Kingdom of Saudi Arabia
Ministry of Education
University of Tabuk
Data Management Office

المملكة العربية السعودية
وزارة التعليم
جامعة تبوك
مكتب إدارة البيانات

وثيقة ضوابط أمن تصنيف البيانات

تفاصيل الوثيقة

اسم الوثيقة	وثيقة ضوابط أمن تصنيف البيانات
المؤسسة	جامعة تبوك – مكتب إدارة البيانات
مالك الوثيقة	مكتب إدارة البيانات
رقم الإصدار	1.0
الحالة	إصدار
تاريخ الإصدار	٢٠٢٣/٨/٣١ م
تصنيف الوثيقة	داخلي

جدول اعتماد الوثيقة

الإصدار	التاريخ	التعديلات	تحرير	مراجعة	موافقة
1.0	٢٠٢٣/٨/٣٠ م	لا يوجد	د. عائشة عبد الله الحكمي مسؤول إدارة البيانات	د. نيفين حسين الطويل مسؤول الامتثال	د. محمد متعب العتيبي مدير مكتب إدارة البيانات

الموافقات

الاسم	الوظيفة	التاريخ	التوقيع
د. محمد متعب العتيبي	مدير مكتب إدارة البيانات	٢٠٢٣/٨/٣٠ م	
اللجنة التنفيذية الدائمة لإدارة وحوكمة البيانات بالجامعة			

جدول المحتويات

التعريفات

المصطلح	التعريف
البيانات	مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظّمة مثل الأرقام أو الحروف أو الصور الثابتة أو الفيديو والتسجيلات الصوتية أو الرموز التعبيرية.
البيانات الشخصية	كل بيان - مهما كان مصدره أو شكله- من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابل للتعرف عليه بصفة مباشرة أو غير مباشرة عند دمجه مع بيانات أخرى، ويشمل ذلك -على سبيل المثال لا الحصر - الاسم، وأرقام الهويات الشخصية، والعناوين، وأرقام التواصل، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور المستخدم الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي
حوكمة البيانات	مجموعة من الممارسات والإجراءات التي تساعد على ضمان إدارة أصول البيانات في الجامعة، بدءً من وضع الخطة المعنية بالبيانات وتطوير المعايير والسياسات وحتى التنفيذ والامتثال.
إدارة البيانات	عملية تطوير وتنفيذ الخطط والسياسات والبرامج والممارسات والإشراف عليها لتمكين الجامعة من حوكمة البيانات وتعزيز قيمتها باعتبارها أحد الأصول القيمة والثمينة.
عنصر البيانات	عنصر البيانات هو وحدة من البيانات لها مفهوم دقيق وسمة واضحة وتمثل سمة من سمات كيان البيانات التابعة له - مثال رقم هوية العميل واسم العميل هي عناصر لبيانات العميل.
قاموس البيانات	قاموس البيانات عبارة عن قائمة مركزية تحتوي على السمات التفصيلية المحددة لعناصر البيانات (مثل اسم العنصر وتوصيفه ومصدره ونوع البيان الذي يحتويه هل هو تاريخ أو رقم أو حرف ...إلخ).
جودة البيانات	جودة البيانات هي قدرة البيانات على تلبية متطلبات العمل والنظام والمتطلبات الفنية المنصوص عليها في الجامعة، ويتم عادةً قياس جودة البيانات من حيث اكتمالها وملاءمتها وتوقيتها ودقتها، واتساقها، وارتباطها، ونزاهتها.
أمن البيانات	أمن البيانات يمثل العمليات والتقنيات المستخدمة لحماية البيانات من عمليات الوصول، أو العرض، أو التعديل، أو الحذف غير المصرح به سواءً كانت النية عرضية أو متعمدة أو كيدية.
بنية البيانات	تشتمل بنية البيانات على النماذج، أو السياسات، أو القواعد، أو المعايير التي تحكم أي بيانات يتعين جمعها وكيفية تخزينها وترتيبها واستخدامها في نظام قاعدة البيانات.
البيانات الوصفية	هي المعلومات التي تصف ماهية عناصر البيانات وخصائصها، ومن بينها بيانات الأعمال والبيانات التقنية والتشغيلية.

مرجعية البيانات	مرجعية البيانات هي الموثوقية المسلم بها والتي بصددها يتم الحفاظ على تعريفات البيانات ومعايير جودة البيانات بالإضافة إلى مشاركة حقوق الوصول.
الإشراف على البيانات	الإشراف على البيانات هي الموثوقية المسلم بها والتي بصددها يتم وضع التوصيات وتنفيذ قرارات ممثل بيانات الأعمال.
قائمة مصطلحات الأعمال	هي قائمة مركزية لتوثيق مصطلحات الأعمال ومشاركتها على نطاق الجامعة.
مستويات تصنيف البيانات	مستويات التصنيف التالية: (سري للغاية)،(سري)، (مقيّد)، (عام).

ضوابط تصنيف البيانات

بناءً على مستويات التصنيف، تقوم جامعة تبوك بتطبيق الضوابط الأمنية المناسبة لحماية البيانات وذلك لضمان التعامل معها ومعالجتها ومشاركتها والتخلص منها بشكل آمن، وفي حال عدم تصنيف البيانات عند إنشائها أو تلقيها وفقاً لمعايير التصنيف، تُعامل هذه البيانات على أنها "مقيّدة" حتى يتم تصنيفها بشكل صحيح.

كما يجب تصنيف البيانات التي لم يتم تصنيفها وقت إصدار هذه السياسة خلال فترة زمنية محددة بموجب خطة عمل تعدها الجهة ويتم اعتمادها من المسؤول الأول بالجهة. أدناه بعض الأمثلة على الضوابط التي يمكن استخدامها عند تصنيف البيانات، ويمكن الرجوع إلى ما يصدر من الهيئة الوطنية للأمن السيبراني من ضوابط وإرشادات تتعلق بحماية البيانات:

علامات الحماية

تُطبق علامات الحماية النصية على الوثائق الورقية والإلكترونية (بما في ذلك رسائل البريد الإلكتروني) وفقاً لكل مستوى من مستويات التصنيف.

الوصول

- يُمنح الوصول – المنطقي والمادي - للبيانات بناءً على مبدأ "الحد الأدنى من الامتيازات" و"الحاجة إلى المعرفة".
- يجب منع حق الوصول إلى البيانات بمجرد انتهاء أو إنهاء الخدمة المهنية للعاملين بالجهة.

الاستخدام

تُستخدم البيانات المصنفة وفقاً لمتطلبات مستويات التصنيف، على سبيل المثال، يتم تقييد استخدام البيانات المصنفة "سرية للغاية" على مواقع محددة سواء مادية – كالمكاتب – أو افتراضية باستخدام ترميز الأجهزة أو تطبيقات خاصة.

التخزين

- لا تُترك البيانات المصنفة على أنها "سري للغاية" و"سري" و "مقيّد" وكذلك الأجهزة المحمولة التي تعالج أو تخزن هذه البيانات دون مراقبة.
- يجب حماية البيانات المصنفة على أنها "سري للغاية" و"سري" و "مقيّد" غير المراقبة أثناء تخزينها مادياً أو إلكترونياً باستخدام أحد طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.

مشاركة البيانات

- تقوم الجهات بتحديد الوسائل المادية والرقمية المناسبة لتبادل البيانات بشكل آمن بما يضمن تقليل المخاطر المحتملة والامتثال لأنظمة مشاركة البيانات.

- يجب الاتفاق على آلية تبادل البيانات، سواء كانت الجهات ستستخدم الوسائل المستخدمة حالياً لتبادل البيانات أم لا، على سبيل المثال قناة التكامل الحكومية وشبكة مركز المعلومات الوطني والشبكة الحكومية الآمنة، أو إعداد اتصال مباشر جديد أو وسائط التخزين القابلة للإزالة أو الشبكة اللاسلكية، أو الوصول عن بعد، أو الشبكة الخاصة الافتراضية...الخ.

الاحتفاظ بالبيانات

- يتم إعداد جدول زمني يحدد فترة الاحتفاظ بجميع البيانات.
- يتم تحديد فترة الاحتفاظ بناءً على ما تحدده المتطلبات التجارية والتعاقدية والتنظيمية والقانونية ذات العلاقة.
- تتم مراجعة الجدول الزمني لفترة الاحتفاظ بشكل دوري - سنوي أو إذا طرأت تغييرات على المتطلبات ذات العلاقة.

التخلص من البيانات

يتم التخلص من جميع البيانات بشكل آمن وفقاً للجدول الزمني للاحتفاظ بالبيانات بعد الحصول على موافقة ممثل بيانات الأعمال.

يتم التخلص من البيانات التي تم تصنيفها على أنها "سرية للغاية" و"سري" التي يتم التحكم بها إلكترونياً باستخدام أحدث طرق التخلص من الوسائط الإلكترونية.

يتم التخلص من جميع الوثائق الورقية باستخدام آلة تمزيق الورق.

يتم إعداد سجل مفصّل عن جميع البيانات التي تم التخلص منها.

الأرشفة

- تتم أرشفة البيانات في مواقع تخزين آمنة وفقاً للطريقة التي يوصي بها ممثل بيانات الأعمال.
- يتم الاحتفاظ بنسخ احتياطية من البيانات المؤرشفة.
- تتم حماية البيانات المؤرشفة التي تم تصنيفها على أنها "سري للغاية" و"سري" باستخدام إحدى طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.
- يتم إعداد وتوثيق قائمة مفصلة تتضمن المستخدمين المصرح لهم بالوصول إلى البيانات المؤرشفة.

إلغاء التصنيف (رفع السرية(

- يجب إلغاء تصنيف البيانات أو خفض مستوى تصنيفها إلى الحد المناسب بعد انتهاء مدة التصنيف عندما لا تكون الحماية مطلوبة أو أنها لم تعد مطلوبة على المستوى الأصلي للتصنيف.
- في حال تم تصنيف البيانات بشكل خاطئ، يجب على مستخدم البيانات إشعار ممثل بيانات الأعمال لتحديد مدى الحاجة إلى إعادة تصنيفها بشكل مناسب.
- يجب تحديد عوامل تساعد على إلغاء تصنيف البيانات عند تحديد مستويات التصنيف لأول مرة، كما يجب تسجيلها في سجل أصول البيانات، قد تتضمن هذه العوامل ما يلي:
  - فترة زمنية محددة بعد إنشاء البيانات أو تلقيها)على سبيل المثال: عامين بعد الإنشاء(.
  - فترة زمنية محددة بعد اتخاذ أخر إجراء على البيانات)على سبيل المثال: ستة أشهر من تاريخ آخر استخدام(.
  - بعد انقضاء تاريخ محدد)على سبيل المثال، من المقرر مراجعتها في 1 يناير 2021 (.
  - بعد ظروف أو أحداث معينة تأثيراً مباشراً مباشرًا على البيانات)على سبيل المثال: إحداث تغيير في الأولويات الاستراتيجية أو تغيير موظفي الجهات الحكومية(.

- يتطلب إلغاء التصنيف - رفع السرية - أو خفض مستويات التصنيف، بعيداً عن العوامل المساعدة على إلغاء التصنيف الواضحة تماماً، فهماً سليماً لمحتوى البيانات السرية والسياق الذي وردت فيه.

نظام الخصوصية وحماية البيانات

اعتمدت المملكة العربية السعودية أنظمة وسياسات حماية البيانات الشخصية الصارمة من أجل ضمان حماية خصوصية المستخدمين، وتتضمن هذه الأنظمة واللوائح نظام حماية البيانات الشخصية (المرسوم الملكي رقم (م/19) بتاريخ 1443/2/9 هـ)، والمبادئ الأساسية لنظام حماية المعلومات الشخصية والمبادئ الأساسية والأحكام العامة لنظام مشاركة البيانات الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي ومكتب إدارة البيانات الوطنية.

نظام حماية البيانات الشخصية

تمّ اعتماد نظام حماية البيانات الشخصية بموجب المرسوم الملكي الصادر بتاريخ 16سبتمبر 2021، وذلك إنفاذًا للقرار رقم (98) بتاريخ 4 سبتمبر 2021. وتُعدّ الهيئة السعودية للبيانات والذكاء الاصطناعي الجهة المختصّة بتطبيق أحكام نظام حماية البيانات الشخصية الجديد ولوائحه التنفيذية وذلك لمدة سنتين، في ضوء نقل مهمة الإشراف على تطبيق أحكام النظام ولوائحه التنفيذية إلى مكتب إدارة البيانات الوطنية الذي يمثّل الذراع التنظيمي للهيئة السعودية للبيانات والذكاء الاصطناعي .

حدّد نظام حماية البيانات الشخصية ولوائحه التنفيذية الأساس القانوني لحماية الحقوق المرتبطة بمعالجة البيانات الشخصية لدى جميع الجهات بالمملكة، إلى جانب جميع الجهات القائمة خارج المملكة التي تضطلع بمعالجة البيانات الشخصية الخاصة بالأفراد المقيمين في المملكة باستخدام أي وسيلة، بما يشمل معالجة البيانات الشخصية عبر مواقع الإنترنت.

تشمل المبادئ الأساسية لسياسة حماية البيانات ما يلي:

- مساءلة رئيس الجهة (أو من ينوب عنه) عن سياسات وإجراءات الخصوصية المتبّعة لدى جهة مراقبة البيانات.
- الشفافية من خلال إشعار الخصوصية الذي يشير إلى الأغراض التي تجمع البيانات الشخصية من أجلها.
- الاختيار والموافقة المعتمدة من خلال الموافقة الضمنية أو الصريحة فيما يتعلق بجمع البيانات الشخصية واستخدامها والإفصاح عنها قبل جمعها.
- اقتصار جمع البيانات على الحد الأدنى من البيانات التي تمكِّن من تحقيق الأغراض.
- الاستخدام والاحتفاظ والإتلاف بشكل صارم للغرض المقصود، والاحتفاظ بالبيانات طالما كان ذلك ضروريًا لتحقيق الأغراض المقصودة أو كما هو مطلوب بموجب الأنظمة واللوائح وإتلافها بأمان، ومنع التسرب، أو الفقدان، أو السرقة، أو سوء الاستخدام أو الوصول غير المصرح به.
- الوصول إلى البيانات الذي يمكّن أي جهة مالكة للبيانات من خلالها استعراض بياناتها الشخصية وتحديثها وتصحيحها.
- قيود الإفصاح عن البيانات المعتمدة من قبل الجهة المالكة للبيانات تُقيّد الجهات الخارجية بالأغراض المنصوص عليها في إشعار الخصوصية.

- أمن البيانات من خلال حماية البيانات الشخصية من التسرب، أو التلف، أو الفقدان، أو السرقة، أو سوء الاستخدام ،أو التعديل أو الوصول غير المصرح به؛ وفقًا للضوابط الصادرة عن الهيئة الوطنية للأمن السيبراني والسلطات الأخرى ذات الصلة.
- جودة البيانات بعد التحقّق من دقتها واكتمالها وتوقيتها.
- مراقبة سياسات وإجراءات خصوصية جهة التحكم بالبيانات والامتثال لها، وأي استفسارات وشكاوى ونزاعات متعلقة بالخصوصية.

تغطي ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية 15 مجالًا ذي صلة. وتنطبق المعايير على جميع البيانات الحكومية بغض النظر عن الشكل أو النوع، بما يشمل السجلات الورقية، أو رسائل البريد الإلكتروني، أو البيانات المخزنة في شكل إلكتروني، أو التسجيلات الصوتية، أو مقاطع الفيديو، أو الخرائط، أو الصور، أو البرامج النصية أو المستندات المكتوبة بخط اليد أو البيانات المسجلة الأخرى. ولا يخل تطبيق أحكام نظام حماية البيانات الشخصية ولائحته التنفيذية باختصاصات ومهام الهيئة الوطنية للأمن السيبراني باعتبارها هيئة أمنية مختصة بالأمن السيبراني وشؤونه في المملكة.

أنظمة وتشريعات الأمن السيبراني

يهدف نظام مكافحة جرائم المعلوماتية إلى الحد من الجرائم المعلوماتية بهدف تحديد الجرائم والعقوبات المترتبة عليها، وذلك للمساعدة في تحقيق أمن المعلومات، وحماية المصلحة العامة والأخلاق، وحفظ الحقوق المترتبة على الاستخدام المشروع للحواسيب الآلية والشبكات المعلوماتية وحماية الاقتصاد الوطني.

أصدرت الهيئة الوطنية للأمن السيبراني مجموعة من الضوابط والأطر التنظيمية والمبادئ التوجيهية المرتبطة بالأمن السيبراني على المستوى الوطني لرفع مستوى الأمن السيبراني في المملكة سعيًا إلى حماية مصالحها الحيوية وأمنها الوطني وبنيتها التحتية الأساسية وخدماتها الحكومية. وتشمل الضوابط والأطر التنظيمية والمبادئ التوجيهية الصادرة عن الهيئة الوطنية للأمن السيبراني ما يلي:

- ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات
- الضوابط الأساسية للأمن السيبراني
- ضوابط الأمن السيبراني للحوسبة السحابية
- ضوابط الأمن السيبراني للعمل عن بعد
- ضوابط الأمن السيبراني للأنظمة الحساسة
- ضوابط الأمن السيبراني للأنظمة التشغيلية
- ضوابط الأمن السيبراني للبيانات
- الإطار السعودي لكوادر الأمن السيبراني (سيوف)
- المعايير الوطنية للتشفير
- الإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم)
- إرشادات الأمن السيبراني لمستهلكي التجارة الإلكترونية

للحصول على مزيد من المعلومات، يُرجى زيارة الموقع الإلكتروني للهيئة الوطنية للأمن السيبراني.

تشريعات حرية المعلومات

يُعد حق الحصول على المعلومات في المملكة العربية السعودية عنصرًا أساسيًا في السياسات المعلوماتية، والتي تؤكد على سياسة حق الحصول على المعلومات ذات الصلة بالمعلومات العامة السرية. ووُضِعت التشريعات بُغية تحديد شروط الأهلية المعنية بالحصول على المعلومات وحق الأفراد في الحصول على المعلومات وفقًا لخمسة شروط، إلى جانب تحديد نوع المعلومات التي يُمكن طلبها والمعلومات المستثناة من ذلك. وهناك خطوات وإجراءات رسمية لطلب الحصول على المعلومات وتحديد المنصات التي يُمكن للمواطنين تقديم الطلب عبرها، إلى جانب توفير معلومات التواصل للجهات ذات العلاقة في حال وجود أي استفسارات تتعلق بسياسة حق الحصول على المعلومات.

تتصل سياسة حرية المعلومات بالمعلومات العامة غير المحمية أو السرية التي تقوم المنصّة بمعالجتها مهما كان مصدرها أو شكلها أو طبيعتها، وتندرج البيانات المفتوحة ضمن فئة المعلومات العامة. ويطلق على عملية توفير البيانات العامة للأفراد بمقابل مادي "حرية المعلومات" أو كما تُعرف باسم "سياسة حق الحصول على المعلومات".

تشريعات حرية المعلومات

تحدّد اللوائح المؤقتة لحرية المعلومات الأساس القانوني لحقوق الأفراد في الوصول إلى معلومات القطاع العام والحصول عليها، والتزامات الجهات العامة بجميع طلبات الوصول إلى المعلومات العامة -غير المحمية- التي تنتجها أو تحتفظ بها، بغض النظر عن المصدر أو الشكل أو الطبيعة. ويشمل ذلك: السجلات الورقية، رسائل البريد الإلكتروني أو المعلومات المخزنة على أجهزة الحاسب، أو التسجيلات الصوتية، أو الفيديو، أو الميكروفيش، أو الخرائط، أو الصور الفوتوغرافية، أو الملاحظات المكتوبة بخط اليد أو أي شكل آخر من أشكال المعلومات المسجلة. كما تحدّد اللائحة أدوار ومسؤوليات الهيئة السعودية للبيانات والذكاء الاصطناعي والجهات التابعة لها، بالإضافة إلى التزامات مكتب إدارة البيانات الوطنية، ومركز المعلومات الوطني.

كل فرد يملك الحق في تقديم طلب ومعرفة المعلومات المتعلقة بأنشطة المنصّة، وأيضًا يملك الحق في الاطلاع على المعلومات العامة – غير المحمية– مقابل رسوم مالية. وليس بالضرورة أن يتمتّع مقدّم الطلب بحيثية معينة أو باهتمام معين بهذه المعلومات ليتمكن من الحصول عليها، كما أنه لن يتعرض لأي مساءلة قانونية متعلقة بهذا الحق، ويأتي ذلك تعزيزًا لمنظومة النزاهة والشفافية والمساءلة.
وتشمل حقوق الفرد في الحصول على المعلومات ما يلي:

- الحق في تقديم طلب للحصول على أو الوصول إلى المعلومات غير محمية لدى الجهات العامة.
- الحق في معرفة سبب رفض طلب الوصول أو الاطلاع على المعلومات المطلوبة.
- الحق في التظلم من قرار رفض طلب الحصول على المعلومات المطلوبة أو الوصول إليها.
- أن يتم التعامل مع جميع طلبات الوصول إلى المعلومات العامة أو الحصول عليها على أساس المساواة وعدم التميز بين الأفراد.
- أن تكون أي قيود على طلب الاطلاع أو الحصول على المعلومات المحمية التي تتلقاها أو تنتجها أو تتعامل معها المنصّة مبررة بطريقة واضحة وصريحة.

تنطبق السياسة على جميع طلبات الوصول إلى المعلومات "غير المحمية والبيانات المفتوحة" مهما كان مصدرها أو شكلها أو طبيعتها بغرض تحسين أداء وكفاءة العمل والاستفادة من البيانات. أما المعلومات المستثناة التي لا تنطبق أحكام هذه السياسة عليها هي "المعلومات المحمية" مثل:

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

لمزيد من المعلومات حول التزامات الجهات العامة والأحكام العامة، يُرجى زيارة هذا الرابط.

سياسات ولوائح البيانات المفتوحة

البيانات الحكومية المفتوحة هي البيانات التي يمكن لأي شخص استخدامها دون أي قيود تقنية أو مالية أو قانونية. كما يُمكن إعادة استخدام البيانات المفتوحة وإعادة توزيعها، شريطة مراعاة متطلبات ترخيص البيانات المفتوحة التي بموجبها يتم توزيع هذه البيانات، فضلًا عن كونها تساعد على سد الفجوة بين الحكومات والمواطنين.

تحقيقًا لمبدأ الشفافية وتمكينًا للمواطنين القائمين في المملكة من الوصول إلى قاعدة كبيرة من البيانات الحكومية، أطلقت المملكة السياسات واللوائح الإرشادية ذات الصلة.

تُعد الهيئة السعودية للبيانات والذكاء الاصطناعي الجهة الوطنية المنظّمة للبيانات في المملكة العربية السعودية، حيث طوّرت سدايا إطار عمل حوكمة البيانات الوطنية لوضع السياسات واللوائح المطلوبة لتصنيف البيانات، ومشاركتها، وخصوصيتها، وحرية المعلومات، والبيانات المفتوحة، وغيرها تحسبًا للتشريعات اللازمة.

اللوائح المؤقتة للبيانات المفتوحة

تحدّد اللوائح المؤقتة للبيانات المفتوحة الأساس القانوني والالتزامات لجميع البيانات والمعلومات العامة التي تنتجها الجهات العامة بغض النظر عن المصدر أو الشكل أو الطبيعة. كما تعين الأسس القانونية والحد الأدنى من المعايير للوكالات الحكومية لنشر

مجموعات البيانات الخاصة بها. وتبيّن اللائحة المؤقتة للبيانات المفتوحة أدوار ومسؤوليات الهيئة السعودية للبيانات والذكاء الاصطناعي وجهاتها الفرعية، ومكتب إدارة البيانات الوطنية ومركز المعلومات الوطني. وجميع الجهات الحكومية الأخرى التي لديها التزامات فيما يتعلق بوضع خطط البيانات المفتوحة وتحديدها ونشرها وصيانتها وتتبع الأداء والامتثال.

لوائح وسياسات التشغيل البيني للبيانات

استجابت الحكومة إلى ضرورة وضع إطار التشغيل البيني رسميًا منذ عام 2006، كجزء من الاستراتيجية الرقمية الوطنية الأولى للحكومة السعودية.

جرى العمل على تطوير إطار التشغيل البيني واعتماده، حيث يتضمن تعريفًا للبيانات المشتركة والمعايير التقنية، وإطار يسّر للتشغيل البيني، ويهدف إلى دعم الوزارات والجهات الحكومية لتبادل البيانات وتقديم الخدمات عن طريق البنية التحتية المشتركة للتكامل. وأدت جهود تيسير تقديم الخدمات الإلكترونية، وتوفير المزايا الفنية المنسّقة إلى تمكين قابلية التشغيل لخطط التحوّل الرقمي ذات الأولوية.

تركّز الخطط الحالية للتشغيل البيني على ما يلي:

- تحديد معايير البيانات المشتركة البيانات على المستويين التشغيلي والمنطقي، ووصف مخططات البيانات الهياكل المستخدمة في الربط بين الأنظمة.
- تحديد معايير البيانات الوصفية الخصائص والقواميس المستخدمة لتصنيف وفهرسة المحتوى الإلكتروني.
- ضمان المعايير والسياسات التقنية لفاعلية التشغيل البيني على المستوى التقني، وشمولية معايير الاتصال والربط ومعايير التكامل والمعايير الأمنية.

لا تشكّل عملية تطوير إطار التشغيل البيني نشاطًا لمرة واحدة، ولكنها مبادرة مستمرة تستدعي بذل جهود متواصلة. ويتضمن التحوّل الرقمي مواصفات مُفصّلة، مثل: المواصفات المتعلقة بالبيانات والبيانات الوصفية والمعايير التقنية. يُعرّف الإطار هياكل البيانات المشتركة وعناصر البيانات بكونها ضرورية لضمان التكامل السلس بين الأنظمة ومشاركة البيانات على مستوى جميع الجهات الحكومية. وتُعد وثيقة معايير قابلية التشغيل البيني الوطنية في غاية الأهمية لأنها توفّر الإرشادات وتعريفات هياكل البيانات اللازمة لضمان التشغيل البيني، والتكامل، وقابلية النقل للأنظمة، وإمكانية إعادة استخدامها. كما وتوضّح المعايير واللوائح التنظيمية التي تمكِّن الجهات من مشاركة الخدمات والاستفادة منها من خلال البنية التحتية التقنية الحكومية، وتزيل أوجه الغموض وعدم الاتساق في استخدام البيانات من خلال تفويض مجموعة من عناصر البيانات وهياكل البيانات للتكامل.

تُولي وزارة الصحة اهتمامًا بالغًا بقابلية التشغيل البيني نظرًا لحساسية مشاركة البيانات بين مواقع وجهات مختلفة. ووُضعت مجموعة من الوثائق المرتبطة بالتشغيل البيني لتحديد الإرشادات واللوائح الأساسية الرامية إلى ضمان مشاركة البيانات القابلة للتشغيل البيني بأمان. وتُطبّق المواصفات الأساسية للتشغيل البيني على أنظمة المعلومات الحالية والجديدة التي سيجري من خلالها تبادل المعلومات الصحية. وتُطبَق هذه المواصفات بوجه خاص على تشغيل منصات تبادل المعلومات لمجال الصحة الإلكترونية. ويُمكن الاطّلاع على أمثلة في المركز الوطني للمعلومات الصحية، مثل:

- تفعيل قابلية التشغيل البيني في السجلات الصحية الإلكترونية IS0010 القائمة على المعايير للمواصفات الأساسية السعودية للتشغيل البيني في مجال الصحة الإلكترونية للمناعة، النسخة الأولى بتاريخ 21 أبريل 2016
- تفعيل قابلية التشغيل البيني في السجلات الصحية الإلكترونية IS0003 القائمة على المعايير للمواصفات الأساسية السعودية المعنية بالتشغيل البيني للصحة الإلكترونية لمشاركة نتائج الفحوص المختبرية المشفرة، بتاريخ 21 أبريل 2016

سياسات البيانات المعنية بتبادل البيانات

ينطوي تخزين البيانات على محتواها وهيكل التخزين وغيرها من المعلومات التي يجب أن تُلحق بها ولا يُمكن أن تُخزن دونها. وتشمل تلك المعلومات إرشادات حول القضايا الإلزامية لضمان صلاحية البيانات واستخداماتها، على سبيل المثال: يجب تحديد مدة التخزين لجميع البيانات المُخزنة أو مدى صلاحيتها، حيث يجب أن تحدّد المدة متى أصبحت البيانات قديمة أو غير قابلة للمشاركة، وهو ما يُعرف بمدة الاحتفاظ بالبيانات. وتشمل القضايا الأخرى ما يلي:

- المعلومات المعنية بهوية الفرد وماهية البيانات التي يجب أن يحتفظ بها، والمدة الزمنية، ومتى وإذا كانت مدة الاحتفاظ هي القصوى أو الدنيا.
- المراجع القانونية والروابط الناقلة إلى المصدر القانوني الرسمي.
- البيانات المحدّثة وجدول بمواعيد تحديثها بوتيرة متكررة.
- الوصول المحمي والخاضع للرقابة.
- يجب أن تكون البيانات التي جرت مشاركتها مرنة من حيث الاستخدام، ويُقصد بذلك أن تكون قابلة للتحويل أو الجمع للتحليلات الفردية أو إصدار التقارير.

يرتبط الغرض من جمع البيانات الشخصية ارتباطًا مباشرًا بأغراض الحكومة الرقمية (GOV.SA) ولا يتعارض مع أي من الأحكام المحدّدة. وتكون طرق ووسائل جمع المعلومات الشخصية مناسبة لظروف المالك، ومباشرة وواضحة وآمنة، وخالية من الخداع أو المعلومات المُضلّلة أو الابتزاز. وفي حال اتضّح أن البيانات الشخصية المجمّعة لم تُعد ضرورية لتحقيق الغرض من جمعها، فستتوقف الحكومة الرقمية (GOV.SA) عن اكتنازها وستتلف البيانات التي جُمعت آنفًا على الفور.

اعتُمدت الاتفاقية بخصوص هذه المعايير مسبقًا ويجري استخدامها في الوقت الحالي، حيث تحدّد ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية(منذ يناير 2021) هذه المعايير.

سياسات إدارة واستخدام البيانات

يجب أن يوافق جميع المستخدمين المُخوّلين على السياسات واللوائح التنظيمية للخصوصية وحماية البيانات المعمول بها في المملكة العربية السعودية. ويجب أن توفّر جميع منصات البيانات إمكانيات وميزات التحكم في البيانات من خلال المنصّة وتطبيقاتها. وتُعد هذه الاتفاقية سارية فور استخدام المنصّة أو الوصول إليها لأول مرة.

يرتبط الغرض من جمع البيانات الشخصية ارتباطًا مباشرًا بأغراض الحكومة الرقمية بهدف تقديم خدمات إلكترونية أسهل وأكثر كفاءة ولا يتعارض مع أي حكم محدّد في أنظمة وسياسات أمن وخصوصية البيانات. وتكون الطرق والوسائل المختلفة لجمع المعلومات

الشخصية مناسبة لظروف المالك، ومباشرة وواضحة وآمنة، وخالية من الخداع أو المعلومات المُضلّلة أو الابتزاز. وفي حال اتضّح أن البيانات الشخصية المجمّعة لم تُعد ضرورية لتحقيق الغرض من جمعها، فستتوقف الجهة ذات العلاقة عن اكتنازها وستتلف البيانات التي جُمعت آنفًا على الفور. وستضمن الحكومة الرقمية (GOV.SA) استيفاء المعايير التالية قبل جمع البيانات الشخصية وفق ما يلي:

- المبرر المنطقي لجمع البيانات الشخصية.
- الغرض من جمع البيانات الشخصية، سواءً كان جميعها أو جزء منها، سواءً بصورة إلزامية أو اختيارية، مع توفير المزيد من المعلومات حول معالجة البيانات التي لا تتعارض مع الغرض من جمعها أو التي ينص عليها النظام بطريقة أخرى.
- الهوية والعنوان المرجعي لجامع البيانات الشخصية عند الاقتضاء، ما لم يكن ذلك لأغراض أمنية.
- الجهات التي ستحظى بإمكانية الاطلاع على البيانات الشخصية ووصفها، وفي حال ستنُقل البيانات الشخصية أو يُفصح عنها أو ستُعالج خارج المملكة.
- العناصر الأخرى التي تحدّدها اللوائح اعتمادًا على طبيعة النشاط الذي تمارسه هذه الجهة.