب الذين يزاولون نشاطاً في دولة قطر الاحتفاظ بالدفاتر المحاسبية والسجلات والمستندات وفقاً للمعايير المحاسبية الدولية (قانون ضريبة الدخل، المادة 18)، وذلك لمدة 10 سنوات في المكان الذي يتم فيه مزاولة النشاط (قانون ضريبة الدخل، المادة 19).
- على جميع مؤسسات هيئة مركز قطر للمال حفظ السجلات المحاسبية لمدة 6 سنوات من نهاية الفترة المحاسبية أو حتى إتمام أي استفسارات حول العوائد للفترة المحاسبية (LLC: لوائح شركات هيئة مركز قطر للمال، المادة 79؛ LP: لوائح الشراكة لهيئة مركز قطر للمال، المادة 62؛ LLP: لوائح شراكات هيئة مركز قطر للمال ذات المسؤولية المحدودة، المادة 34؛ الفروع التابعة لشراكات غير مسجلة في هيئة مركز قطر للمال:. لوائح الشراكة في هيئة مركز قطر للمال، المادة 81).

يجب على الجهات مراجعة جميع التشريعات واللوائح والمعايير المعمول بها وتحديد سياسات حفظ البيانات على أساس نطاق تطبيقها على أنواع البيانات التي تحتفظ بها، وذلك بما يتماشى مع سياسة تأمين المعلومات الوطنية - الإصدار الثاني - (المادة 11، *حفظ البيانات والمحفوظات الجزء ب* - حوكمة

[16] القوانين المذكورة اعلاه هي أمثلة فقط ولا تمثل بالضرورة قائمة حصرية. وعلى الجهات مراجعة كل التشريعات المعمول بها لتحديد سياسات أمد حفظ البيانات. التشريعات والسياسات إلخ خاضعة للتعديل والتغيير لذا يجب مراجعتها دورياً للتأكد من استمرارية سريانها في ضوء التعديلات والتغييرات.

التأمين، وعمليات التأمين، دليل تأمين المعلومات الوطنية القطرية). يجب على الجهات أيضاً إنشاء نظام آمن للتخلص من البيانات وأرشفتها استناداً إلى السياسات الموضوعة.

iii التوزيع والتعامل

خلال هذه المرحلة، غالباً ما يتم إرسال البيانات بمجرد إنشائها وتخزينها إلى أحد مسارات العمل لتوجيهها كجزء من العمل. ولمعالجة البيانات، فإنه يتم تصفحها وتداولها بنشاط من قبل الجهات الحكومية وموظفيها في هذه المرحلة. ويتم تحديد القواعد الخاصة بأحقية الوصول إلى أي سجلات في المرحلة السابقة، بحيث توفر بيئة مناسبة للنفاذ السهل إلى معلومات آنية ودقيقة ومتاحة، في إطار المبادئ التوجيهية المتعلقة بالأمن والخصوصية. ويجب على الجهات إرساء عمليات من شأنها تسهيل اكتشاف وتصفح البيانات المدخلة، وإدارة البيانات المنتجة.

الملحق 2: نموذج معايير البيانات

م	عنصر البيانات	الوصف	الشكل	الطول	القيمة (نموذج)	بطاقة XML	مخطط XML	عنصر البيانات الأصلي	عنصر البيانات الفرعي	الجهة الراعية	الإدارة الراعية	نظام السجل	آخر إصدارة	تاريخ النشر يوم/شهر/سنة	ملاحظات
النموذج*															
1.0.0	تركيبة العنوان	تمثل تركيبة العنوان في قطر				تركيبة العنوان	عنوان-v2-0.xsd	(عنصر الجذر)	رقم المبنى معلومات عن الموقع معلومات عن المدينة	الجهة X	الإدارة Y	System Z	2.0	16/01/2014	
1.1.0	رقم المبنى	يحدد رقم المبنى	حرف ابجدي رقمي	5	18-A	رقم المبنى	مبنى-v1-0.xsd	تركيبة العنوان		الجهة X	الإدارة Y	System Z	1.0	01/09/2013	
1.2.0	معلومات الموقع	يحدد الموقع في مدينة				معلومات عن الموقع	موقع-v1-1.xsd	تركيبة العنوان	اسم الموقع اسم الشارع رقم المنطقة	الجهة X	الإدارة Y	System Z	1.1	16/01/2014	
1.2.1	اسم الموقع	يحدد اسم الموقع	حرف ابجدي رقمي	30	المرخية	اسم الموقع	اسم الموقع-v1-0.xsd	معلومات عن الموقع		الجهة X	الإدارة Y	System Z	1.0	01/09/2013	
1.2.2	رقم الشارع	يحدد معلومات عن الشارع	حرف ابجدي رقمي	30	الخليفة	اسم الشارع	الشارع-v1-0.xsd	معلومات عن الموقع		الجهة X	الإدارة Y	System Z	1.0	01/09/2013	
1.2.3	رقم المنطقة	يحدد رمز المنطقة	رقمي	5	67	رقم المنطقة	المنطقة v1-1.xsd	معلومات عن الموقع		الجهة X	الإدارة Y	System Z	1.1	16/01/2014	
1.3.0	اسم المدينة	يحدد اسم المدينة	حرف ابجدي رقمي	30	الدوحة	يحدد اسم المدينة	المدينة 0.xsdl-v1-	تركيبة العنوان		الجهة X	الإدارة Y	System Z	1.0	01/09/2013	

* هذا مجرد نموذج ولا يمثل بياناً لمعايير البيانات الفعلية

قد يتوسع هذا القالب كلما تم تطوير معايير بيانات إضافية ومع استمرار الجهات في التعاون والتنسيق

الملحق 3: عينة بيان الخصوصية

هذا هو الموقع الإلكتروني لـ(اسم الوزارة / الجهة)

نحن ملتزمون بحماية خصوصيتك وتوفير بيئة إلكترونية آمنة، ونتخذ الاحتياطات اللازمة لحماية المعلومات الخاصة بك. وعندما تقدم معلومات حساسة عبر شبكة الإنترنت، تأكد أن معلوماتك تجد الحماية الكافية سواء على الإنترنت أو خارج الشبكة.

جمع واستخدام وتداول وتصحيح المعلومات

إذا كنت تتصفح هذا الموقع فقط، تأكد بأننا لن نطلع على أي معلومات تتيح لنا التعرف على هويتك الشخصية.

إذا كنت ترغب في تقديم طلب لخدمة إلكترونية عبر الإنترنت يحوي معلومات شخصية تتعلق بك، فقد نقوم بتداول هذه البيانات مع جهات حكومية أخرى، أو مع جهات غير حكومية مخولة لتقديم خدمات حكومية محددة، وذلك لخدمتك بطريقة فعالة ومتميزة، ما لم يكن مثل هذا التبادل محظوراً بحكم القانون.

من أجل راحتك، قد نعرض لك البيانات التي قدمتها لنا أو لجهات حكومية أخرى سابقاً، وسيساعد هذا على تسريع المعاملات، كما يوفر عليك الوقت الذي ستستغرقه في تزويدنا بنفس المعلومات التي أرسلت بها من قبل.

وبالرغم من أننا سوف نبذل كل ما بوسعنا لتحديث المعلومات الخاصة بك، يرجى التكرم بتزويدنا بأحدث المعلومات التي تخصك إذا رأيت أنها تحتاج إلى تحديث.

الأمن

لحماية معلوماتك الشخصية، نود التأكيد على أن جميع وسائل التخزين الإلكتروني ونشر البيانات الشخصية قد جرى تأمينها باستخدام التقنيات الأمنية المناسبة.

الاتصال بمواقع إلكترونية خارجية

قد يحتوي هذا الموقع على روابط لمواقع خارجية غير حكومية تختلف تدابيرها المتعلقة بحماية البيانات وسياسة الخصوصية عن ممارساتنا نحن، وبالتالي فنحن لا نتحمل أي مسؤولية تجاه ممارسات وسياسات المحتوى والخصوصية لدى تلك المواقع الأخرى.

يرجى الاتصال بنا باستخدام نموذج الملاحظات التفاعلية لموقعنا في حالة:

(i) الاستفسار أو إبداء ملاحظات حول سياستنا وإجراءاتنا المتعلقة بحماية البيانات، أو
(ii) إذا كنت في حاجة لمزيد من المعلومات حول البيانات التي أرسلتها إلينا أو حول الوصول إليها.

تحديثات على سياسة الخصوصية

قد تتغير سياسة الخصوصية للموقع من وقت إلى آخر، وسوف يتم نشر كافة التحديثات على هذه الصفحة.