سيادة البيانات

القوانين والتحديات وأفضل الممارسات

WHITEPAPER

tenx

tenx.ai

مقدمة

تُعدّ البيانات المحرك الأساسي للابتكار الحديث والنمو الاقتصادي، إذ تفتح آفاقاً جديدة كالتحليل التنبؤي وإدارة الموارد بكفاءة عالية، مما يُحوّل طريقة عمل الشركات والحكومات والأفراد. غير أن الاعتماد المتزايد على البيانات يستوجب تعزيز الحماية من التهديدات كاختراق البيانات والهجمات الإلكترونية، والامتثال للوائح والأنظمة الإقليمية والدولية

وقد دفعت المخاوف المتعلقة بخصوصية البيانات الحكوماتِ إلى اتخاذ إجراءات تشريعية. فعلى سبيل المثال، تخضع قوانين سيادة البيانات ومتطلبات الإقامة في أستراليا لمنظومة من القواعد والأنظمة الرامية إلى تحقيق التوازن بين حرية تدفق المعلومات وحماية الأفراد والمؤسسات، وتسري على البيانات والتقنيات المعنية بإدارتها. ووفقاً لتقرير IBM، يبلغ متوسط تكلفة اختراق البيانات في أستراليا نحو 4.03 مليون دولار أسترالي، فيما قد تتجاوز تكاليف الاختراق في قطاع الاتصالات حاجز 100 مليون دولار أسترالي

ثلاثة جوانب جوهرية للبيانات

قبل التعمق في منظومة لوائح البيانات وتحدياتها، يُعدّ التمييز بين سيادة البيانات وحوكمتها وأمنها أمراً بالغ الأهمية، إذ تُشكّل هذه المفاهيم الثلاثة ركائز إدارة البيانات الفعّالة

سيادة البيانات

الاختصاص القانوني للبيانات في الدولة التي تقطن فيها. تحكم قوانين الدولة وأنظمتها طريقة جمع تلك البيانات ومعالجتها وتخزينها ونقلها

يتعين على المؤسسات الامتثال للوائح حماية البيانات المعمول بها في الاختصاص القانوني المعني، لضمان الالتزام وتفادي الانتهاكات والعقوبات

أمن البيانات

التدابير والممارسات المُتّبعة لحماية المعلومات الرقمية، كقواعد البيانات والملفات والأنظمة، من الوصول غير المصرح به والإفصاح والتعديل والتدمير أو التعطيل

يتمثّل الهدف الأساسي لأمن البيانات في ضمان سريتها وسلامتها وإتاحتها، وصونها من التهديدات والثغرات المحتملة

حوكمة البيانات

إطار شامل من السياسات والعمليات والمعايير والمسؤوليات المحددة للبيانات طوال دورة حياتها، يضمن توافقها مع الأهداف المؤسسية والمتطلبات التنظيمية

التحديات والانعكاسات

تحديات سيادة البيانات

تحديات نقل البيانات
تتسم إدارة البيانات عبر الحدود الدولية بالتعقيد نظراً لتباين قوانين حماية البيانات، مما يُفضي إلى تعقيدات تتعلق بالامتثال وتعارضات محتملة

متطلبات تحليل البيانات المحلية
لا يزال النقاش قائماً حول تحليل البيانات المحلية (الإبقاء على البيانات داخل الحدود الوطنية) وعولمة البيانات (الاستفادة من مراكز البيانات العالمية)، ويمثّل ذلك تحدياً جوهرياً مستمراً. إذ قد تتعارض متطلبات سيادة البيانات مع مزايا الوصول إلى البيانات وتخزينها على المستوى العالمي

التهديدات المالية
كثيراً ما يستلزم الحفاظ على البيانات داخل حدود جغرافية محددة تكاليف مرتفعة، مما يُلقي بأعباء مالية ثقيلة على كاهل المؤسسات
.

التكيّف مع الخدمات السحابية
يمكن أن تؤثر لوائح سيادة البيانات على مزودي الخدمات السحابية، مما يُحدّ من قدرتهم على تقديم خدماتهم عبر مختلف الاختصاصات القضائية، وقد يؤثر ذلك على توقيت إتاحة الميزات السحابية وتوفرها في مواقع جغرافية بعينها

تحديات حوكمة البيانات

التعامل مع القوانين واللوائح
يتعين على المؤسسات التعامل مع لوائح حماية البيانات المعقدة والمتطلبات الخاصة بكل قطاع. وقد يستنزف الوفاء بهذه الالتزامات التنظيمية الموارد بشكل كبير ويُشكّل تحدياً حقيقياً

تحديات تطبيق مبدأ الخصوصية بالتصميم
قد يتعارض تطبيق مبدأ الخصوصية بالتصميم (نهج دمج تدابير الخصوصية في الأنظمة والعمليات والتقنيات منذ البداية) مع الأنظمة والعمليات القائمة، مما يؤدي إلى تطبيق متأخر قد يكون مكلفاً

الموازنة بين الوصول العالمي والتخزين المحلي
تتسم إدارة البيانات العالمية مع الالتزام باللوائح المحلية بالتعقيد، مما قد يُقيّد قدرة المنظمات الدولية على إدارة بياناتها بصورة متسقة

ضمان دقة تصنيف البيانات
يُعدّ تصنيف البيانات وفق مستوى حساسيتها أمراً بالغ التعقيد، إذ قد يفضي سوء التصنيف إلى ثغرات أمنية. كما تزيد إدارة البيانات الحساسة عبر السحابة من هذا التعقيد؛ فالإفراط في تأمين البيانات قد يُقيّد الوصول إليها، فيما يُهدد التأمين غير الكافي بنشوء ثغرات

تحديات أمن البيانات

مواكبة التطور في مجال الأمن الإلكتروني
يُشكّل التطور المستمر في طبيعة التهديدات الإلكترونية تحدياً جسيماً، إذ يتعين على المؤسسات التكيّف باستمرار مع أساليب الهجوم الجديدة لصون أصولها من البيانات

صون الخصوصية
لا يقتصر أمن البيانات على التهديدات الخارجية، بل يمتد ليشمل مخاطر الاختراق الداخلي. وتستلزم إدارة صلاحيات وصول الموظفين ومراقبتها دون انتهاك حقوق الخصوصية وقتاً وموارد كبيرة

تأمين تدفقات البيانات عبر الحدود
يتعين على المؤسسات التي تتعامل مع تدفقات البيانات الدولية ضمان أمن البيانات أثناء النقل، لا سيما حين تعبر الحدود حيث قد تختلف القوانين المعمول بها

فاعلية الوصول إلى البيانات
يستلزم تطبيق ضوابط الوصول المناسبة وتدابير حماية البيانات دون تقييد الاستخدام السليم توازناً دقيقاً

حوكمة البيانات وأمنها في أستراليا

تخضع حوكمة البيانات وأمنها في أستراليا لمنظومة تنظيمية متينة تضمن الحماية والخصوصية والتعامل الأخلاقي مع البيانات، بما يتوافق مع المعايير الدولية ويعالج الاحتياجات المحلية. فيما يلي نظرة عامة على ثلاثة تشريعات وإرشادات رئيسية في أستراليا

قانون الخصوصية 1988

يُلزم قانون الخصوصية المؤسساتِ باتباع مبادئ (APPs) تُعرف بالمبادئ الأسترالية للخصوصية لتطبيق ممارسات أمن بيانات صارمة

الوصول إلى البيانات
يحق للأفراد الاطلاع على معلوماتهم الشخصية المحتفظ بها لدى المؤسسات وتعديلها، لضمان دقة البيانات والشفافية

موافقة الأفراد
يُقيّد القانون طريقة استخدام المعلومات الشخصية أو مشاركتها، ويشترط على المؤسسات الحصول على موافقة الأفراد أو التأكد من أن الاستخدام أو الإفصاح يتم وفق أحكام القانون

دليل أمن المعلومات (ISM)

لا يُعدّ دليل أمن المعلومات قانوناً بحد ذاته، بل هو إرشادات تُصدرها مديرية الإشارات لتأمين الأنظمة والمعلومات (ASD) الأسترالية

تصنيف المعلومات
توجيهات بشأن تصنيف المعلومات وفق درجة حساسيتها، لضمان توافر تدابير أمنية مناسبة لكل نوع من البيانات

التحكم في الوصول
تدابير للتحكم في الوصول إلى الأنظمة والبيانات، تشمل مصادقة المستخدمين وتفويضهم والتدقيق في صلاحياتهم

أمن الشبكات
لوائح تفصيلية لتهيئة شبكات آمنة وتطبيق جدران الحماية والتصدي للتهديدات الإلكترونية

قانون أمن البنية التحتية الحيوية 2018

صُمّم هذا القانون تحديداً لتعزيز أمن قطاعات البنية التحتية الحيوية في أستراليا، وتشمل الطاقة والاتصالات والخدمات المالية والمياه والصحة والنقل

التزامات الإبلاغ
يتعين على مزودي البنية التحتية الحيوية الإبلاغ عن الحوادث الإلكترونية الجسيمة، مما يُعزز تبادل المعلومات الاستخباراتية حول التهديدات وتنسيق الاستجابة في القطاعات الحيوية
.

صلاحيات الحكومة
يمنح التشريع الحكومة صلاحيات محددة للاستجابة لحوادث الأمن الإلكترونية الكبرى في قطاعات البنية التحتية الحيوية والتخفيف من حدتها، مما يُؤكد أهمية تأمين الخدمات الأساسية

تنظيم البيانات: تحليل مقارن للقوانين الأسترالية مقارنةً بالقوانين العالمية

تمتد مخاوف حماية البيانات والخصوصية عبر الحدود، مما أفضى إلى تباين الأطر القانونية. وعلى الرغم من توافق أستراليا مع المبادئ الدولية، فإنها تتبنى مقاربات فريدة، لا سيما في مجال تحليل البيانات المحلية. ويُعدّ التنقل في هذا المشهد التنظيمي المعقد أمراً لا غنى عنه للمؤسسات لضمان امتثال البيانات وأمنها عبر الحدود

سنستعرض فيما يلي القوانين الأسترالية للبيانات مقارنةً بقوانين الولايات المتحدة وكندا والاتحاد الأوروبي والمملكة المتحدة ومنطقة الشرق الأوسط وأفريقيا، مع إبراز أوجه الاختلاف والتشابه

الدولة	أستراليا	الولايات المتحدة	كندا	الاتحاد الأوروبي	المملكة المتحدة	الشرق الأوسط وأفريقيا
القوانين المنظِّمة	قانون الخصوصية 1988	قوانين خاصة بكل قطاع (HIPAA مثل) وولاية	يسري على PIPEDA – الأنشطة التجارية	اللائحة العامة لحماية البيانات (GDPR)	قانون حماية البيانات البريطاني و UK GDPR	تتباين بحسب الدولة؛ بعضها شامل والبعض قطاعي
الموافقة	يجب الحصول على موافقة الأفراد لجمع معلوماتهم واستخدامها والإفصاح عنها	تتباين تباينا كبيرا بين الولايات	موافقة مستنيرة مع الشفافية وحق التحكم	تركيز قوي على الموافقة وحق المحو والقرار الآلي	الأوروبي GDPR متوافقة مع	مناهج متباينة؛ بعضها وأخرى أكثر GDPR يحاكي مرونة
العقوبات	حتى 10 مليون دولار أسترالي أو 10% من حجم الأعمال السنوي	غرامات وإجراءات قانونية وعقوبات تنظيمية	غرامات مالية؛ يجري تعديل القانون لرفع العقوبات	حتى 4% من حجم الأعمال العالمي السنوي	الأوروبي GDPR متوافقة مع	أقل صرامة مقارنةً بـ GDPR

تطبيق سيادة البيانات

يستلزم تطبيق سيادة البيانات اتباع نهج مزدوج: استراتيجية واضحة المعالم، إلى جانب نشر الحلول التقنية المناسبة

تستوجب الاستراتيجية الواضحة المعالم تعاون الشركات مع خبراء قانونيين ومسؤولي حماية البيانات وفرق تقنية المعلومات لصياغة

- فهم المتطلبات القانونية
- تقييم مخاطر البيانات
- وضع تصنيف للبيانات
- صياغة السياسات وإقرارها
- إجراء عمليات تدقيق دورية ومراجعات الامتثال

ولذلك، يُعدّ التعامل مع تطبيق هذه الاستراتيجية بأسلوب منظم وشامل باستخدام أفضل الممارسات أمراً بالغ الأهمية.
ولضمان نشر الحلول التقنية المناسبة، ينبغي على الشركات تقييم خياراتها واختيار ما يلبي احتياجاتها في مجال سيادة البيانات، ويشمل ذلك

- مزودو الخدمات السحابية الذين يوفرون مراكز بيانات محلية
- أدوات التشفير لحماية البيانات والمعلومات الشخصية التعريفية (PII)
- أنظمة إدارة صلاحيات الوصول
- حلول منع فقدان البيانات
- أطر آمنة لمشاركة البيانات

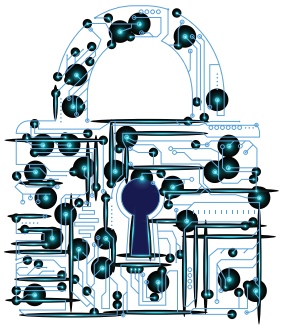
التحديات

- الموازنة بين إمكانية الوصول إلى البيانات ومتطلبات السيادة
- الاستثمار في آليات الحوكمة غير المُدرّة للإيرادات
- الامتثال لاختصاصات قانونية متعددة وعمليات نقل البيانات عبر الحدود وبروتوكولات الأمن والاتفاقيات المعمول بها

إرشادات أفضل الممارسات

أفضل الممارسات	إرشادات
فهم المنظومة التنظيمية	الالتزام بقوانين البيانات العالمية والإقليمية ومتطلبات الإقامة والتغييرات التنظيمية من خلال دمجها في استراتيجية البيانات الخاصة بكم
إطار حوكمة البيانات	وضع إطار متين لحوكمة البيانات يشمل السياسات والعمليات والتقنيات الخاصة بسيادة البيانات، وضمان التعاون الوثيق مع الفرق القانونية وفرق الامتثال لمواءمة الممارسات مع السياسات المؤسسية
الاتفاقيات القانونية	وإنفاذها بما يتضمن متطلبات سيادة البيانات وتدابير الامتثال (SLAs) صياغة العقود واتفاقيات مستوى الخدمة
حقوق أصحاب البيانات	إرساء إدارة حقوق البيانات لصون حقوق أصحاب البيانات، بما تشمل: الموافقة المستنيرة والوصول والتصحيح والمحو والاعتراض وقيود المعالجة. وتطبيق منظومة لتتبع هذه الطلبات والاستجابة لها
إرساء إدارة حقوق البيانات لصون حقوق أصحاب البيانات،	إجراء تقييمات لأثر البيانات لفهم المخاطر والانعكاسات المحتملة لمعالجة البيانات في اختصاصات قانونية مختلفة
عملية إدارة اختراق البيانات	وضع عمليات إدارة الاختراقات وخطة الاستجابة للحوادث واختبار الإجراءات التصحيحية لحماية البيانات. ينبغي أن تشمل العملية • مراجعة الحوادث مع الجهة التنظيمية المختصة • الاستجابة الفورية من قبل مراقب البيانات و/أو المعالج • تطبيق الإجراءات التصحيحية الدائمة التي تفرضها الجهة التنظيمية
تصنيف البيانات	تصنيف البيانات والتعامل معها وفق درجة حساسيتها ومتطلبات الامتثال لضمان الالتزام
حذف البيانات والاحتفاظ بها	وضع سياسات واضحة وتطبيق عمليات للحذف الآمن والدائم للبيانات عند انتهاء الحاجة إليها
إدارة الوصول	تطبيق ضوابط وصول قوية وتشفير ومصادقة لحماية البيانات الحساسة، وضمان التحديث المنتظم لصلاحيات الوصول وفق المهام الوظيفية
التدقيق والمراقبة	التدقيق المنتظم في ممارسات البيانات ومراقبتها لضمان الامتثال، والاستفادة من سجلات التتبع لرصد الوصول إلى البيانات، وتطبيق إجراءات تصحيحية للمخالفات كما هو موثق في نتائج التدقيق، بما يشمل إخطار الجهة التنظيمية المختصة
تدريب الموظفين	إجراء برامج تدريبية شاملة في مجال حماية البيانات لجميع الموظفين بصفة منتظمة، تتناول • أهمية حماية البيانات وتبعات الإخلال بها • تعريف البيانات الشخصية • حقوق أصحاب البيانات • مسؤوليات الجهة والأفراد • إجراءات الإخطار وإدارة اختراق البيانات

يُمكّن دمج أفضل الممارسات في منهجية سيادة البيانات المؤسساتِ من التعامل مع قوانين حماية البيانات المعقدة، وضمان الامتثال والاستفادة من التقنيات الحديثة



سيادة البيانات

القوانين والتحديات وأفضل الممارسات

WHITEPAPER

Authors:
Ali Manzoor, Head of Information Technology
Rafay Kazi, Country Director Australia and New Zealand
Fatima Naqvi, Manager Digital Communications

tenx.ai

info@tenx.ai

TenX
شركة استشارية عالمية حائزة على جوائز في مجالات الذكاء الاصطناعي وتحليلات البيانات وتطوير البرمجيات. نُساعد الشركات من خلال حلولنا المخصصة على أتمتة العمليات وتعزيز الإيرادات وتحسين التكاليف
أتاح نموذج تعاملنا الذي يضع العميل في صدارة اهتمامنا تحقيق تعاون سلس وتنفيذ ناجح لأكثر من 130 مشروعاً على المستوى العالمي في أمريكا الشمالية وأستراليا والشرق الأوسط وجنوب آسيا، وذلك عبر قطاعات متنوعة تشمل: الخدمات المالية والاتصالات والتقنيات الحيوية والرعاية الصحية والرياضة والترفيه والسفر واللوجستيات والقطاع الحكومي