الإصدار 1.0

إطار عمل الخصوصية
من المعهد الوطني للمعايير والتكنولوجيا:
أداة لتحسين الخصوصية
من خلال إدارة المخاطر المؤسسية – الإصدار 1.0

16 يناير 2020

هذا المنشور متاح مجانًا على الرابط التالي:

https://doi.org/10.6028/NIST.CSWP.10.ara

National Institute of Standards and Technology
U.S. Department of Commerce

الملخص التنفيذي

على مدار أكثر من عقدين من الزمن، قدمت شبكة الإنترنت وتكنولوجيا المعلومات المرتبطة بها ابتكارات غير مسبوقة أضافت قيمة اقتصادية كبيرة وحسّنت العديد من الخدمات الاجتماعية. وتحققت كل تلك الإنجازات عبر البيانات التي كانت تتوفر عن الأفراد في رحاب ذلك الفضاء شديد التعقيد. ولم يكن في إمكان العديد من الأفراد، بسبب هذا التعقيد، فهم تبعات تفاعلهم مع الأنظمة والمنتجات والخدمات المختلفة على خصوصياتهم، ولم تتمكن حتى المؤسسات نفسها من إدراك تبعات ما تقوم به على الأفراد أو المجتمع أو المشروعات وحتى على علاماتهم التجارية نفسها وأعمالهم وآفاق نموهم المستقبلي.

وانطلاقاً مما سبق، قام "المعهد الوطني للمعايير والتكنولوجيا" (اختصاراً "المعهد") بإجراء عملية شفافة شارك فيها أصحاب مصلحة متنوعين من القطاعين العام والخاص نتج عنها "إطار عمل الخصوصية: أداة لتحسين الخصوصية من خلال إدارة المخاطر المؤسسية" (اختصاراً: "إطار عمل الخصوصية" أو "الإطار"). وتهدف الأداة التطوعية هذه إلى المساعدة في تحسين ممارسات إعداد الخصوصية لدى المؤسسات بطريقة تزيد من قدرتها على دعم الخصوصية عبر تصميم المفاهيم المتصلة بالخصوصية، وأيضاً مساعدة المؤسسات على حماية خصوصية الأفراد عموماً. ويمكن لإطار عمل الخصوصية مساعدة المؤسسات فيما يتعلق بكل مما يلي:

- كسب ثقة العملاء عبر من خلال عرض كيف أن عملية تصميم ونشر المنتجات والخدمات تتم بشكل أخلاقي، وكيف يتم الاستفادة من البيانات بأفضل شكل ممكن مع تقليل العواقب السلبية على خصوصية الأفراد والمجتمع ككل.[1]
- الوفاء بالتزامات الامتثال الحالية، والتأكد من تلبية أي منتجات وخدمات مستقبلية لهذه الالتزامات أيضاً (خصوصاً في ظل بيئة تكنولوجية وسياسية متغيرة).
- تسهيل التواصل بين الأفراد وشركاء الأعمال وجهات التقييم والتنظيم والرقابة بشأن ممارسات الخصوصية.

ولا يوجد حل واحد يناسب الجميع عندما يتعلق الأمر بالجمع بين استخلاص الفوائد من البيانات وإدارة المخاطر المهددة لخصوصية الأفراد، لكن يشبه الأمر – في الوقت نفسه – بناء منزل؛ فصحيح أن في إمكان قاطني المنزل اتخاذ القرارات المتعلقة بتصميمه ومظهره الخارجي، لكن يجب أن يكون لهذا المنزل في المقام الأول هياكل مشيّدة بشكل راسخ ويُعتمد عليها. وبشكل مشابه، ينبغي أن يتيح مفهوم "حماية الخصوصية" إمكانية اتخاذ الأفراد للخيارات المناسبة لهم طالما أن تصميم المنتجات والخدمات يقدم بدوره إجراءات فاعلة تعمل على التخفيف من مخاطر الخصوصية. ويتسم إطار عمل الخصوصية بالمرونة التي تلبي مختلف احتياجات الخصوصية على اعتبار أنه يقدّم نهجاً قائماً على المخاطر والنتائج، ويعطي القدرة على إنشاء حلول أكثر ابتكاراً وفاعلية قادرة على تحقيق نتائج أفضل للأفراد والمؤسسات، ومواكبة الاتجاهات التكنولوجية السائدة (مثل الذكاء الاصطناعي وإنترنت الأشياء).

ويتّبع إطار عمل الخصوصية نفس الهيكلية التي اتبعها إطار عمل تحسين الأمن السيبراني للبنية التحتية الحرجة (إطار عمل الأمن السيبراني) [1] بهدف تسهيل استخدام كلا الإطارين مع بعضها البعض. ويتألف إطار عمل الخصوصية، كما هو الحال في إطار عمل الأمن السيبراني، من ثلاثة أجزاء: النواة، وملفات التعريف، ومستويات التنفيذ. وتعزز هذه الأجزاء الثلاثة إدارة مخاطر الخصوصية من خلال ربطها بين أساسياً الأعمال والمهام والأدوار والمسؤوليات التنظيمية وأنشطة حماية الخصوصية.

- تساعد **النواة** على إقامة حوار حول الأنشطة المهمة لحماية الخصوصية والنتائج المنشودة؛ من المستوى التنفيذي إلى مستوى العمليات/ التنفيذ.

[1] لا يوجد معيار موضوعي لاتخاذ القرارات الأخلاقية، على اعتبار أنها مستقاة من المعايير والقيم والتوقعات القانونية في مجتمع معين.

- تمنح **ملفات التعريف** القدرة على الترتيب بحسب الأولوية النتائج والأنشطة التي تحقق على أفضل وجه قيم الخصوصية المؤسسية والمهمة أو احتياجات العمل والمخاطر.
- تعمل **مستويات التنفيذ** على دعم اتخاذ القرار والتواصل حول مدى ملاءمة العمليات والموارد التنظيمية لإدارة مخاطر الخصوصية.

وإيجازاً لما سبق، يهدف إطار عمل الخصوصية إلى مساعدة المؤسسات على بناء أسس أفضل للخصوصية من خلال إدراج المخاطر المتصلة بالخصوصية ضمن محفظة المخاطر الأوسع للمؤسسة.

شكر وتقدير

جاء هذا المنشور نتيجةً لجهد تعاوني بين المعهد الوطني للمعايير والتكنولوجيا وبين مؤسسات وأفراد مهمتين بهذا الموضوع من القطاعين العام والخاص. واعتمد المعهد، أثناء إعداد الإطار، على ثلاث ورش عمل عامة، وطلب للمعلومات، وطلب للملاحظات، وخمس ندوات عبر الإنترنت، ومئات من التفاعلات المباشرة مع أصحاب المصلحة[2]. يتقدم المعهد بالشكر والتقدير لكل من ساهم في إعداد هذا المنشور.

[2] يتوفر الأرشيف بالكامل على الرابط التالي: https://www.nist.gov/privacy-framework.

جدول المحتويات

قائمة الأشكال

قائمة الجداول

1.0 مقدمة إلى إطار عمل الخصوصية

على مدار أكثر من عقدين من الزمن، قدمت شبكة الإنترنت وتكنولوجيا المعلومات المرتبطة بها ابتكارات غير مسبوقة أضافت قيمة اقتصادية كبيرة وحسّنت العديد من الخدمات الاجتماعية. وتحققت كل تلك الإنجازات عبر البيانات التي كانت تتوفر عن الأفراد في رحاب ذلك الفضاء شديد التعقيد. ولم يكن في إمكان العديد من الأفراد، بسبب هذا التعقيد، فهم تبعات تفاعلهم مع الأنظمة والمنتجات والخدمات المختلفة على خصوصياتهم، ولم تتمكن حتى المؤسسات نفسها من إدراك تبعات ما تقوم به على الأفراد أو المجتمع أو المشروعات وحتى على علاماتهم التجارية نفسها وأعمالهم وآفاق نموهم المستقبلي. وليس من السهولة بمكان إيجاد طريقة يمكن فيها مواصلة جني الفوائد من معالجة البيانات مع حماية خصوصية الأفراد في الوقت نفسه، فضلاً عن أنه لا يوجد حل واحد يناسب للجميع.

ويمثل مفهوم "الخصوصية" في حد ذاته تحدياً على اعتبار أنه لا يوجد "مفهوم جامع" لكل القيم المهمة (مثل استقلالية الإنسان وكرامته)، فضلاً عن وجود اختلاف أيضاً في الوسائل الكفيلة بحماية تلك القيم.[3] فعلى سبيل المثال، يمكن تحقيق الخصوصية من خلال العزلة، أو الحد من المراقبة، أو بمنح الأفراد القدرة على التحكم في الجوانب المتصلة بهويتهم (مثل جسد المرء وبياناته وسمعته).[4] وإضافةً إلى ما سبق، لا تعتبر "استقلالية الإنسان وكرامته" مفاهيم ثابتة قابلة للقياس، إذ تختلف النظرة إليها بين كل ثقافة وأخرى، بل وحتى بين كل شخص وآخر، وهو ما يُصعّب أي عمليات تواصل قد تحدث لمناقشة مخاطر الخصوصية داخل المؤسسات وفيما بين تلك المؤسسات وحتى مع الأفراد، في سبب يعود إلى عدم وجود لغة مشتركة ولا أداة عملية تتسم بالمرونة الكافية لتلبية الاحتياجات المتنوعة للخصوصية.

ويتمثل الهدف من "إطار عمل الخصوصية" هذا في تمكين المؤسسات – على اختلاف حجمها – من استخدامه بغض النظر عن التقنية أو القطاع أو القانون أو الولاية القضائية لها، حيث يتمثل الغرض منه في مساعدتها على إدارة مخاطر الخصوصية باستخدام نهج مشترك قابل للتطويع وفقاً لدورها (أدوارها) في منظومة معالجة البيانات، وذلك من خلال:

- أخذ الخصوصية بعين الاعتبار عند تصميم ونشر الأنظمة والمنتجات والخدمات التي تؤثر على الأفراد.
- التواصل بشأن ممارسات الخصوصية.
- تشجيع التعاون بين موظفي المؤسسات المختلفة (كالتعاون بين المديرين التنفيذيين، وموظفي الشؤون القانونية، وفرق تكنولوجيا المعلومات) عبر وضع ملفات التعريف واختيار المستويات وتحقيق النتائج.

---

[3] يتناول الإعلان العالمي لحقوق الإنسان التابع للأمم المتحدة مفهومي "الاستقلالية" و"الكرامة". والإعلان متاح على الرابط التالي: https://www.un.org/en/universal-declaration-human-rights/

[4] ثمة منشورات عديدة تتناول بالتفصيل المعلومات الأساسية عن الخصوصية، أو مختلف جوانب هذا المفهوم. المثال الأول هو Solove D (2010) *Understanding Privacy*- [فهم الخصوصية] (دار نشر جامعة هارفارد، كامبريدج، ماساتشوستس)، https://ssrn.com/abstract=1127888؛ والمثال الثاني هو Selinger E, Hartzog W (2017) - *Obscurity and Privacy, Spaces for the Future: A Companion to Philosophy of Technology* [الغموض والخصوصية، مجالات المستقبل: رفيق فلسفة التكنولوجيا]، المحرر Pitt J, Shew A (Taylor & Francis)، نيويورك)، الفصل 12، الطبعة الأولى، https://doi.org/10.4324/9780203735657

1.1 لمحة عامة عن إطار عمل الخصوصية

يتألف إطار عمل الخصوصية من ثلاثة أجزاء يوضحها الشكل 1: النواة وملفات التعريف ومستويات التنفيذ. ويساهم كل مكوّن من تلك المكونات الثلاثة في تحسين الطريقة التي تتبعها المؤسسة فيما يتعلق بإدارة مخاطر الخصوصية من خلال الربط بين محركات الأعمال أو المهام والأدوار التنظيمية والمسؤوليات وبين أنشطة حماية الخصوصية. وستتناول ذلك بالتفصيل في القسم 2:

شكل 1: الهيكل الأساسي وملفات التعريف ومستويات التنفيذ

- *النواة* هي مجموعة من الأنشطة والنواتج المتصلة بحماية الخصوصية والتي تساعد في توصيل أنشطة ونواتج الخصوصية – مرتبة بحسب الأولوية – إلى المؤسسة (من مستوى المدراء التنفيذيين إلى مستوى العمليات/التنفيذ). وينقسم النواة كذلك إلى فئات رئيسية وفئات فرعية لكل وظيفة، والتي هي نواتج متفردة بذاتها.

- تمثل *ملفات التعريف* أنشطة الخصوصية الحالية أو النواتج التي تنشد المؤسسة تحقيقها. ويمكن للمؤسسة إعداد ملف تعريف عبر مراجعة جميع النتائج والأنشطة المُدرجة في *النواة* لتحديد أيها يجب التركيز عليه (انطلاقاً من أعمال أو مهمة المؤسسة، ودورها (أدوارها) في منظومة معالجة البيانات، وأنواع معالجة البيانات، واحتياجات الخصوصية للأفراد). كما يمكن للمؤسسة إنشاء أو إضافة وظائف وفئات رئيسية وفئات فرعية حسب الحاجة. ويمكن استخدام ملفات التعريف لتحديد الفرص المتاحة الكفيلة بتحسين وضع الخصوصية لديها، ويمكنها القيام بذلك عبر مقارنة ملف التعريف "الحالي" (الوضع "الراهن") بملف التعريف "المستهدف" (الوضع "المستهدف"). ويمكن استخدام ملفات التعريف أيضاً لإجراء تقييمات ذاتية وللتواصل داخل المؤسسة أو بين المؤسسات حول كيفية إدارة مخاطر الخصوصية.

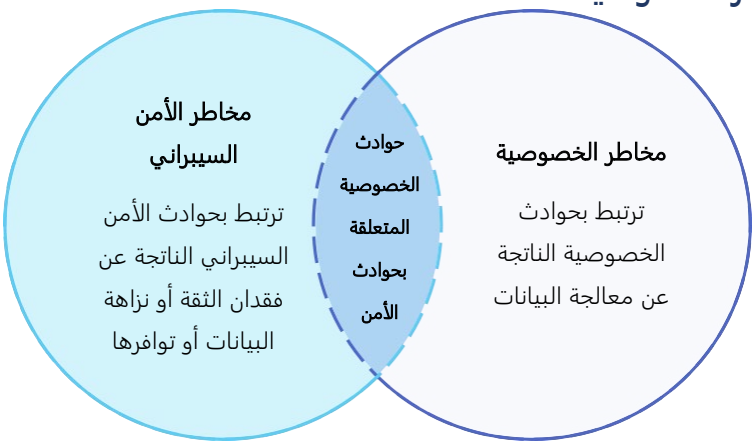
- تقدم *مستويات التنفيذ* نقطة مرجعية للطريقة التي تنظر فيها المؤسسة إلى مخاطر الخصوصية، وما إذا كان لديها عمليات وموارد كافية لإدارة المخاطر، فضلاً عن أنها تعكس التقدم المحرز من الاستجابات والملاحظات غير الرسمية ضمن نُهج يتسم بالمرونة والوعي بالمخاطر. وينبغي على المؤسسة، عند اختيار مستويات التنفيذ، أخذ ملف (أو ملفات) التعريف المستهدفة الخاصة بها في الاعتبار، وكيف يمكن لممارسات إدارة المخاطر الحالية دعم إنجاز هذه المستويات أو عرقلتها، ونسبة إدراج مخاطر الخصوصية ضمن محفظة إدارة المخاطر المؤسسية، والعلاقات في منظومة معالجة بيانات المؤسسة، وتشكيل القوى العاملة وبرنامج التدريب.

1.2 إدارة مخاطر الخصوصية

لا يزال موضوع إدارة المخاطر المؤسسية محدود الفهم ولدى بعض المؤسسات فقط.[5] ويقدم هذا القسم المفاهيم والاعتبارات التي قد تستخدمها المؤسسات لتطوير إدارة مخاطر الخصوصية أو تحسينها أو توصيلها بهدف زيادة فهمها لهذا الموضوع، بينما يتضمن الملحق (د) معلومات إضافية حول أهم الممارسات.

1.2.1 إدارة مخاطر الأمن السيبراني ومخاطر الخصوصية

ساعد إطار عمل الأمن السيبراني، منذ إطلاقه في عام 2014، المؤسسات على التواصل وإدارة المخاطر المتصلة بالأمن السيبراني[1]. ورغم وجود بعض الأمور المشتركة بين إدارة مخاطر الأمن السيبراني وإدارة مخاطر الخصوصية، لكن لا يوجد تطابق بينهما على اعتبار إمكانية حدوث مخاطر متصلة بالخصوصية خارج نطاق الأمن السيبراني أيضاً، كما يوضح الشكل 2. ويمكن أن تساعد الدراية بمختلف الأصول لمخاطر الأمن السيبراني ومخاطر الخصوصية تحديد الحلول الأكثر كفاءة للتعاطي معها.



شكل 2: العلاقة بين مخاطر الأمن السيبراني ومخاطر الخصوصية

إجراء متعلق بالبيانات
عملية دورة حياة البيانات (تشمل على سبيل المثال لا الحصر، جمع البيانات والاحتفاظ بها وتسجيلها وتوليدها وتحويلها واستخدامها والإفصاح عنها ومشاركتها ونقلها والتخلص منها).

معالجة البيانات
الجمع لإجراء متعلق بالبيانات

ويتمثل نهج إطار عمل الخصوصية فيما يتعلق بمخاطر الخصوصية في رؤية *حوادث الخصوصية* على أنها مشكلات محتملة قد يواجهها الأفراد نتيجة لتعامل النظام أو المنتجات أو الخدمات مع بياناتهم، الرقمية أو غير الرقمية، على امتداد دورة حياة تلك البيانات (أي من جمعها إلى التخلص منها).

ويصف إطار عمل الخصوصية العمليات المتصلة بالبيانات إما بصيغة "المفرد" كما في حالة "*إجراء متعلق بالبيانات*" أو بصيغة "الجمع" كما في حالة "*معالجة البيانات*"، حيث يمكن التعبير عن المشكلات التي قد يواجهها الأفراد نتيجة معالجة بياناتهم بطرق مختلفة: من الآثار المتعلقة بالكرامة (مثل الإحراج أو الوصم الاجتماعي)، وصولاً إلى الأضرار الملموسة (مثل التمييز أو الخسارة الاقتصادية أو الضرر المادي).[6]

تختلف المشكلات التي يواجهها فرد وآخر، حيث يُظهر الشكل 2 كيف تنشأ المشكلات لدى مؤسسة كإحدى الآثار السلبية لعمليات معالجتها للبيانات (والتي تجريها تلك المؤسسة بهدف تحقيق مهمتها أو أهداف أعمالها). ومن إحدى الأمثلة حول هذا الأمور المخاوف التي أبدتها

[5] انظر *Summary Analysis of the Responses to the NIST Privacy Framework Request for Information* [التحليل الموجز للاستجابة لطلب المعلومات الخاص بإطار عمل الخصوصية الذي وضعه المعهد الوطني للمعايير والتكنولوجيا] [2]، صفحة 7.

[6] قام المعهد بإنشاء دليل توضيحي بالمشكلات لاستخدامه في تقييم مخاطر الخصوصية. راجع *NIST Privacy Risk Assessment Methodology* [منهجية تقييم مخاطر الخصوصية الخاصة بالمعهد] [3]. ربما قد تكون مؤسسات أخرى قائمة قد وضعت فئات مختلفة أخرى من المشكلات، أو قد تشير إليها بأنها عواقب أو أضرار وخيمة.

بعض المجتمعات من تركيب "العدادات الذكية" كجزء من الشبكة الذكية والتي كانت فيها الحكومة تستهدف زيادة كفاءة الطاقة.[7] كانت تلك العدادات قادرة على جمع وتسجيل وتقديم معلومات دقيقة للغاية حول استخدام كل منزل للكهرباء، وهو ما من شأنه أن يوفر رؤى مهمة حول سلوك الأفراد داخل منازلهم[8]. ورغم عمل هذه العدادات وفق النحو المنشود منها، تسببت معالجة البيانات الناتجة عنها في شعور المواطنين بأنهم قيد المراقبة.

وفي عالم يتزايد الترابط والتواصل فيه تعقيداً، يُمكن أن تنشأ بعض المشكلات فقط من مجرد تفاعلات الأفراد مع الأنظمة والمنتجات والخدمات، حتى عندما لا تكون البيانات التي تتم معالجتها مرتبطة ارتباطاً مباشراً بأفراد يمكن التعرف عليهم. فعلى سبيل المثال، يمكن استخدام تقنيات المدن الذكية لتغيير سلوك الأشخاص أو التأثير عليهم في أماكن محدد أو خلال تنقلهم عبر المدينة[9]. كما يمكن أن تنشأ مشكلات عند فقدان *البيانات لسريتها* أو *نزاهتها* أو *توافرها* ضمن إحدى مراحل معالجتها (كما في حالة سرقتها على يد مخترقين خارجيين، أو وصول موظفين غير مصرح لهم إلى تلك البيانات، أو إساءة استخدام تلك البيانات). ويوضح الشكل 2 أنواع حوادث الخصوصية المتعلقة بالأمن السيبراني (مثل التداخل بين مخاطر الخصوصية والأمن السيبراني).

ويمكن للمؤسسة إجراء "تقييم للأثر" (نقطة تتلاقي مخاطر الخصوصية مع المخاطر التنظيمية) بمجرد تمكنها من تحديد احتمالية حدوث مشكلة ما نتيجة معالجة البيانات (والتي يشير إليها إطار عمل الخصوصية بعبارة *إجراءات بيانات إشكالية)*. ويختبر الأفراد، فرادى أم جماعات (وحتى على مستوى المجتمع المحلي) التأثير المباشر للمشكلات، حيث قد تواجه المؤسسة نتيجةً لذلك بعض الآثار (كالتكاليف الناتجة عن عدم الامتثال، أو فقد الإيرادات الناتجة عن مقاطعة العملاء لمنتجاتها وخدماتها، أو تضرر سمعتها الخارجية أو ثقافتها الداخلية). وعادةً ما تدير المؤسسات هذه الآثار عبر إدارة المخاطر المؤسسية، حيث يمكن لها الموازنة بين مخاطر الخصوصية وباقي المخاطر في محفظتها الأوسع عبر ربط المشكلات التي يواجهها الأفراد بالتأثيرات التنظيمية المفهومة، وبالتالي تُتخذ قرارات مستنيرة حول تخصيص الموارد لتعزيز برامج الخصوصية. ويوضح الشكل 3 العلاقة بين مخاطر الخصوصية والمخاطر التنظيمية.

شكل 3: العلاقة بين مخاطر الخصوصية والمخاطر التنظيمية

[7] انظر، على سبيل المثال، تقرير مشترك بين الوكالات أو التقرير الداخلي للمعهد الوطني للمعايير والتكنولوجيا رقم 7628 المراجعة 1، المجلد 1، *Guidelines for Smart Grid Cybersecurity: Volume 1 – Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements* [المبادئ التوجيهية لتنفيذ الأمن السيبراني للشبكة الذكية: المجلد 1 - استراتيجية الأمن السيبراني للشبكة الذكية، وبنيتها الهندسية، والمتطلبات عالية المستوى] [4] صفحة 26.

[8] انظر التقرير الداخلي للمعهد رقم 8062، *An Introduction to Privacy Engineering and Risk Management in Federal Systems* [مقدمة لهندسة الخصوصية وإدارة المخاطر في الأنظمة الفيدرالية] [5] صفحة 2. للاطلاع على أنواع إضافية من مخاطر الخصوصية المرتبطة بالتأثيرات الضارة على الأفراد أثناء معالجة البيانات، راجع الملحق هـ من تقرير المعهد المشار له.

[9] انظر Newcombe T (2016) - *Security, Privacy, Governance Concerns About Smart City Technologies Grow. Government Technology* [زيادة مخاوف الأمن والخصوصية والحوكمة نتيجة تقنيات المدن الذكية. التكنولوجيا الحكومية]. والمتاح على الرابط https://bit.ly/3vgRYr8.

1.2.2 تقييم مخاطر الخصوصية

يتم إدارة مخاطر الخصوصية عبر مجموعة عمليات تتم على امتداد المؤسسة وتساعدها على فهم ما تسببه أنظمتها ومنتجاتها وخدماتها من أي مشكلات محتملة لدى الأفراد، وكيفية إنشاء حلول فعالة لإدارة تلك المشاكل. و*تقييم مخاطر الخصوصية* هو عملية فرعية تهدف إلى تحديد مخاطر الخصوصية وتقييمها لاستخلاص المعلومات الكفيلة بمساعدة المؤسسة على الموازنة بين فوائد معالجتها للبيانات والمخاطر المحتملة، ثم تحديد الطرق المناسبة للاستجابة (في عملية يشار إليها أحياناً باسم "التناسبية").[10] وتختلف كل مؤسسة عن أخرى في طريقة ترتيبها لمخاطر الخصوصية والاستجابة لها (أي ترتيبها بحسب التأثير المحتمل على الأفراد، وعلى المؤسسة ذاتها). وتشمل نُهج الاستجابة لهذه المخاطر ما يلي:[11]

- الحد من المخاطر: قد تُطبق المؤسسة مثلاً إجراءات فنية و/أو سياسات تقلل من المخاطر إلى حدٍ مقبول؛
- نقل المخاطر أو تقاسمها مع جهة أخرى: تعتبر "العقود" مثلاً وسيلة لنقل/تشارك المخاطر مع مؤسسات أخرى، بينما تعتبر "إشعارات الخصوصية"/"اتفاقيات المستخدم" وسائل لتشارك المخاطر مع الأفراد؛
- تجنّب المخاطر: قد تقرر المؤسسة مثلاً أن المخاطر تفوق الفوائد، وقد تتوقف بالتالي عن معالجة البيانات.
- قبول المخاطر: قد تقرر المؤسسة مثلاً أن المشكلات التي يواجهها الأفراد هيّنة، أو غير محتملة؛ بالتالي تفوق الفوائد المخاطر، وليس من الضروري استثمار أي موارد في تخفيف المخاطر.

وكما أوضحنا أنفاً، تعتبر عمليات تقييم مخاطر الخصوصية عمليات مهمة للغاية بسبب أهمية الخصوصية في حماية العديد من القيّم. وقد تختلف طرق حماية هذه القيم، وقد تتعارض مع بعضها. فإذا كانت المؤسسة تحاول تحقيق الخصوصية عبر الحد من المراقبة، فقد تطبّق تدابير مثل "البيانات الموزعة" أو "تقنيات التشفير" والتي تعزز الخصوصية وتخفي البيانات حتى عن المؤسسة ذاتها؛ لكن إذا كانت المؤسسة تحاول أيضاً تمكين التحكم الفردي، فقد تُدرج تدابير أخرى تتعارض بدورها مع التدابير المذكورة أعلاه. فعلى سبيل المثال، لنفرض مثلاً قيام فرد ما بتقديم طلب للوصول إلى بياناته لدى تلك المؤسسة؛ فإذا كانت المؤسسة قد استخدم طريقة حماية خصوصية يتم فيها توزيع تلك البيانات أو تشفيرها بطرق لا يمكنها هي نفسها الوصول إليها، فقد لا تتمكن من تزويد الفرد ببياناته. بالتالي، يُمكن لعمليات تقييم مخاطر الخصوصية مساعدة المؤسسة على فهم القيم الواجب عليها حمايتها، وطرق استخدامها للبيانات، وكيف يمكنها الموازنة بين تنفيذ تدابير مختلفة في سياق معين.

وأخيراً، تساعد عمليات تقييم مخاطر الخصوصية المؤسسات على التمييز بين مخاطر الخصوصية ومخاطر الامتثال، وهو ما يمكن أن يساعد في تحديد احتمال تسبب معالجة البيانات في مشاكل للأفراد، حتى عندما تكون المؤسسة ممتثلة كلياً للقوانين أو اللوائح الناظمة، في اتخاذ القرارات الأخلاقية المتعلقة بتصميم أو نشر النظام والمنتج والخدمة. وترتكز عملية اتخاذ القرارات الأخلاقية في العادة على المعايير والقيم والتوقعات القانونية السائدة ضمن مجتمع معين رغم عدم وجود معيار موضوعي لاتخاذ تلك القرارات، وهو ما يُسهل تحسين الاستخدامات المفيدة للبيانات مع تقليل العواقب السلبية على خصوصية الأفراد وعلى المجتمع ككل، فضلاً عن تجنب فقدان الثقة التي تضر بسمعة المؤسسة أو بطء اعتماد منتجاتها، أو حتى التخلي عن منتجاتها وخدماتها.

انظر الملحق (د) لمعلومات إضافية حول الجوانب التشغيلية لتقييم مخاطر الخصوصية.

---

[10] انظر مشرف حماية البيانات الأوروبي (2019) Necessity & Proportionality [الضرورة والتناسب]. متاح على الرابط https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en.

[11] انظر المنشور الخاص للمعهد الوطني للمعايير والتكنولوجيا 800 -39، Managing Information Security Risk: Organization, Mission, and Information System View [إدارة مخاطر أمن المعلومات: المؤسسة والمهمة وعرض نظام المعلومات] [6].

1.3 لمحة عامة عن الوثيقة

يتألف الجزء المتبقي من الوثيقة من الأقسام والملاحق التالية:

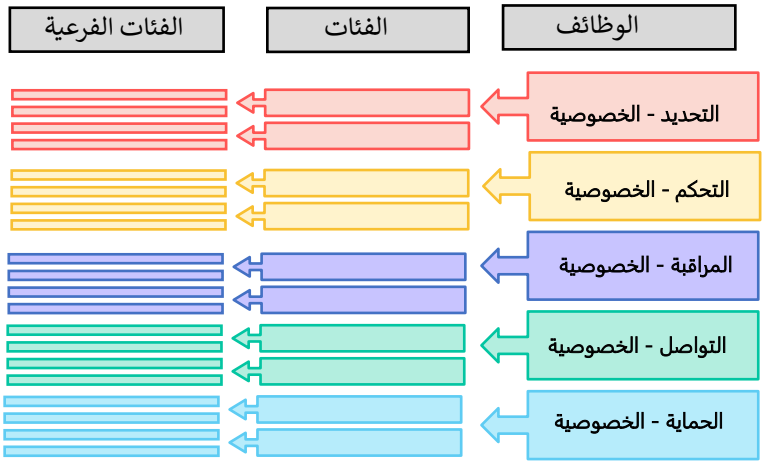
- **القسم الثاني** – يصف مكونات إطار عمل الخصوصية: النواة وملفات التعريف ومستويات التنفيذ.
- **القسم الثالث** – يعرض أمثلة حول كيفية استخدام إطار عمل الخصوصية.
- **قسم المراجع** - يسرد المراجع المستشهد بها في الوثيقة.
- **الملحق (أ)** – يتناول نواة إطار عمل الخصوصية في صورة جدول: الوظائف والفئات الرئيسية والفئات الفرعية.
- **الملحق (ب)** – يحتوي على مسرد بمصطلحات مختارة.
- **الملحق (ج)** - يسرد الاختصارات المستخدمة في هذه الوثيقة.
- **الملحق (د)** – يتناول الممارسات الرئيسية التي تُسهم في الإدارة الناجحة لمخاطر الخصوصية.
- **الملحق (هـ)** – يحدد مستويات التنفيذ.

2.0 أساسيات إطار عمل الخصوصية

يوفر إطار عمل الخصوصية لغة مشتركة لفهم مخاطر الخصوصية وإدارتها والتواصل بشأنها مع أصحاب المصلحة الداخليين والخارجيين، وهو قابل للتعديل بحيث يتناسب مع دور (أدوار) أي مؤسسة في منظومة معالجة البيانات. ويمكن استخدام الإطار للمساعدة في تحديد الإجراءات وترتيبها بحسب الأولوية للتقليل من مخاطر الخصوصية، فضلاً عن أنه أداة تساعد في مواءمة السياسات والأعمال والأساليب التكنولوجية لإدارة تلك المخاطر.

2.1 النواة

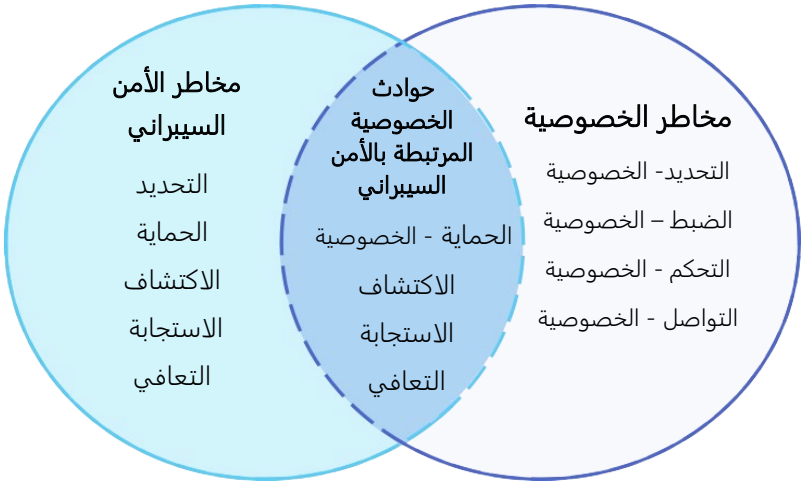
كما هو مبين في الملحق (أ)، يوفر النواة مجموعة مفصلة بشكل متزايد من الأنشطة والنتائج التي تتيح إجراء حوار حول إدارة مخاطر النواة إلى وظائف وفئات وفئات فرعية.



شكل 4: الهيكل الأساسي لإطار عمل الخصوصية

تعمل عناصر النواة معاً على النحو التالي:

- تعمل *الوظائف* على تنظيم أنشطة الخصوصية التأسيسية في أعلى مستوى، وتساعد المؤسسات في الإبلاغ عن إدارة مخاطر الخصوصية من خلال فهم معالجة البيانات وإدارتها، وتمكين اتخاذ القرارات المتصلة *بإدارة المخاطر*، وتحديد كيفية التفاعل مع الأفراد، والتحسّن من خلال التعلّم من الأنشطة السابقة. ولا يُقصد من النواة أن تشكل مساراً تسلسلياً أو أن تؤدي إلى حالة نهائية ثابتة مطلوبة، وإنما تنفيذ الوظائف بشكل متزامن ومستمر لتشكيل أو تعزيز ثقافة تشغيلية تعالج الطبيعة الديناميكية لمخاطر الخصوصية.
- تقوم *الفئات* بتقسيم الوظيفة إلى مجموعات من نواتج الخصوصية وترتبط بشدة باحتياجات البرامج وبأنشطة محددة.
- تقوم *الفئات الفرعية* أيضاً بتقسيم الفئة إلى نواتج محددة للأنشطة الفنية و/أو الإدارية، وتوفر مجموعة من النتائج التي تساعد في دعم تحقيق النتائج المنشودة في كل فئة، رغم أنها مجموعة غير شاملة.



شكل 5: استخدام الوظائف لإدارة الأمن السيبراني ومخاطر الخصوصية

ويمكن استخدام الوظائف الخمس، التحديد-، والضبط-، والتحكم-، والتواصل-، والحماية- (للخصوصية)، والمذكورة أدناه، لإدارة مخاطر الخصوصية الناشئة عن معالجة البيانات.[12] وتركز وظيفة الحماية-الخصوصية مثلاً على إدارة المخاطر المرتبطة بأحداث الخصوصية ضمن فضاء الأمن السيبراني (مثل *انتهاكات الخصوصية*). ويمكن الاستفادة من إطار عمل الأمن السيبراني لزيادة دعم إدارة المخاطر المرتبطة بأحداث الخصوصية باستخدام وظائف الاكتشاف والاستجابة والاستعادة رغم أن الإطار يستهدف تغطية جميع أنواع حوادث الأمن السيبراني. وبشكل بديل، قد تستخدم المؤسسات جميع وظائف إطار عمل الأمن السيبراني الخمس وأيضاً وظائف إطار عمل الخصوصية في موازاة مع التحديد-، والضبط-، والتحكم-، والتواصل-، والحماية- (للخصوصية)، للتعاطي مع مخاطر الخصوصية ومخاطر الأمن السيبراني معاً. ويستخدم الشكل 5 "مخطط فين" (Venn Diagram) الوارد في القسم 1.2.1 لتوضيح كيف يمكن استخدام الوظائف من كلا الإطارين في إدارة الجوانب المختلفة لمخاطر الخصوصية وأيضاً الأمن السيبراني. ويتم تحديد وظائف إطار عمل الخصوصية الخمس على النحو التالي:

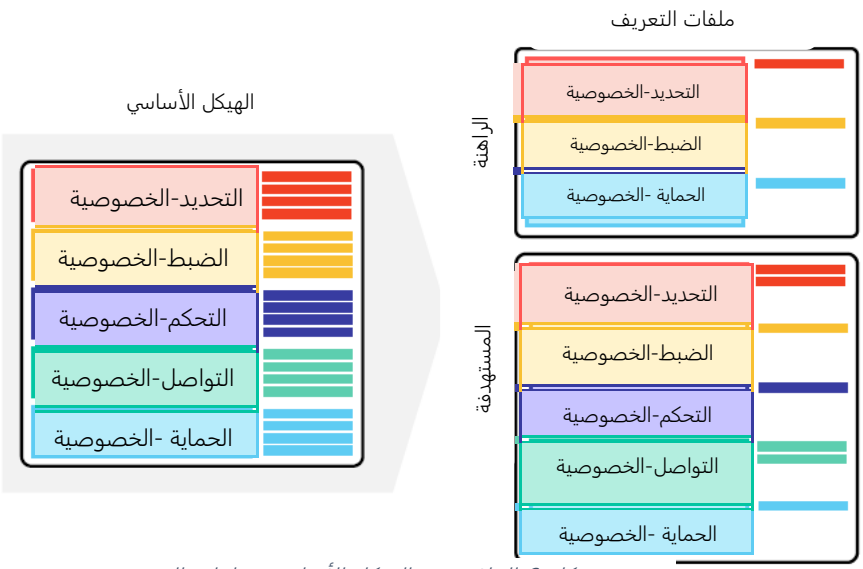
- *وظيفة التحديد–الخصوصية*: إعداد الفهم التنظيمي لإدارة مخاطر الخصوصية التي قد يتعرض إليها الأفراد جرّاء معالجة بياناتهم.
تعتبر أنشطة وظيفة التحديد-الخصوصية من الأنشطة الأساسية لتحقيق الاستخدام الأمثل لإطار عمل الخصوصية، على اعتبار أنها تساعد في حصر الظروف التي تتم فيها معالجة البيانات، وفهم اهتمامات الخصوصية للأفراد المستفيدين من المؤسسة أو المتأثرين بها بشكل مباشر أو غير مباشر، وإجراء تقييمات للمخاطر؛ وهو ما يعطي المؤسسة القدرة على فهم بيئة الأعمال التي تنشط فيها وتحديد مخاطر الخصوصية وتربيتها بحسب الأولوية.
- وظيفة *الضبط–الخصوصية*: إعداد وتنفيذ هيكل حوكمة تنظيمية يُمكّن من الفهم المستمر لأولويات إدارة المخاطر في المؤسسة انطلاقاً من مخاطر الخصوصية التي تم تحديدها.
تعتبر وظيفة الضبط–الخصوصية وظيفة أساسية أيضاً، لكنها تركز على الأنشطة المنفذة على المستوى التنظيمي (مثل إنشاء قيم وسياسات الخصوصية المؤسسية، وتحديد المتطلبات القانونية/التنظيمية، وفهم درجة تحمل المخاطر المؤسسية) والتي تساعد المؤسسة على تركيز جهودها وتحديد أولوياتها بما يتوافق مع استراتيجية إدارة المخاطر واحتياجات أعمالها.
- وظيفة *التحكم – الخصوصية:* وضع وتنفيذ الأنشطة المناسبة التي تعطي المؤسسات أو الأفراد القدرة على إدارة البيانات بدقة كافية فيما يتعلق بإدارة مخاطر الخصوصية.
تركز وظيفة التحكم – الخصوصية على إدارة معالجة البيانات من وجهة نظر المؤسسات والأفراد.

[12] وضعنا كلمة "-الخصوصية" بعد اسم كل وظيفة للإشارة إلى أن هذه الوظيفة ترتبط بإطار عمل الخصوصية لتجنب الخلط مع وظائف إطار عمل الأمن السيبراني.

- وظيفة *التواصل–الخصوصية*: إعداد وتنفيذ الأنشطة المناسبة لتمكين المؤسسات والأفراد من التحلي بفهم موثوق والمشاركة في حوار حول كيفية معالجة البيانات ومخاطر الخصوصية المرتبطة بها.
تُدرك وظيفة التواصل–الخصوصية حاجة المؤسسات والأفراد لمعرفة كيفية معالجة البيانات للتمكن من إدارة مخاطر الخصوصية بطريقة فعالة.
- وظيفة *الحماية–الخصوصية*: إعداد وتنفيذ الضمانات الوقائية المناسبة لمعالجة البيانات.
تتناول وظيفة الحماية–الخصوصية حماية البيانات من أجل منع حوادث الخصوصية المرتبطة بالأمن السيبراني، وأي تداخل بين إدارة مخاطر الخصوصية ومخاطر الأمن السيبراني.

2.2 ملفات التعريف

ملفات التعريف هي مجموعة من الوظائف، والفئات، والفئات الفرعية، المحددة انطلاقاً من النواة، والتي أعطتها المؤسسة الأولوية لمساعدتها في إدارة مخاطر الخصوصية. ويمكن استخدام هذه الملفات لوصف الحالة الراهنة والحالة المستهدفة المطلوبة لأنشطة خصوصية محددة. ويشير "ملف التعريف الراهن" إلى النتائج التي تحققها المؤسسة حالياً فيما يتعلق بالخصوصية، في حين يشير "ملف التعريف المستهدف" إلى النتائج التي ترغب في تحقيقها مستقبلاً فيما يتعلق بالخصوصية. ويمكن للمؤسسة استخدام الفروقات بين الملفين لتحديد الثغرات ووضع خطة عمل للتحسين وحشد الموارد المطلوبة للتحقيق النتائج المرغوبة (مثل تعيين الموظفين وجلب التمويل)، بحيث تحد المؤسسة من مخاطر الخصوصية بطريقة فعالة من حيث التكلفة ومرتبة بحسب الأولوية. ويمكن أن تساعد ملفات التعريف أيضاً في الإبلاغ عن المخاطر داخل المؤسسة وبين المؤسسات المختلفة لمساعدتها في فهم الحالة الحالية والمرغوبة لنتائج الخصوصية.



شكل 6. العلاقة بين الهيكل الأساسي وملفات التعريف

ولا يضع إطار عمل الخصوصية قوالب محددة لملفات التعريف (للسماح بمرونة في التنفيذ)، وقد لا تحتاج المؤسسة لتحقيق كل نتيجة أو نشاط وارد في النواة عند التطبيق.

ويمكن للمؤسسة، عند إعداد ملف التعريف، تحديد الوظائف، والفئات، والفئات الفرعية أو تخصيصها وفقاً لاحتياجاتها المحددة، بما في ذلك إنشاء وظائف، وفئات، وفئات فرعية إضافية خاصة بها تراعي مخاطرها التنظيمية الفريدة، وتضع في الاعتبار أهداف عملها أو مهمتها، وقيم الخصوصية، ودرجة تحمل المخاطر، ودورها في منظومة معالجة البيانات أو قطاع الصناعة، والمتطلبات القانونية/التنظيمية وأفضل الممارسات في القطاع، وأولويات إدارة المخاطر والموارد، واحتياجات الخصوصية للأفراد المستفيدين من أنظمتها أو منتجاتها أو خدماتها، والمتأثرين بها بشكل مباشر أو غير مباشر.

ولا يوجد ترتيب محدد لإعداد ملفات التعريف، كما يُظهر الشكل 6، فقد تضع المؤسسة أولاً ملف تعريف مستهدف يُدرج نتائج الخصوصية التي تريد تحقيقها، ثم تُعد ملف الوضع الراهن والذي يُدرج الثغرات؛ أو قد تبدأ المؤسسة بتحديد أنشطتها الحالية، ثم تدرس في ملف التعريف المستهدف كيفية تعديلها. وقد تختار المؤسسة إعداد ملفات تعريف متعددة بحسب الأدوار أو الأنظمة أو المنتجات أو الخدمات المختلفة التي تقدمها أو بحسب فئات الأفراد

الذين تقدم خدماتها لهم (مثلاً الموظفين في مقابل العملاء) لتتمكن من ترتيب الأنشطة والنتائج بشكل أفضل، وأيضاً لمعرفة مدى ارتباط كل نشاط/نتيجة بدرجة مختلفة من مخاطر الخصوصية. وقد تنسّق المؤسسات في قطاع صناعي معين، أو لديها أدوار متماثلة في منظومة معالجة البيانات، مع بعضها لإعداد ملفات تعريف مشتركة.

2.3 مستويات التنفيذ

تدعم مستويات التنفيذ عملية اتخاذ القرارات المتصلة بإدارة مخاطر الخصوصية في المؤسسة من خلال مراعاة طبيعة مخاطر الخصوصية التي تولدها أنظمة أو منتجات أو خدمات المؤسسة، ومدى كفاية وملاءمة العمليات والموارد التي تمتلكها المؤسسة لإدارة مثل هذه المخاطر. وينبغي أن تضع المؤسسة في اعتبارها، عند اختيار مستويات التنفيذ، ملف (ملفات) التعريف المستهدفة، وكيف يمكن دعم إنجاز هذه المستويات (أو عرقلتها) نتيجة ممارسات إدارة المخاطر الحالية، ومستوى إدراج مخاطر الخصوصية في محفظة إدارة المخاطر المؤسسية الحالية، والعلاقات في منظومة معالجة بيانات المؤسسة، وتشكيل القوى العاملة وبرنامج التدريب.

وثمة أربعة مستويات متمايزة للتنفيذ (يفصّلها الملحق (هـ)) هي: الجزئي (المستوى الأول)، والمُدرك للمخاطر (المستوى الثاني)، والقابل للتكرار (المستوى الثالث)، والتكيُّفي (المستوى الرابع)، ويعتبر كل مستوى بمثابة خطوة متقدمة عن المستوى السابق له، إلا أن الانتقال من مستوى إلى آخر ليس إلزامياً. ورغم الاستفادة المحتملة للمؤسسة من انتقالها من المستوى الأول إلى الثاني، لا تعتبر جميع المؤسسات بحاجة إلى الوصول إلى المستويين الثالث أو الرابع (أو قد تركز المؤسسة على أجزاء معينة منهما فقط). ويعتبر التقدم إلى المستويات الأعلى مناسباً عندما تكون عمليات أو موارد المؤسسة في مستواها الحالي غير كافية لمساعدتها على إدارة مخاطر الخصوصية.

ويُمكن للمؤسسة استخدام مستويات التنفيذ تلك للتواصل على المستوى الداخلي (حيال تخصيص الموارد اللازمة للتقدم إلى مستوى أعلى)، أو يمكنها استخدامها كمعايير عامة لقياس مدى تقدمها فيما يتعلق بقدرتها على إدارة مخاطر الخصوصية. ويمكن للمؤسسة كذلك استخدام هذه المستويات لفهم حجم الموارد والعمليات الخاصة بالمؤسسات الأخرى في منظومة معالجة البيانات وكيفية توافقها مع أولويات إدارة مخاطر الخصوصية للمؤسسة. لكن سيعتمد التنفيذ الناجح لإطار عمل الخصوصية على تحقيق النتائج الموضحة في ملف التعريف المستهدف الخاص بالمؤسسة، وليس على مستوى التنفيذ.

3.0 كيفية استخدام إطار عمل الخصوصية

من شأن توظيف إطار عمل الخصوصية كأداة لإدارة المخاطر مساعدة المؤسسة في جهودها لتحسين الاستخدامات المفيدة للبيانات، وإعداد أنظمة ومنتجات وخدمات مبتكرة، مع تقليل العواقب السلبية على الأفراد. كما يمكن أن يساعد الإطار المؤسسة أيضاً في الإجابة عن السؤال الأساسي التالي: "كيف نفكر في الآثار المترتبة على الأفراد أثناء إنشائنا لأنظمتنا ومنتجاتنا وخدماتنا؟" ويتسم استخدام إطار الخصوصية بالمرونة، لتلبية الاحتياجات الفريدة للمؤسسة، رغم أنه مصمم لاستكمال عمليات إنشاء الأعمال والأنظمة الحالية، بمعنى أن المؤسسة التي تنفذ هذا الإطار هي وحدها التي تقرر كيفية استخدامه.

فعلى سبيل المثال، قد يكون لدى المؤسسة بالفعل عمليات ممتازة لإدارة مخاطر الخصوصية، ولكنها قد تستخدم الوظائف الخمس للنواة بشكل مبسّط لتحليل أي ثغرات قد تكون لديها؛ كما قد يكون في إمكان المؤسسة التي تسعى إلى إنشاء برنامج الخصوصية استخدام الفئات والفئات الفرعية للنواة كمرجع. وقد تقارن مؤسسات أخرى ملفات التعريف أو مستويات التنفيذ لمحاذاة الأولويات الخاصة بإدارة مخاطر الخصوصية عبر الأدوار المختلفة في منظومة معالجة البيانات. وينبغي أن يؤدي تنوع الطرق التي يمكن من خلالها استخدام المؤسسات للإطار إلى تثبيط فكرة "الامتثال لإطار عمل الخصوصية" كمفهوم موحد أو كإطار يمكن الرجوع إليه من أي جهة خارج المؤسسة. وتقدم الأقسام الفرعية التالية بعض الخيارات لاستخدام إطار عمل الخصوصية.

3.1 وضع خرائط بالمراجع الزاخرة بالمعلومات

إن المراجع الزاخرة بالمعلومات هي خرائط محددة للفئات الفرعية تهدف إلى تقديم الدعم للتنفيذ، وتشمل وضع خرائط للأدوات والإرشادات الفنية والمعايير والقوانين واللوائح وأفضل الممارسات. ويمكن أن تساعد المسارات التي تحدد أحكام المعايير والقوانين واللوائح الخاصة بالفئات الفرعية المؤسسة في تحديد الأنشطة أو النتائج التي ينبغي إجراؤها أولاً لتسهيل الامتثال. ويعتبر إطار عمل الخصوصية محايداً من الناحية التكنولوجية، لكنه يدعم الابتكار التكنولوجي، حيث في إمكان أي مؤسسة أو قطاع صناعي إعداد عملية وضع الخرائط هذه مع تطور التكنولوجيا واحتياجات أعمالها. ويمكن للأدوات والأساليب المتاحة لتحقيق نتائج إيجابية للخصوصية بالاعتماد على المعايير والإرشادات والممارسات القائمة على الإجماع، أن تتوسع لتمتد عبر الحدود وتستوعب الطبيعة العالمية لمخاطر الخصوصية. وسيؤدي استخدام المعايير الحالية والناشئة إلى تمكين وفورات الحجم والمساهمة في إعداد أنظمة ومنتجات وخدمات تلبي احتياجات المؤسسة وتراعي أيضاً احتياجات الخصوصية للأفراد.

ويمكن أيضاً الاستفادة من الثغرات في وضع الخرائط لتحديد المواضع التي قد تساعد فيها المعايير والمبادئ التوجيهية والممارسات الإضافية أو المنقحة المؤسسة على تلبية الاحتياجات الناشئة. وعندها، قد تكتشف المؤسسة التي تنفذ فئة فرعية معينة، أو تضع فئة فرعية جديدة، أنه لا توجد إرشادات كافية لنشاط أو نتيجة ذات صلة. ولتلبية هذه الحاجة، قد تتعاون المؤسسة مع مدراء التكنولوجيا و/أو هيئات المعايير في صياغة وتطوير وتنسيق المعايير أو الإرشادات أو الممارسات.

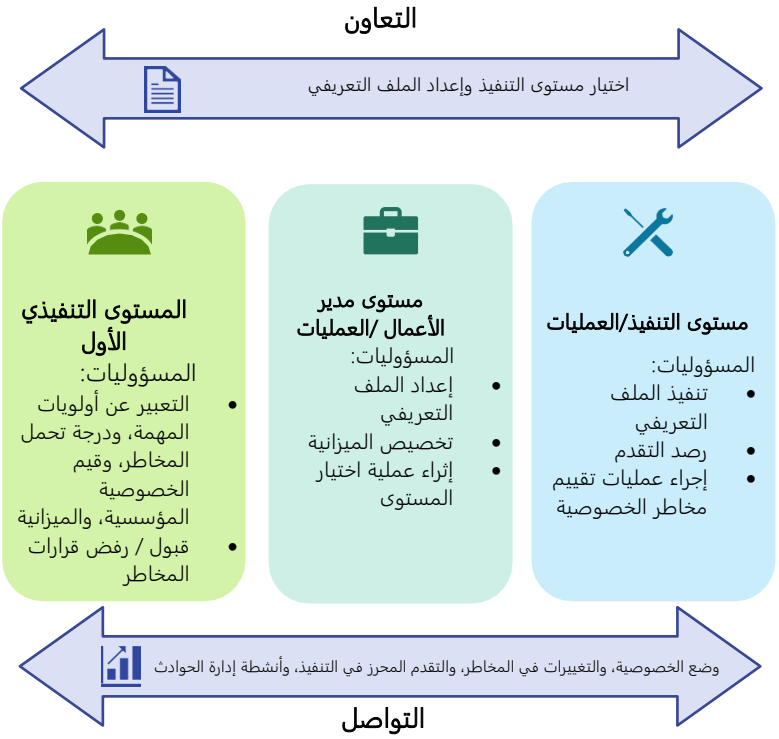
يمكن الاطلاع على مستودع بالمراجع الزاخرة بالمعلومات على الرابط التالي https://www.nist.gov/privacy-framework، حيث يُمكن لهذه الموارد أن تدعم استخدام المؤسسات لإطار عمل الخصوصية وتحقيق ممارسات أفضل للخصوصية.

3.2 تعزيز المساءلة

تعتبر المساءلة عموماً من المبادئ الأساسية للخصوصية، رغم أنها – نظرياً – لا تقتصر على الخصوصية.[13] وتتم المساءلة في جميع أنحاء المؤسسة، ويمكن التعبير عنها بدرجات متفاوتة من الأفكار والمفاهيم، كقيمة ثقافية، مثل سياسات وإجراءات الحوكمة، أو كعلاقات تتبع بين *متطلبات الخصوصية* و*ضوابطها*. ويُمكن أن تكون إدارة مخاطر الخصوصية وسيلة لدعم المساءلة على جميع المستويات التنظيمية لأنها تربط كبار المديرين التنفيذيين، الذين يمكنهم الإبلاغ بقيم الخصوصية للمؤسسة ودرجة تحمل المخاطر، بمدراء الأعمال/العمليات، الذين يمكنهم التعاون في تطوير وتنفيذ سياسات وإجراءات الحوكمة التي تدعم قيم الخصوصية المؤسسية.

---

[13] انظر، على سبيل المثال، منظمة التعاون والتنمية في الميدان الاقتصادي (2013) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, [إرشادات منظمة التعاون والتنمية في الميدان الاقتصادي بشأن حماية الخصوصية وتدفقات البيانات الشخصية العابرة للحدود. متاحة على الرابط: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm؛ المنظمة الدولية للتوحيد القياسي / اللجنة الكهروتقنية الدولية – *ISO/IEC 29100:2011 (2011) (IEC) [ISO / IEC 29100: 2011] Information technology – Security techniques – Privacy framework* - تكنولوجيا المعلومات - تقنيات الأمان - إطار عمل الخصوصية (المنظمة الدولية للتوحيد القياسي، جنيف، سويسرا)]. مُتاح على الرابط: https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip. تحالف مُصنعيّ السيارات، رابطة شركات صناعة السيارات العالمية، (2014)، مبادئ حماية خصوصية المستهلك: مبادئ حماية خصوصية المستهلك: *Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services* [مبادئ الخصوصية لتقنيات وخدمات المركبات]. متاح على الرابط: https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf.



شكل 7: التعاون النظري والتواصل داخل المؤسسة

يُمكن بعد ذلك إبلاغ المسؤولين في مستوى التنفيذ/العمليات بهذه السياسات والإجراءات، والذين سيتعاونون في تحديد متطلبات الخصوصية التي تدعم التعبير عن السياسات والإجراءات في أنظمة ومنتجات وخدمات المؤسسة.

يقوم الموظفون على مستوى التنفيذ/العمليات أيضاً باختيار وتنفيذ وتقييم الضوابط باعتبارها الإجراءات الفنية والسياسية التي تفي بمتطلبات الخصوصية، والإبلاغ عن التقدم المحرز والفجوات وأوجه القصور وإدارة الحوادث ومخاطر الخصوصية المتغيرة بحيث يتمكن مدراء الأعمال /العمليات وكبار المديرين التنفيذيين من استيعاب الوضع والاستجابة له بالشكل المناسب.

يعرض الشكل 7 تمثيلاً رسومياً لهذا التعاون والتواصل ثنائي الاتجاه وكيفية دمج عناصر إطار عمل الخصوصية لتسهيل العملية. بهذه الطريقة، يمكن للمؤسسات استخدام إطار عمل الخصوصية كأداة لدعم المساءلة، كما يمكنها استخدامه إلى جانب أطر العمل والتوجيهات الأخرى التي توفر ممارسات إضافية لتحقيق المساءلة داخل المؤسسات وفيما بينها.[14]

3.3. إنشاء برنامج الخصوصية أو تحسينه

يمكن أن يدعم إطار عمل الخصوصية إنشاء برنامج جديد للخصوصية أو تحسين برنامج قائم بالفعل باستخدام نموذج بسيط لمراحل "استعد، تجهز، انطلق"، حيث يمكن للمؤسسة أثناء مرورها بهذه المراحل استخدام المراجع الزاخرة بالمعلومات للحصول على إرشادات حيال تحديد الأولويات أو تحقيق النتائج (انظر القسم 3.1 لمعلومات أكثر حول المراجع الزاخرة بالمعلومات). كما يمكن الاطلاع على مستودع مليء بالمراجع الزاخرة بالمعلومات على الرابط التالي https://www.nist.gov/privacy-framework.

[14] انظر على سبيل المثال، المنشور الخاص للمعهد الوطني للمعايير والتكنولوجيا رقم 37- 800، المراجعة 2، *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [إطار عمل إدارة مخاطر أنظمة المعلومات والمؤسسات: نهج دورة حياة النظام للأمن والخصوصية] [7]؛ ومنظمة تطوير معايير المعلومات المهيكلة (2016)، *Privacy Management Reference Model and Methodology (PMRM)* [النموذج المرجعي لإدارة الخصوصية ومنهجيتها]، الإصدار 1.0، https://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf.

استعد

تتطلب الإدارة الفعالة لمخاطر الخصوصية استيعاب المؤسسة لمهمتها أو بيئة أعمالها، أو بيئتها القانونية، ودرجة تحملها للمخاطر، ومخاطر الخصوصية الناجمة عن أنظمة المؤسسة أو منتجاتها أو خدماتها، ودورها في منظومة معالجة البيانات. ويمكن للمؤسسة استخدام وظيفتي تحديد مخاطر الخصوصية وضبطها "للاستعداد" من خلال مراجعة الفئات والفئات الفرعية، والبدء في إعداد ملف التعريف الحالي وملف التعريف المستهدف.[15] توفر بعض الأنشطة والنتائج أساساً لإكمال ملفات التعريف في مرحلة "تجهز"، مثل إنشاء قيم وسياسات الخصوصية المؤسسية، وتحديد تحمل المخاطر المؤسسية والتعبير عنها، وإجراء تقييمات مخاطر الخصوصية (انظر الملحق (د) للحصول على مزيد من المعلومات حول تقييمات مخاطر الخصوصية).

طريقة مبسطة لإنشاء أو تحسين برنامج الخصوصية

استعد: استخدام وظيفتي تحديد مخاطر الخصوصية وضبطها "للاستعداد"

تجهز: وضع خطة عمل تستند إلى الاختلافات بين ملف التعريف الحالي وملف التعريف المستهدف.

انطلق: المضي قُدماً والبدء بتنفيذ خطة العمل.

تجهز

تستكمل المؤسسة ملفها التعريفي الحالي بالرجوع إلى نتائج الفئات والفئات الفرعية من الوظائف المتبقية التي يتم تحقيقها. وإذا تم تحقيق نتيجة جزئية، ستساعد هذه الحقيقة في دعم الخطوات اللاحقة عبر توفيرها معلومات أساسية. وتسترشد المؤسسة بالأنشطة المدرجة في وظيفتي "تحديد مخاطر الخصوصية وضبطها" - مثل قيم وسياسات الخصوصية المؤسسية، ودرجة تحمل المخاطر المؤسسية، ونتائج تقييم مخاطر الخصوصية – لاستكمال ملف التعريف المستهدف الذي يركز على تقييم الفئات والفئات الفرعية التي تصف نتائج الخصوصية المرغوبة. ويمكن كذلك أن تقوم المؤسسة بتطوير وظائفها وفئاتها وفئاتها الفرعية الإضافية لحساب المخاطر المؤسسية الفريدة، وقد تأخذ في الاعتبار تأثيرات ومتطلبات أصحاب المصلحة الخارجيين (مثل العملاء والشركاء) عند إنشاء ملف التعريف المستهدف. ويمكن لها إعداد ملفات تعريف متعددة لدعم خطوط أعمالها أو عملياتها المختلفة، والتي قد تختلف فيما بينها من حيث احتياجات العمل ودرجة تحمل المخاطر ذات الصلة.

وتقارن المؤسسة ملف التعريف الحالي بملف التعريف المستهدف لتحديد الفجوات، ثم تضع خطة عمل بأولويات لمعالجة هذه الفجوات (تعكس دوافع المهمة وتكاليفها وفوائدها ومخاطرها) لتحقيق النتائج ضمن ملف التعريف المستهدف. ةقد تقوم المؤسسة التي تستخدم إطار عمل الأمن السيبراني وإطار عمل الخصوصية معاً بوضع خطط عمل متكاملة، ثم تحدد الموارد، بما في ذلك احتياجات التمويل والقوى العاملة، اللازمة لمعالجة الفجوات، والتي يمكن أن تساعد في اختيار مستوى التنفيذ المناسب. ويشجع استخدام ملفات التعريف بهذه الطريقة المؤسسة على اتخاذ قرارات مستنيرة بشأن أنشطة الخصوصية، ويدعم إدارة المخاطر، ويمكّن المؤسسة من إجراء تحسينات مستهدفة وفعالة من حيث التكلفة.

انطلق

بعد "تجهيز" خطة العمل، تعطي المؤسسة الأولوية للإجراءات التي ينبغي اتخاذها لمعالجة أي فجوات، ثُم تعدل ممارسات الخصوصية الحالية بهدف تحقيق ملف التعريف المستهدف.[16]

---

[15] للحصول على معلومات إضافية، انظر خطوة "الإعداد"، القسم 3.1، المنشور الخاص للمعهد الوطني للمعايير والتكنولوجيا، المراجعة 2، رقم 37- 800 [7]

[16] يتضمن المنشور الخاص للمعهد الوطني للمعايير والتكنولوجيا 800 -37، المراجعة [7] 2، معلومات حول خطوات تنفيذ خطة العمل، شاملة خطوة التحكم في الاختيار والتنفيذ والتقييم وحتى خطوة القضاء على أي فجوات.

لا يُشترط تنفيذ هذه المراحل بنفس التسلسل، بل يمكن تنفيذها حسب الحاجة للتقييم المستمر وتحسين وضع الخصوصية لدى المؤسسة، إذ قد تجد المؤسسة مثلاً أن تكرار مرحلة الاستعداد يحسّن من جودة تقييمات مخاطر الخصوصية. علاوةً على ذلك، قد تراقب المؤسسة التقدم المحرز عبر التحديثات المتكررة لملف التعريف الحالي أو ملف التعريف المستهدف للتكيف مع المخاطر المتغيرة، وبالتالي مقارنة الملف الحالي بالملف المستهدف.

3.4 تطبيق المراحل على دورة حياة تطوير النظام

يمكن مواءمة ملف التعريف المستهدف مع مراحل دورة حياة تطوير النظام (أي التخطيط ثم التصميم ثم البناء/الشراء ثم النشر ثم التشغيل ثم إيقاف التشغيل)، لدعم تحقيق نتائج الخصوصية ذات الأولوية.[17] ويمكن تحويل نتائج الخصوصية ذات الأولوية إلى إمكانيات ومتطلبات الخصوصية الخاصة بالنظام، بدءاً من مرحلة وضع الخطة، مع إدراك أنه من المحتمل أن تتطور المتطلبات خلال الفترة المتبقية من دورة حياة النظام. ومن أهم محطات مرحلة التصميم التحقق من أن إمكانيات ومتطلبات الخصوصية تتطابق مع احتياجات المؤسسة وقدرتها على تحمل المخاطر (كما هو موضح في ملف التعريف المستهدف). كما يمكن استخدام ملف التعريف المستهدف ذاته كقائمة داخلية يتم تقييمها عند نشر النظام للتحقق من تنفيذ جميع إمكانيات ومتطلبات الخصوصية، حيث ينبغي أن تكون نتائج الخصوصية المحددة باستخدام الإطار بمثابة أساس للتشغيل المستمر للنظام. ويتضمن ذلك إعادة التقييم العرضية، وإدراج النتائج في ملف التعريف الحالي، للتحقق من استيفاء إمكانيات ومتطلبات الخصوصية.

تركز تقييمات مخاطر الخصوصية عادةً على دورة حياة البيانات، والمراحل التي تمر البيانات عبرها، وهي غالباً إنشاء البيانات أو جمعها ومعالجتها ونشرها واستخدامها وتخزينها والتخلص منها، إما بتدميرها أو حذفها. وتساعد المواءمة بين دورة حياة تطوير النظام ودورة حياة البيانات على إدارة مخاطر الخصوصية بشكل أفضل من خلال تحديد وفهم كيفية معالجة البيانات خلال جميع مراحل دورة حياة تطوير النظام المؤسسات، وتوجيهها عند اختيار وتنفيذ عناصر التحكم في الخصوصية لاستيفاء المتطلبات ذات الصلة.

[17] في إطار دورة حياة تطوير النظام، يمكن للمؤسسة استخدام مجموعة متنوعة من منهجيات التطوير (مثل نموذج الشلال أو الدوامة أو النموذج المرن).

3.5 الاستخدام في منظومة معالجة البيانات

شكل 8: العلاقات في منظومة معالجة البيانات

يعتبر الدور الذي تقوم به المؤسسة في منظومة معالجة البيانات العامل الرئيسي في إدارة مخاطر الخصوصية، حيث يمكن أن يؤثر على التزاماتها القانونية، وأيضاً على الإجراءات التي قد تتخذها لإدارة مخاطر الخصوصية. وتشمل منظومة معالجة البيانات، والموضحة الشكل 8، مجموعة من الكيانات والأدوار التي قد تربط بينها وبين الأفراد علاقات معقدة ومتعددة الاتجاهات يمكن أن تزداد تعقيداً عندما تكون الكيانات مدعومة بسلسلة من الكيانات الفرعية. فعلى سبيل المثال، قد يدعم مقدم خدمة سلسلة من مقدمي الخدمة، أو قد يكون لدى شركة مصنعة عدة موردين للمستلزمات. ويوضح الشكل 8 أن للكيانات أدوار مميزة، وقد يكون لبعضها أدوار متعددة، مثل المؤسسة التي تقدم خدمات لمؤسسة أخرى، والتي تقدم بدورها منتجات للمستهلكين. وتعتبر الأدوار المبينة في الشكل رقم 8 مجرد تصنيفات افتراضية، ومن الناحية العملية، قد يتم تقنين دور (أدوار) الكيان قانوناً، فعلى سبيل المثال، تصنف بعض القوانين المؤسسات على أنها وحدات لجمع البيانات أو معالجتها - أو قد يتم اشتقاق التصنيفات من التسميات المتداولة في قطاع الصناعة.

ويمكن لمؤسسة ما، عبر إعداد ملف تعريف واحد – أو أكثر – حيال دورها/أدوارها، استخدام إطار عمل الخصوصية لتحديد كيفية إدارة مخاطر الخصوصية، طبقاً لأولوياتها، وأيضاً لمعرفة كيف يمكن أن تؤثر تدابير إدارة مخاطر الخصوصية التي تتخذها على منظومة معالجة البيانات الأخرى لها. على سبيل المثال:

- يُمكن لمؤسسة تتخذ قرارات حول كيفية جمع واستخدام بيانات الأفراد استخدام ملف التعريف لإخطار مقدم خدمة خارجي بمتطلبات الخصوصية الخاصة بها (والذي قد يكون مثلاً مقدم خدمة سحابية يتم تصدير البيانات إليه)، وقد يستخدم مقدم الخدمة الخارجي الذي يعالج البيانات ملف التعريف الخاص به لإثبات توافق تدابير معالجة البيانات التي اعتمدها مع الالتزامات التعاقدية.
- يمكن للمؤسسة استخدام ملف التعريف الحالي لها لتعبّر من خلاله عن كيفية تعاطيها مع موضوع الخصوصية لعرض النتائج أو مقارنتها بالمتطلبات الملقاة على عاتقها.
- قد يقوم قطاع صناعي بإنشاء ملف تعريف مشترك يمكن لأعضائه استخدامه لتخصيص ملفات التعريف الخاصة بهم.
- قد تستخدم شركة مصنّعة ملف التعريف المستهدف لتحديد القدرات اللازمة لإدراج منتجاتها حتى يتمكن عملاؤها التجاريون من تلبية احتياجات الخصوصية لمستخدميهم النهائيين.
- قد يستخدم مطور ملف التعريف المستهدف للنظر في كيفية تصميم تطبيق يتيح حماية الخصوصية عند استخدامه في بيئات أنظمة المؤسسات الأخرى.

يوفر إطار عمل الخصوصية لغة مشتركة للتواصل بشأن متطلبات الخصوصية مع الكيانات داخل منظومة معالجة البيانات، والذي يعتبر ضرورياً بشكلٍ خاص عندما تعبر منظومة معالجة البيانات الحدود الوطنية، كما هو الحال في عمليات نقل البيانات الدولية. قد تشمل الممارسات التنظيمية التي تدعم التواصل ما يلي:

- تحديد متطلبات الخصوصية.
- النص على متطلبات الخصوصية في اتفاقيات رسمية (كالعقود وأطر العمل متعددة الأطراف).
- الإبلاغ عن كيفية التحقق من صحة متطلبات الخصوصية.
- التحقق من استيفاء متطلبات الخصوصية باستخدام مجموعة متنوعة من منهجيات التقييم.
- حوكمة وإدارة الأنشطة السابقة.

3.6 توجيه قرارات الشراء

يمكن أيضاً استخدام نفس ملفات التعريف لاتخاذ قرارات مستنيرة حول شراء المنتجات والخدمات، على اعتبار أنه يمكن استخدام ملف التعريف الحالي أو المستهدف لإنشاء قائمة بمتطلبات الخصوصية يمكن فيها للمؤسسة تقييم أنظمة الشركاء أو منتجاتها أو خدماتها بحسب نتيجة هذه القائمة من خلال تحديد النتائج ذات الصلة بأهداف الخصوصية. فعلى سبيل المثال، إذا تم شراء جهاز لمراقبة بيئة غابة، قد تكون *قابلية الإدارة* مهمة لدعم القدرات لتقليل عمليات معالجة بيانات الأشخاص الذين يستخدمون الغابة، ولا بد كذلك من تقييم الشركة المصنعة على أساس الفئات الفرعية المبينة في الهيكل (على سبيل المثال، CT.DP-P4: تسمح تهيئة النظام أو الجهاز بالتجميع الانتقائي لعناصر البيانات أو الكشف عنها).

في الظروف التي قد لا يكون فيها من الممكن فرض متطلبات الخصوصية على المورد، ينبغي أن يكون الهدف اتخاذ قرار الشراء الأمثل من بين عدة موردين، مع أخذ قائمة محددة بمتطلبات الخصوصية في الاعتبار. في كثير من الأحيان، يعني إجراء مفاضلة بين مورد وآخر، أو مقارنة بين المنتجات أو الخدمات وبين الفجوات المعروفة في ملف التعريف. وإذا كان النظام أو المنتج أو الخدمة المشتراة لا تفي بجميع الأهداف الموضحة في ملف التعريف، يمكن للمؤسسة معالجة المخاطر المتبقية باتخاذ تدابير التخفيف أو إجراءات إدارية أخرى.

المراجع

[1] المعهد الوطني للمعايير والتكنولوجيا (2018) تحسين إطار عمل الأمن السيبراني للبنية التحتية الحرجة، الإصدار 1.1. (المعهد الوطني للمعايير والتكنولوجيا، جايثرسبيرغ، ماريلاند).
https://doi.org/10.6028/NIST.CSWP.04162018

[2] المعهد الوطني للمعايير والتكنولوجيا (2019). تحليل موجز للاستجابات لطلب معلومات عن إطار عمل الخصوصية الخاص بالمعهد. (المعهد الوطني للمعايير والتكنولوجيا، جايثرسبيرغ، ماريلاند).
https://www.nist.gov/sites/default/files/documents/2019/02/27/rfi_response_analysis_privacyframework_2.27.19.pdf

[3] المعهد الوطني للمعايير والتكنولوجيا (2019) منهجية المعهد الخاصة بتقييم مخاطر الخصوصية (المعهد الوطني للمعايير والتكنولوجيا، جايثرسبيرغ، ماريلاند).
https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

[4] لوحة التشغيل التفاعلي للشبكة الذكية - لجنة الأمن السيبراني للشبكة الذكية (2014) إرشادات للأمن السيبراني للشبكة الذكية: المجلد 1 - استراتيجية الأمن السيبراني للشبكة الذكية، وبنيتها الهندسية، والمتطلبات عالية المستوى. (المعهد الوطني للمعايير والتكنولوجيا، جايثرسبيرغ، ماريلاند). تقرير مشترك بين الوكالات أو التقرير الداخلي للمعهد الوطني للمعايير والتكنولوجيا رقم 7628 المراجعة 1، المجلد 1.
https://doi.org/10.6028/NIST.IR.7628r1

[5] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017). مقدمة إلى هندسة الخصوصية وإدارة المخاطر في الأنظمة الفيدرالية. المعهد الوطني للمعايير والتكنولوجيا، جايثرسبيرغ، ماريلاند). تقرير مشترك بين الوكالات أو التقرير الداخلي للمعهد الوطني للمعايير والتكنولوجيا رقم 8062.
https://doi.org/10.6028/NIST.IR.8062

[6] مبادرة التحول الخاصة بفريق العمل المشترك (2011) إدارة مخاطر أمن المعلومات: المؤسسة والمهمة وعرض نظام المعلومات. (المعهد الوطني للمعايير والتكنولوجيا، جايثرسبيرغ، ماريلاند). المنشور الخاص للمعهد الوطني للمعايير والتكنولوجيا 800 -39.
https://doi.org/10.6028/NIST.SP.800-39

[7] فريق العمل المشترك (2018) إطار عمل إدارة المخاطر المتعلقة بأنظمة المعلومات والمؤسسات: نهج دورة حياة النظام للأمن والخصوصية. (المعهد الوطني للمعايير والتكنولوجيا، جايثرسبيرغ، ماريلاند)، المنشور الخاص للمعهد الوطني للمعايير والتكنولوجيا، المراجعة 2، 800-37.
https://doi.org/10.6028/NIST.SP.800-37r2

[8] Grassi PA, Garcia ME, Fenton JL (2017) إرشادات الهوية الرقمية (المعهد الوطني للمعايير والتكنولوجيا، جايثرسبيرغ، ماريلاند). المنشور الخاص للمعهد الوطني للمعايير والتكنولوجيا 3-63-800، تشمل تحديثات اعتباراً من 1 ديسمبر 2017.
https://doi.org/10.6028/NIST.SP.800-63-3

[9] مكتب الإدارة والميزانية (2017) الاستعداد لخرق معلومات التعريف الشخصية والتصدي له. (البيت الأبيض، واشنطن العاصمة)، OMB Memorandum M-17-12، 3 يناير 2017. متاح على الرابط https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf

[10] مبادرة التحول الخاصة بفريق العمل المشترك (2013). ضوابط الأمن والخصوصية لأنظمة المعلومات في المؤسسات الفيدرالية (المعهد الوطني للمعايير والتكنولوجيا، جايثرسبيرغ، ماريلاند). المنشور الخاص للمعهد الوطني للمعايير والتكنولوجيا 800 -53. المراجعة 4، تشمل تحديثات اعتباراً من 22 يناير 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[11] Grassi PA, Lefkovitz NB, Nadeau EM, Galluzzo RJ, Dinh AT (2018). سمات البيانات الوصفية: مخطط مقترح لتقييم السمات الاتحادية. (المعهد الوطني للمعايير والتكنولوجيا، جايثرسبيرغ، ماريلاند). تقرير مشترك بين الوكالات أو التقرير الداخلي للمعهد الوطني للمعايير والتكنولوجيا رقم 8112. https://doi.org/10.6028/NIST.IR.8112

[12] مبادرة التحول الخاصة بفريق العمل المشترك (2012) دليل لإجراء عمليات تقييم المخاطر: المؤسسة والمهمة وعرض نظام المعلومات. (المعهد الوطني للمعايير والتكنولوجيا، جايثرسبيرغ، ماريلاند). المنشور الخاص للمعهد الوطني للمعايير والتكنولوجيا 800 -30، المراجعة 1. https://doi.org/10.6028/NIST.SP.800-30r1

[13] "التعريفات" الباب 44 من القانون الأمريكي رقم 3542. 2011 https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542

الملحق (أ): نواة إطار عمل الخصوصية

يعرض هذا الملحق نواة إطار عمل الخصوصية والذي يتألف من جدول الوظائف والفئات والفئات الفرعية والتي تصف أنشطة ونتائج محددة يمكنها دعم إدارة مخاطر الخصوصية عند معالجة البيانات ضمن الأنظمة والمنتجات والخدمات.

ملاحظة للمستخدمين

النهج القائم على المخاطر:

- **لا تعتبر النواة قائمة مرجعية بالإجراءات الواجب تنفيذها، حيث يمكن للمؤسسة اختيار الفئات الفرعية المتسقة مع إستراتيجية المخاطر الخاصة بها لحماية خصوصية الأفراد.** يمكن ألا تحتاج المؤسسة إلى تحقيق كل نتيجة أو نشاط موجود في النواة، حيث يُتوقع أن تستخدم المؤسسة ملفات التعريف لتحديد وانتقاء الوظائف والفئات والفئات الفرعية التي تلبي احتياجاتها على أفضل وجه (من خلال التركيز على أهدافها وأدوارها في منظومة معالجة البيانات أو القطاع الذي تنشط فيه)، وتراعي أيضاً المتطلبات القانونية/التنظيمية وأفضل الممارسات في القطاع، وكذلك أولويات إدارة المخاطر، واحتياجات الخصوصية للأفراد المستفيدين من أنظمة أو منتجات أو خدمات المؤسسة أو المتأثرين بها بشكل مباشر أو غير مباشر.
- ليس من الضروري تحقيق النتيجة بالكامل، إذ يمكن للمؤسسة استخدام ملفات التعريف الخاصة بها للتعبير عن تحقيق نتيجة ما بشكل جزئي فقط في حال لا يمكن لجميع جوانب النتيجة إدارة مخاطر الخصوصية، أو قد تستخدم المنظمة ملف التعريف المستهدف للتعبير عن جانب من نتيجة لا يمكنها تحقيقه حالياً لافتقارها للقدرة على ذلك.
- ربما يلزم النظر في عدة نتائج في نفس الوقت للنجاح في إدارة مخاطر الخصوصية بشكل مناسب. فعلى سبيل المثال، قد تختار مؤسسة تستجيب لطلبات الأفراد للوصول إلى البيانات لملفها التعريفي كلاً من الفئة الفرعية CT.DM-P1: "يمكن الوصول إلى عناصر البيانات للمراجعة" والفئة "إدارة الهوية والمصادقة والتحكم في الوصول" (PR.AC-P) لضمان الوصول إلى البيانات من قبل صاحبها فقط.

التنفيذ: لا يُقصد من تنسيق الجدول النواة بتلك الطريقة اقتراح أمر تنفيذ محدد أو الإشارة إلى وجود تراتبية معينة للوظائف، والفئات، والفئات الفرعية، إذ قد يكون التنفيذ غير تسلسلي أو متزامن أو تكراري، اعتماداً على مرحلة دورة حياة تطوير النظام، أو حالة برنامج الخصوصية، أو حجم القوة العاملة، أو دور (أدوار) المؤسسة في منظومة معالجة البيانات. كما يعتبر أيضاً النواة غير شامل، ويمكن تجديده، وبالتالي يسمح للمؤسسات والقطاعات والكيانات الأخرى بتطويعه أو إضافة وظائف، وفئات، وفئات فرعية إضافية إلى كل ملف تعريف.

الأدوار:

- **أدوار المنظومة**: صُممت النواة بحيث تتمكن جميع المؤسسات أو الكيانات من استخدامها بغض النظر عن دورها/أدوارها في منظومة معالجة البيانات، ويجب على المؤسسة مراجعة النواة انطلاقاً من موقعها في تلك المنظومة. وقد ينظّم قانون ما دور (أدوار) المؤسسة، إذ تصنف بعض القوانين المؤسسات مثلاً على أنها "وحدات لجمع البيانات أو معالجتها" أو تذكر مسميات أخرى مشتقة من القطاع الصناعي للمؤسسة. ويمكن للمؤسسة استخدام ملفات التعريف الخاصة بها لتحديد الوظائف، والفئات، والفئات الفرعية ذات الصلة بدورها (أدوارها) في حال لم يكن دور المنظومة يعيّن العناصر الأساسية.
- **الأدوار التنظيمية:** قد يتحمل بعض موظفي المؤسسة المسؤولية عن فئات أو فئات فرعية مختلفة، فقد تكون الإدارة القانونية مثلاً مسؤولة عن تنفيذ الأنشطة ضمن "سياسات الحوكمة وعملياتها وإجراءاتها"، في

حين يُناط بإدارة تكنولوجيا المعلومات مسؤولية "الجرد والتعيين". ومثالياً، تشجع النواة التعاون بين المؤسسات لوضع ملفات تعريف وتحقيق النتائج.

قابلية التوسع: ربما يكتنف الغموض صياغة بعض جوانب النتائج. على سبيل المثال، قد تتضمن النتائج مصطلحات مثل "أُبلغ بشأنه" أو "أُفصح عنه" دون توضيح هوية من قام بالإبلاغ أو الإفصاح. ويعود سبب هذا الغموض إلى إتاحة الفرصة للمؤسسات المختلفة (وحالات الاستخدام المختلفة) بتحديد ما هو مناسب أو مطلوب في سياق معين.

مستودع الموارد: يمكن إيجاد موارد توفر معلومات إضافية حول كيفية تحديد الأولويات أو تحقيق النتائج على الرابط التالي: https://www.nist.gov/privacy-framework.

مواءمة إطار عمل الأمن السيبراني:

- كما يذكر القسم 1-2، يمكن للمؤسسات استخدام وظائف إطار عمل الخصوصية الخمسة (التحديد-الخصوصية، والضبط-الخصوصية، والتحكم-الخصوصية، والتواصل-الخصوصية، والحماية-الخصوصية) لإدارة مخاطر الخصوصية الناشئة عن معالجة البيانات. وتركز وظيفة الحماية-الخصوصية بشكل خاص على إدارة المخاطر المرتبطة بأحداث الخصوصية المتعلقة بالأمن (مثل انتهاكات الخصوصية). وقد تختار المؤسسات استخدام وظائف الاكتشاف والاستجابة والتعافي من إطار عمل الأمن السيبراني لدعم إضافي لإدارة مخاطر الخصوصية المتعلقة بالأمن. لهذا السبب، يُدرج الجدول 1 هذه الخصائص، ولكنها غير مفعلة. وقد تستخدم المؤسسة، بدلاً من ذلك، جميع وظائف إطار عمل الأمن السيبراني الخمس جنباً إلى جنب مع وظائف التحديد-الخصوصية، والضبط-الخصوصية، والتحكم-الخصوصية، والتواصل-الخصوصية لمعالجة مخاطر الخصوصية والأمن معاً. انظر الشكل 5 للحصول على مثال توضيحي لكيفية استخدام وظائف كلا الإطارين في مجموعات مختلفة لإدارة الجوانب المختلفة لمخاطر الخصوصية والأمن السيبراني.
- قد تكون بعض الوظائف أو الفئات أو الفئات الفرعية متطابقة مع إطار عمل الأمن السيبراني أو تم تعديلها بناءً عليه. ويمكن استخدام وسيلة الإيضاح التالية لتوضيح هذه العلاقة في الجدول 2. يمكن التعرف على نقاط التلاقي بين الإطارين في مستودع الموارد على الرابط التالي: https://www.nist.gov/privacy-framework.
  - تتماشى الوظيفة أو الفئة أو الفئة الفرعية مع إطار عمل الأمن السيبراني، ولكن تم تعديل النص ليناسب إطار عمل الخصوصية
  - تتطابق الفئة أو الفئة الفرعية مع إطار عمل الأمن السيبراني.

معرفات النواة: يُخصص لكل مكون في النواة معرفاً فريداً لسهولة الاستخدام. ولكل وظيفة وفئة معرف أبجدي فريد، كما يوضح الجدول 1. تحتوي الفئات الفرعية داخل كل فئة على رقم مضاف إلى المعرف الأبجدي، ويتضمن الجدول 2 المعرف الفريد لكل فئة فرعية.

جدول 1: المعرفات الفريدة للوظيفة والفئة في إطار عمل الخصوصية

المعرف الفريد للوظيفة	الوظيفة	المعرف الفريد للفئة	الفئة
ID-P	التحديد-الخصوصية	ID.IM-P	الجرد والتعيين
		ID.BE-P	بيئة الأعمال
		ID.RA-P	تقييم المخاطر
		ID.DE-P	إدارة مخاطر منظومة معالجة البيانات
GV-P	الضبط–الخصوصية	GV.PO-P	سياسات الحوكمة وعملياتها وإجراءاتها
		GV.RM-P	استراتيجية إدارة المخاطر
		GV.AT-P	التوعية والتدريب
		GV.MT-P	المتابعة والمراجعة
CT-P	التحكم–الخصوصية	CT.PO-P	سياسات معالجة البيانات وعملياتها وإجراءاتها
		CT.DM-P	إدارة معالجة البيانات
		CT.DP-P	المعالجة غير المقترنة
CM-P	التواصل-الخصوصية	CM.PO-P	سياسات التواصل وعملياتها وإجراءاتها
		CM.AW-P	التوعية بمعالجة البيانات
PR-P	الحماية–الخصوصية	PR.PO-P	سياسات حماية البيانات وعملياتها وإجراءاتها
		PR.AC-P	إدارة وظيفة التحديد والمصادقة عليها، والتحكم في الوصول
		PR.DS-P	أمن البيانات
		PR.MA-P	الصيانة
		PR.PT-P	التكنولوجيا الوقائية
DE	الاكتشاف	DE.AE	الحالات غير الطبيعية والحوادث
		DE.CM	المراقبة الأمنية المستمرة
		DE. DP	عمليات الاكتشاف
RS	الاستجابة	RS.RP	تخطيط الاستجابة
		RS.CO	التواصل
		RS.AN	التحليل
		RS.MI	التخفيف من حدة المخاطر
		RS.IM	التحسينات
RC	التعافي	RC.RP	التخطيط للتعافي
		RC.IM	التحسينات
		RC.CO	التواصل

جدول 2: نواة إطار عمل الخصوصية

	الوظيفة	الفئة	الفئة الفرعية
	التحديد–الخصوصية: إعداد الفهم المؤسسي لإدارة مخاطر الخصوصية الناشئة عن معالجة بيانات الأفراد.	**الجرد والتعيين (ID.IM-P):** يتم توجيه إدارة مخاطر الخصوصية من خلال استيعاب وفهم البيانات التي يتم معالجتها ضمن الأنظمة أو المنتجات أو الخدمات.	**ID.IM-P1:** جرد الأنظمة/المنتجات/الخدمات التي تقوم بمعالجة البيانات
			ID.IM-P2: جرد المالكين أو المشغلين (مثلاً، المؤسسة، أطراف خارجية [مثل مقدمي الخدمات والشركاء والعملاء والمطورين]) وأدوارهم فيما يتعلق بالأنظمة/المنتجات/الخدمات والمكونات التي تعالج البيانات (مثلاً، على المستوى الداخلي أو الخارجي).
			ID.IM-P3: جرد فئات الأفراد الذين تتم معالجة بيانتهم (مثلاً، العملاء، الموظفين، الموظفين المحتملين، المستهلكين).
			ID.IM-P4: جرد إجراءات بيانات الأنظمة/المنتجات/الخدمات
			ID.IM-P5: جرد الغايات من إجراءات البيانات.
			ID.IM-P6: جرد عناصر البيانات في إطار إجراءات البيانات.
			ID.IM-P7: تحديد بيئة معالجة البيانات (مثل: الموقع الجغرافي، والأطراف الداخلية، والأطراف عبر السحابة، والأطراف الخارجية)
			ID.IM-P8: يتم تعيين عملية معالجة البيانات، مما يوضح إجراءات البيانات وعناصر البيانات المرتبطة بالأنظمة/المنتجات/الخدمات، بما في ذلك المكونات، وأدوار مالكيها أو مشغليها، وتفاعلات الأفراد أو الأطراف الخارجية مع الأنظمة/المنتجات/الخدمات.

	الوظيفة	الفئة	الفئة الفرعية
		بيئة الأعمال (ID.BE-P): فهم ما هي مهمة المؤسسة وأهدافها ومن هم أصحاب المصلحة فيها وما هي أنشطتها وأولوياتها. ستُستخدم هذه المعلومات لتمكين اتخاذ قرارات مستنيرة حول أدوار الخصوصية والمسؤوليات وإدارة المخاطر.	**ID.BE-P1:** تحديد دور المؤسسة في منظومة معالجة البيانات والإبلاغ عن هذا الدور.
			ID.BE-P2: تحديد أولويات المؤسسة (فيما يتعلق بمهمتها وأنشطتها وأهدافها) والإبلاغ عن هذا الدور.
			ID.BE-P3: تحديد الأنظمة/المنتجات/الخدمات التي تدعم أولويات المؤسس والإبلاغ عن المتطلبات الأساسية.
		تقييم المخاطر (ID.RA-P): تتفهم المؤسسة مخاطر الخصوصية التي يتعرض لها الأفراد وتفهم كيف يمكن لهذه المخاطر أن تخلق تأثيرات على عملياتها، بما في ذلك مهمتها ووظائفها وأولويات إدارة المخاطر الأخرى (مثلاً، الامتثال، الأولويات المالية)، وسمعتها وموظفيها وثقافتها.	**ID.RA-P1:** يتم تحديد العوامل السياقية المتعلقة بالأنظمة/المنتجات/الخدمات وإجراءات البيانات (مثلاً، التركيبة السكانية للأفراد، اهتماماتهم أو تصوراتهم للخصوصية، حساسية البيانات و/أو أنواعها، إمكانية الاطلاع على معالجة بيانات الأفراد والأطراف الثالثة).
			ID.RA-P2: تحديد المدخلات والمخرجات التحليلية للبيانات وتقييمها لاكتشاف أي تحيز.
			ID.RA-P3: تحديد أي إجراءات متصلة بالبيانات قد تكون متسببة بمشاكل محتملة أو مشكلات ذات صلة.
			ID.RA-P4: تُستخدم الإجراءات المتصلة بالبيانات والمتسببة في المشاكل، والاحتمالات، والتأثيرات لتحديد المخاطر وترتيبها بحسب الأولوية.
			ID.RA-P5: تحديد طرق الاستجابة للمخاطر وترتيب طرق الاستجابة بحسب الأولوية وتنفيذها.

	الوظيفة	الفئة	الفئة الفرعية
		إدارة مخاطر منظومة معالجة البيانات (ID.DE-P): يتم تحديد أولويات المؤسسة والقيود ودرجة تحمل المخاطر والافتراضات، والتي تُستخدم لاحقاً لدعم القرارات المتصلة بإدارة مخاطر الخصوصية والأطراف الثالثة داخل منظومة معالجة البيانات. أنشأت المؤسسة ونفذت عمليات لتحديد وتقييم وإدارة مخاطر الخصوصية داخل منظومة معالجة البيانات.	**ID.DE-P1:** تحديد سياسات وعمليات وإجراءات إدارة مخاطر منظومة معالجة البيانات وتقييمها وإدارتها والاتفاق عليها بين أصحاب المصلحة في المؤسسة.
			ID.DE-P2: تحديد الأطراف المشاركة في منظومة معالجة البيانات (مثال: مقدمي الخدمات والعملاء والشركاء ومُصنعي المنتجات ومطوري التطبيقات) وترتيبهم من حيث الأولوية وتقيمهم باستخدام عملية تقييم مخاطر الخصوصية.
			ID.DE-P3: تُستخدم العقود المبرمة مع أطراف منظومة معالجة البيانات في تنفيذ التدابير المناسبة المصممة لتلبية أهداف برنامج الخصوصية الخاص بالمؤسسة.
			ID.DE-P4: تُستخدم أطر التشغيل البيني أو نُهج متعددة الأطراف مماثلة لإدارة مخاطر خصوصية منظومة معالجة البيانات.
			ID.DE-P5: يتم تقييم أطراف منظومة معالجة البيانات بشكل دوري باستخدام عمليات التدقيق أو نتائج الاختبار أو غيرها من أشكال التقييم للتأكد من أنها تفي بإطار العمل التعاقدي أو إطار العمل المتبادل أو غيرها من الالتزامات.
	الضبط-الخصوصية (GV-P): إعداد وتنفيذ هيكل الحوكمة التنظيمية حتى يمكن دائماً فهم أولويات إدارة المخاطر في المؤسسة من	**سياسات الحوكمة وعملياتها وإجراءاتها (GV.PO-P):** فهم سياسات وعمليات وإجراءات إدارة ومتابعة المتطلبات التنظيمية والقانونية والبيئية والتشغيلية للمؤسسة، وكذا مخاطرها، والاستفادة مما سبق في توجيه إدارة مخاطر الخصوصية.	**GV.PO-P1:** يتم تحديد قيم وسياسات خصوصية المؤسسة (مثل، شروط معالجة البيانات كاستخدامات البيانات أو فترات الاحتفاظ بها، وامتيازات الأفراد فيما يتعلق بمعالجة البيانات) والإبلاغ عنها.
			GV.PO-P2: يتم وضع وتنفيذ عمليات تعمل على غرس قيم الخصوصية التنظيمية في إطار تطوير النظام/المنتج/الخدمة والعمليات.
			GV.PO-P3: يتم تحديد أدوار ومسؤوليات أفراد القوى العاملة فيما يتعلق بالخصوصية.

	الوظيفة	الفئة	الفئة الفرعية
	خلال مخاطر الخصوصية.		**GV.PO-P4:** يتم تنسيق أدوار ومسؤوليات الخصوصية ومواءمتها مع أصحاب المصلحة الخارجيين (مثل مقدمي الخدمات والعملاء والشركاء).
			GV.PO-P5: فهم وإدارة المتطلبات القانونية والتنظيمية والتعاقدية المتعلقة بالخصوصية.
			GV.PO-P6: تتعاطى سياسات وعمليات وإجراءات الحوكمة وإدارة المخاطر مع مخاطر الخصوصية.
		استراتيجية إدارة المخاطر (GV.RM-P): يتم تحديد أولويات المؤسسة والقيود التي تواجهها ودرجة تحمل المخاطر والافتراضات واستخدام ذلك لدعم القرارات المتصلة بالمخاطر التشغيلية.	**GV.RM-P1:** وضع عمليات إدارة المخاطر وإدارتها والاتفاق عليها بين أصحاب المصلحة في المؤسسة.
			GV.RM-P2: تحديد درجة تحمل المخاطر التنظيمية وتوصيلها بوضوح.
			GV.RM-P3: يتم إبلاغ تحديد درجة تحمل المخاطر بالمؤسسة من خلال دورها (أدوارها) في منظومة معالجة البيانات.
		التوعية والتدريب (GV.AT-P): يتم توعية القوى العاملة في المؤسسة والأطراف الثالثة المشاركة في معالجة البيانات بمفهوم الخصوصية وتدريبهم على أداء واجباتهم ومسؤولياتهم المتعلقة بالخصوصية بما يتوافق مع السياسات والعمليات والإجراءات والاتفاقيات وقيم الخصوصية المؤسسية ذات الصلة.	**GV.AT-P1:** توجيه أفراد القوى العاملة وتدريبهم على أدوارهم ومسؤوليتهم.
			GV.AT-P2: يفهم كبار المديرين التنفيذيين أدوارهم ومسؤولياتهم.
			GV.AT-P3: يفهم فريق عمل الخصوصية أدوارهم ومسؤولياتهم.
			GV.AT-P4: تفهم الأطراف الثالثة (أي مقدمي الخدمة والعملاء والشركاء) أدوارهم ومسؤولياتهم.

	الوظيفة	الفئة	الفئة الفرعية
		المتابعة والمراجعة (GV.MT-P): يتم فهم السياسات والعمليات والإجراءات الخاصة بالمراجعة المستمرة لوضع خصوصية المؤسسة وتوجيه عملية إدارة مخاطر الخصوصية.	**GV.MT-P1:** يتم إعادة تقييم مخاطر الخصوصية على أساس مستمر وكعوامل رئيسية، بما في ذلك بيئة أعمال المؤسسة (مثل إدخال تقنيات جديدة)، والحوكمة (مثل الالتزامات القانونية، ودرجة تحمل المخاطر)، ومعالجة البيانات، وتغيير الأنظمة/المنتجات/الخدمات.
			GV.MT-P2: تتم مراجعة قيم الخصوصية والسياسات والتدريب، ويتم الإبلاغ بأي تحديثات تتم على أي منها.
			GV.MT-P3: وضع وتنفيذ السياسات والعمليات والإجراءات لتقييم مدى الامتثال للمتطلبات القانونية وسياسات الخصوصية.
			GV.MT-P4: وضع وتنفيذ السياسات والعمليات والإجراءات للإبلاغ بالتقدم المحرز في إدارة مخاطر الخصوصية.
			GV.MT-P5: وضع وتنفيذ سياسات وعمليات وإجراءات حول إجراءات البيانات المسببة للمشاكل التي كشفت عنها مصادر داخلية وخارجية للمؤسسة وتحليلها والاستجابة لها (على سبيل المثال، الاكتشاف الداخلي، وباحثو الخصوصية، والحوادث المهنية).
			GV.MT-P6: تتضمن السياسات والعمليات والإجراءات الدروس المستفادة من إجراءات البيانات المسببة للمشاكل.
			GV.MT-P7: وضع وتنفيذ سياسات وعمليات وإجراءات تلقي شكاوى وشواغل واستفسارات الأفراد حول ممارسات الخصوصية بالمؤسسة ومتابعتها والاستجابة لها.

	الوظيفة	الفئة	الفئة الفرعية
	التحكم– الخصوصية: وضع وتنفيذ الأنشطة المناسبة لتمكين المؤسسات والأفراد من إدارة البيانات بالدقة الكافية لإدارة مخاطر الخصوصية.	**سياسات وعمليات وإجراءات معالجة البيانات (CT.PO-P):** يتم الاحتفاظ بالسياسات والعمليات والإجراءات واستخدامها لإدارة معالجة البيانات (كالغرض والنطاق والأدوار والمسؤوليات في منظومة معالجة البيانات، والتزام الإدارة) بما يتفق مع استراتيجية المخاطر التي تطبقها المؤسسة لحماية خصوصية الأفراد.	**CT.PO-P1:** وضع وتنفيذ سياسات وعمليات وإجراءات التصريح بمعالجة البيانات (كالقرارات التنظيمية والموافقات الفردية)، وإلغاء التراخيص، والإبقاء على التراخيص.
			CT.PO-P2: وضع وتنفيذ سياسات وعمليات وإجراءات لتمكين مراجعة البيانات أو نقلها أو مشاركتها أو الكشف عنها وتعديلها وحذفها (للحفاظ على جودة البيانات وإدارة الاحتفاظ بالبيانات).
			CT.PO-P3: وضع وتنفيذ سياسات وعمليات وإجراءات تمكين أفضليات وطلبات معالجة بيانات الأفراد.
			CT.PO-P4: مواءمة دورة حياة البيانات لإدارة البيانات وتنفيذها مع دورة حياة تطوير النظام لإدارة الأنظمة.
		إدارة معالجة البيانات (CT.DM-P): تتم إدارة البيانات بما يتوافق مع إستراتيجية المخاطر التي تنفذها المؤسسة لحماية خصوصية الأفراد، وزيادة القدرة على الإدارة، وتمكين تنفيذ مبادئ الخصوصية (مثال، المشاركة الفردية، وجودة البيانات، وتصغير حجم البيانات).	**CT.DM-P1:** يمكن الوصول إلى عناصر البيانات لمراجعتها.
			CT.DM-P2: يمكن الوصول إلى عناصر البيانات لنقلها أو الإفصاح عنها.
			CT.DM-P3: يمكن الوصول إلى عناصر البيانات لتغيرها.
			CT.DM-P4: يمكن الوصول إلى عناصر البيانات لحذفها.
			CT.DM-P5: تدمير البيانات وفقاً للسياسة المتبعة.
			CT.DM-P6: نقل البيانات باستخدام تنسيقات موحدة.

	الوظيفة	الفئة	الفئة الفرعية
			CT.DM-P7: وضع وتنفيذ آليات لنقل أذونات المعالجة البيانات ذات الصلة وقيمها بعناصر البيانات.
			CT.DM-P8: تحديد سجلات التدقيق أو الدخول وتوثيقها وتنفيذها ومراجعتها وفقاً للسياسة وتضمين مبدأ تصغير حجم البيانات.
			CT.DM-P9: اختبار وتقييم التدابير الفنية المعمول بها في إدارة معالجة البيانات.
			CT.DM-P10: إدراج تفضيلات خصوصية أصحاب المصلحة في أهداف التصميم الحسابي، وتقييم المخرجات بمقارنتها بهذه التفضيلات.
		المعالجة غير المقترنة (CT.DP-P): تزيد حلول معالجة البيانات من عدم الاقتران وفقاً لاستراتيجية المخاطر المتبعة في المؤسسة لحماية خصوصية الأفراد وتمكين تنفيذ مبادئ الخصوصية (مثال، تصغير حجم البيانات).	**CT.DP-P1:** يتم معالجة البيانات للحد من قابلية المراقبة والربط (مثال: تُنفذ إجراءات البيانات على الأجهزة المحلية والحفاظ على الخصوصية بالتشفير).
			CT.DP-P2: معالجة البيانات للحد من تحديد هوية الأفراد (مثال: وتقنيات خصوصية إلغاء التعريف والترميز المميز).
			CT.DP-P3: يتم معالجة البيانات للحد من صياغة استنتاجات حول سلوك الأفراد أو أنشطتهم (مثال، معالجة البيانات هي عملية لامركزية، والتصميمات الموزعة).
			CT.DP-P4: تسمح تكوينات النظام أو الجهاز بالتجميع الانتقائي لعناصر البيانات أو الكشف عنها.
			CT.DP-P5: يتم استبدال مراجع السمة بقيم السمة.

	الوظيفة	الفئة	الفئة الفرعية
	التواصل– الخصوصية (CM-P): وضع وتنفيذ الأنشطة المناسبة لتمكين المؤسسات والأفراد من اكتساب فهم موثوق والمشاركة في حوار حول كيفية معالجة البيانات ذات الصلة بمخاطر الخصوصية.	**سياسات التواصل وعملياتها وإجراءاتها (CM.PO-P):** يتم الاحتفاظ بالسياسات والعمليات والإجراءات واستخدامها لزيادة شفافية ممارسات معالجة البيانات (كالغرض والنطاق والأدوار والمسؤوليات في منظومة معالجة البيانات، والالتزام بالإدارة) ومخاطر الخصوصية ذات الصلة.	**CM.PO-P1:** وضع وتنفيذ سياسات وعمليات وإجراءات الشفافية للتواصل بشأن أغراض معالجة البيانات وممارساتها ومخاطر الخصوصية المرتبطة بها.
			CM.PO-P2: تحديد الأدوار والمسؤوليات (مثل العلاقات العامة) للتواصل بشأن أغراض معالجة البيانات وممارساتها ومخاطر الخصوصية المرتبطة بها.
		التوعية بمعالجة البيانات (CM.AW-P): يتمتع الأفراد والمؤسسات بمعرفة موثوقة حول ممارسات معالجة البيانات ومخاطر الخصوصية المرتبطة بها، ويتم استخدام الآليات الفعالة والمحافظة عليها لزيادة إمكانية التنبؤ بما يتوافق مع استراتيجية المخاطر التي تستخدمها المؤسسة لحماية خصوصية الأفراد.	**CM.AW-P1:** آليات (مثل الإشعارات والتقارير الداخلية أو العامة) للتواصل بشأن أغراض معالجة البيانات وممارساتها ومخاطر الخصوصية المرتبطة بها وإتاحة خيارات لتمكين تفضيلات الأفراد وطلبات معالجة البيانات.
			CM.AW-P2: وضع وتنفيذ آليات الحصول على ملاحظات من الأفراد (باستخدام الدراسات الاستقصائية ومجموعات التركيز) للتواصل بشأن أغراض معالجة البيانات وممارساتها ومخاطر الخصوصية المرتبطة بها.
			CM.AW-P3: يُمكّن تصميم النظام/المنتج/الخدمة من قابلية الرؤية لمعالجة البيانات.
			CM.AW-P4: الاحتفاظ بسجلات حالات الإفصاح عن البيانات ومشاركتها، لإمكانية الوصول إليها لمراجعتها أو نقلها/الكشف عنها.
			CM.AW-P5: يمكن إبلاغ الأفراد أو المؤسسات بعمليات تصحيح البيانات أو حذفها (مثل مصادر البيانات) في منظومة معالجة البيانات
			CM.AW-P6: الاحتفاظ بمصدر البيانات ومنشأها ويمكن الوصول إليها لمراجعتها أو نقلها/الكشف عنها.

	الوظيفة	الفئة	الفئة الفرعية
			CM.AW-P7: إخطار الأفراد والمؤسسات المتأثرين بوقوع خرق أو حادث لخصوصيتهم.
			CM.AW-P8: يتم تعريف الأفراد بآليات التخفيف (مثل، مراقبة الائتمان، وسحب الموافقة، وتعديل البيانات أو حذفها) لمعالجة آثار إجراءات البيانات المسببة للمشاكل.
	الحماية–الخصوصية (PR-P): وضع وتنفيذ الضمانات الوقائية المناسبة لمعالجة البيانات	**سياسات حماية البيانات وعملياتها وإجراءاتها (PR.PO-P):** الاحتفاظ بسياسات وعمليات وإجراءات الأمن والخصوصية (كالغرض والنطاق والأدوار والمسؤوليات في منظومة معالجة البيانات، والالتزام بالإدارة)، واستخدامها لحماية البيانات.	**PR.PO-P1:** إنشاء التكوين الأساسي لتكنولوجيا المعلومات والمحافظة عليه مع دمج مبادئ الأمن (مثل، مفهوم الأداء الوظيفي الأدنى).
			PR.PO-P2: إنشاء وتنفيذ عمليات التحكم في تغيير التكوين.
			PR.PO-P3: إجراء النسخ الاحتياطي للمعلومات، والاحتفاظ به واختباره.
			PR.PO-P4: الالتزام بالسياسات واللوائح ذات الصلة بالبيئة التشغيلية المادية للأصول المؤسسية.
			PR.PO-P5: تحسين عمليات الحماية.
			PR.PO-P6: مشاركة تكنولوجيات كفاءة الحماية.
			PR.PO-P7: وضع خطط الاستجابة (الاستجابة للحوادث واستمرارية الأعمال) وخطط التعافي (التعافي من الحوادث والتعافي من الكوارث) وإدارتها.
			PR.PO-P8: اختبار خطط الاستجابة والتعافي.

	الوظيفة	الفئة	الفئة الفرعية
			PR.PO-P9: يتم إدراج إجراءات الخصوصية في ممارسات الموارد البشرية (مثل إلغاء التكوين، وفحص الموظفين).
			PR.PO-P10: وضع وتنفيذ خطة لإدارة الثغرات الأمنية.
		إدارة الهوية والمصادقة والتحكم في الوصول (PR.AC-P): يقتصر الوصول إلى البيانات والأجهزة على الأفراد والعمليات والأجهزة المصرح لها، وتتم إدارتها بما يتوافق مع ما المخاطر المقيمة للوصول غير المصرح به.	**PR.AC-P1**: يتم إصدار الهويات وبيانات الاعتماد وإدارتها والتحقق منها وإبطالها وتدقيقها للأفراد والعمليات والأجهزة المصرح لهم.
			PR.AC-P2: إدارة الوصول المادي إلى البيانات والأجهزة.
			PR.AC-P3: إدارة الوصول عن بعد.
			PR.AC-P4: تتم إدارة أذونات وتصاريح الوصول، بما في ذلك مبادئ الامتياز الأقل وفصل المهام.
			PR.AC-P5: حماية سلامة الشبكة (مثل فصل الشبكة أو تقسيم الشبكة)
			PR.AC-P6: يتم إثبات هوية الأفراد والأجهزة وفقاً لبيانات الاعتماد والمصادقة عليها بما يتناسب مع مخاطر المعاملة (مثل، مخاطر أمن وخصوصية الأفراد والمخاطر التنظيمية الأخرى).
		أمن البيانات (PR.DS-P): إدارة البيانات بما يتماشى مع استراتيجية المخاطر التي	**PR.DS-P1**: حماية البيانات الخاملة المخزنة
			PR.DS-P2: حماية البيانات المتنقلة

	الوظيفة	الفئة	الفئة الفرعية
		تستخدمها المؤسسة لحماية خصوصية الأفراد، والحفاظ على سرية البيانات وسلامتها وإتاحتها.	**PR.DS-P3:** إدارة الأنظمة/المنتجات/الخدمات والبيانات المرتبطة بها بشكلٍ رسمي خلال عمليات إزالة البيانات ونقلها والتخلص منها.
			PR.DS-P4: الحفاظ على القدرة الكافية لضمان إتاحة البيانات.
			PR.DS-P5: تنفيذ سبل الحماية من تسريب البيانات.
			PR.DS-P6: استخدام آليات فحص السلامة للتحقق من سلامة البرمجيات الحاسوبية والبرامج الثابتة وسلامة المعلومات.
			PR.DS-P7: فصل بيئة التطوير والاختبار عن بيئة الإنتاج.
			PR.DS-P8: استخدام آليات فحص السلامة للتحقق من سلامة الأجهزة.
		الصيانة (PR.MA-P): إجراء صيانة النظام والإصلاحات بما يتفق مع السياسات والعمليات والإجراءات.	**PR.MA-P1:** تنفيذ عمليات صيانة أصول المؤسسة وإصلاحها وتسجيلها باستخدام أدوات معتمدة وخاضعة للرقابة.
			PR.MA-P2: الموافقة على صيانة أصول المؤسسة عن بُعد وتسجيلها وتنفيذها بطريقة تحول دون الوصول غير المصرح به إليها.

	الوظيفة	الفئة	الفئة الفرعية
		التكنولوجيا الوقائية (PR.PT-P): إدارة الحلول الأمنية التكنولوجية لضمان أمن ومرونة الأنظمة/المنتجات/الخدمات والبيانات المرتبطة بها، بما يتوافق مع السياسات والعمليات والإجراءات والاتفاقيات ذات الصلة.	**PR.PT-P1:** حماية الوسائط القابلة للإزالة وفرض قيود على استخدامها وفقاً للسياسة المتبعة.
			PR.PT-P2: إدراج مبدأ الأداء الوظيفي الأدنى من خلال تكوين الأنظمة بغرض توفير الإمكانات الأساسية فقط.
			PR.PT-P3: حماية شبكات التواصل والتحكم.
			PR.PT-P4: تنفيذ بعض الآليات (مثل، ضمان الأمن من الفشل، وضبط موازنة الحمل، والتبديل الفوري) لتحقيق متطلبات المرونة في المواقف العادية والمعاكسة.

الملحق (ب): مسرد المصطلحات

يتضمن هذا الملحق تعريفات محددة تُستخدم لأغراض هذا المنشور.

مرجع السمة (المنشور الخاص للمعهد 800-63-3[8])
بيان يؤكد ملكية المشترك دون احتوائه بالضرورة على معلومات الهوية، بغض النظر عن التنسيق. على سبيل المثال، مرجع السمة "يوم الميلاد"، قد يكون "أكبر من 18" أو " مواليد شهر ديسمبر".

قيمة السمة (المنشور الخاص للمعهد 800-63-3[8])
بيان كامل يؤكد ملكية المشترك، بغض النظر عن تنسيقه. على سبيل المثال، قيمة السمة "يوم الميلاد"، قد تكون "1980/1/12" أو "1 ديسمبر 1980."

الإتاحة (الباب 44 من القانون الأمريكي [13])
ضمان الوصول إلى المعلومات واستخدامها في الوقت المناسب وبطريقة موثوقة.

الفئة
التقسيم الفرعي للوظيفة إلى مجموعات من نتائج الخصوصية المرتبطة ارتباطاً وثيقاً بالاحتياجات البرمجية والأنشطة الخاصة.

التواصل–الخصوصية (الوظيفة)
وضع وتنفيذ الأنشطة المناسبة لتمكين المؤسسات والأفراد من اكتساب فهم مؤكد والمشاركة في حوار حول كيفية معالجة البيانات ومخاطر الخصوصية المرتبطة بها.

السرية (الباب 44 من القانون الأمريكي [13])
الحفاظ على القيود المصرح بها على الوصول إلى المعلومات والكشف عنها، بما في ذلك وسائل حماية الخصوصية الشخصية ومعلومات الملكية.

التحكم – الخصوصية (الوظيفة)
وضع وتنفيذ الأنشطة المناسبة لتمكين المؤسسات والأفراد من إدارة البيانات بالدقة الكافية حتى تتمكن من إدارة مخاطر الخصوصية.

النواة
مجموعة من أنشطة ونتائج حماية الخصوصية. يتألف النواة لإطار الخصوصية من ثلاثة عناصر: الوظائف، والفئات، والفئات الفرعية.

حوادث الأمن السيبراني:

(إطار عمل تحسين الأمن السيبراني للبنية التحتية الحرجة[1])
أحد أحداث الأمن السيبراني حُدد أن لها أثراً على المؤسسة على نحو يستدعي الاستجابة والتعافي.

(مكتب الإدارة والميزانية 12-17[9])

حدث (1) يُعرض سلامة المعلومات أو نظام المعلومات أو سريتها أو إتاحتها لخطر فعلي أو وشيك في غياب سلطة قانونية؛ أو (2) يُشكل انتهاكاً أو تهديداً وشيكاً بانتهاك القانون أو السياسات الأمنية أو الإجراءات الأمنية أو سياسات الاستخدام المقبولة.

البيانات تمثيل للمعلومات في صورة رقمية أو غير رقمية.

إجراءات البيانات (مقتبس من التقرير الداخلي للمعهد رقم 8062[5]) عملية دورة حياة بيانات النظام/المنتج/الخدمة - بما في ذلك على سبيل المثال لا الحصر - جمع البيانات والاحتفاظ بها وتسجيلها وتوليدها وتحويلها واستخدامها والإفصاح عنها ومشاركتها ونقلها والتخلص منها.

عنصر البيانات أصغر وحدة محددة من البيانات تنقل معلومات ذات معنى.

معالجة البيانات (مقتبس من التقرير الداخلي للمعهد رقم 8062[5]) مجموعة مكتملة من إجراءات البيانات (أي دورة حياة البيانات الكاملة - بما في ذلك على سبيل المثال لا الحصر - جمع البيانات والاحتفاظ بها وتسجيلها وتوليدها وتحويلها واستخدامها والإفصاح عنها ومشاركتها ونقلها والتخلص منها).

منظومة معالجة البيانات العلاقات المعقدة والمتداخلة بين الكيانات المشاركة في إنشاء أو نشر الأنظمة أو المنتجات أو الخدمات أو أي مكونات أخرى تستخدم لمعالجة البيانات.

عدم الاقتران (مقتبس من التقرير الداخلي للمعهد رقم 8062[5]) تمكين معالجة البيانات أو الأحداث دون الاقتران بأفراد أو أجهزة تتجاوز المتطلبات التشغيلية للنظام.

الوظيفة أحد مكونات النواة الذي يوفر الحد الأعلى من الهيكل المطلوب لتنظيم أنشطة الخصوصية الأساسية في فئات وفئات فرعية.

وظيفة ضبط – الخصوصية وضع وتنفيذ هيكل الحوكمة التنظيمية لتمكين الفهم المستمر لأولويات إدارة المخاطر في المؤسسة التي يتم إبلاغها بمخاطر الخصوصية.

وظيفة تحديد – الخصوصية وضع الفهم التنظيمي لإدارة مخاطر الخصوصية التي يتعرض لها الأفراد نتيجة معالجة البيانات.

مستويات التنفيذ توفر نقطة مرجعية حول كيفية عرض المؤسسة لمخاطر الخصوصية وما إذا كان لديها عمليات وموارد كافية لإدارة هذه المخاطر.

الفرد شخص واحد أو مجموعة واحدة من الأشخاص على المستوى المجتمعي.

النزاهة (الباب 44 من القانون الأمريكي[13]) الحماية من أي تعديل أو إتلاف غير سليم للمعلومات، بما في ذلك ضمان عدم إنكار المعلومات وأصالتها.

الأصل تاريخ معالجة عنصر البيانات، الذي قد يشمل تدفقات البيانات من نقطة إلى نقطة، وإجراءات البيانات التي يتم تنفيذها على عنصر البيانات.

سهولة الإدارة (مقتبس من التقرير الداخلي للمعهد رقم 8062[5]) توفير القدرة على الإدارة الدقيقة للبيانات، بما في ذلك تعديل البيانات وحذفها والكشف الاختياري عنها.

البيانات الوصفية (مقتبس من المنشور الخاص للمعهد 53-800[10]) المعلومات التي تصف خصائص البيانات

قد تشمل هذه البيانات على سبيل المثال، البيانات الوصفية الهيكلية التي تصف هياكل البيانات (أي تنسيق البيانات، وصيغة بناء الجملة، والدلالات) والبيانات الوصفية التي تصف محتويات البيانات.

إمكانية التنبؤ (مقتبس من التقرير الداخلي للمعهد رقم 8062[5]) تمكين الافتراضات الموثوقة من قبل الأفراد والمالكين والمشغلين حول البيانات ومعالجتها بواسطة نظام أو منتج أو خدمة.

انتهاك الخصوصية (مقتبس من مذكرة مكتب الإدارة والميزانية رقم 17-12[9]) حالات فقدان السيطرة أو الاختراق أو الإفشاء غير المصرح به أو الاستحواذ غير المصرح به أو أي حدث مشابه حيث (1) يقوم شخص غير المستخدم المصرح له بالوصول إلى البيانات أو يحتمل أن يصل لها أو (2) وصول مستخدم مصرح به إلى البيانات لغرض آخر غير مصرح به.

مراقبة الخصوصية (مقتبس من المنشور الخاص للمعهد رقم 37-800[7]) الضمانات الإدارية والفنية والمادية التي تستخدمها المؤسسة لتلبية متطلبات الخصوصية.

حدث الخصوصية الحدوث الفعلي أو المحتمل لأحد إجراءات البيانات المسببة للمشاكل.

متطلبات الخصوصية مواصفات لوظائف النظام/المنتج/الخدمة تحقق نتائج الخصوصية المرغوبة لأصحاب المصلحة.

مخاطر الخصوصية احتمالية تعرض الأفراد للمشاكل الناجمة عن معالجة البيانات، والأثر الذي قد ينجم عن حدوثها.

تقييم مخاطر الخصوصية عملية فرعية لإدارة مخاطر الخصوصية لتحديد وتقييم بعض مخاطر الخصوصية.

إدارة مخاطر الخصوصية مجموعة من العمليات التنظيمية الشاملة تتمثل في تحديد وتقييم مخاطر الخصوصية والاستجابة والتصدي لها.

إجراءات البيانات المسببة للمشاكل أحد إجراءات البيانات التي قد تؤدي إلى وقوع تأثير سلبي على الأفراد.

(مقتبس من التقرير الداخلي للمعهد رقم 8062[5])

المعالجة انظر معالجة البيانات.

الملف التعريفي مجموعة من الوظائف، والفئات، والفئات الفرعية من النواة أعطتها المؤسسة الأولوية لتساعدها في إدارة مخاطر الخصوصية.

وظيفة حماية – الخصوصية وضع وتنفيذ الضمانات الوقائية المناسبة لمعالجة البيانات.

المنشأ (مقتبس من التقرير الداخلي للمعهد رقم 8112[11]) البيانات الوصفية المتعلقة بمنشأ أو مصدر البيانات المحددة.

المخاطر (المنشور الخاص للمعهد 800-30[12]) مقياس لمدى التهديد الذي يتعرض له كيان نتيجة ظرف أو حدث محتمل، وعادةً ما يكون دالة لـ: (1) الآثار السلبية التي قد تنشأ في حالة حدوث الظرف أو الحدث، و(2) احتمال حدوثها.

إدارة المخاطر عملية تحديد المخاطر وتقييمها والتصدي لها.

درجة تحمل المخاطر (المنشور الخاص للمعهد 800-39[6]) مستوى المخاطر أو درجة عدم اليقين المقبولة لدى المؤسسات.

الفئة الفرعية تقسيمات إضافية للفئة لنتائج محددة للأنشطة الفنية و/أو الإدارية.

المحلق (ج): الاختصارات

يُعرّف هذا الملحق بعض الاختصارات المُستخدمة في هذا المنشور.

IEC	اللجنة الكهروتقنية الدولية
IR	التقرير المشترك بين الوكالات أو التقرير الداخلي
ISO	المنظمة الدولية للتوحيد القياسي
IT	تكنولوجيا المعلومات
NIST	المعهد الدولي للمعايير والتكنولوجيا
OASIS	منظمة تطوير معايير المعلومات المهيكلة
OECD	منظمة التعاون والتنمية في الميدان الاقتصادي
OMB	مكتب الإدارة والميزانية
PMRM	النموذج المرجعي لإدارة الخصوصية ومنهجيتها
PRAM	منهجية تقييم مخاطر الخصوصية
RFC	طلب تعليقات
RFI	طلب معلومات
SDLC	دورة حياة تطوير المشروع
SP	المنشور الخاص

الملحق (د): ممارسات إدارة مخاطر الخصوصية

يقدم القسم 1.2 عدداً من الاعتبارات حول إدارة مخاطر الخصوصية، بما في ذلك العلاقة بين مخاطر الأمن السيبراني ومخاطر الخصوصية، وكذلك دور تقييم مخاطر الخصوصية. ويركز هذا الملحق على بعض الممارسات الرئيسية التي تساهم في الإدارة الناجحة لمخاطر الخصوصية، وذلك بعدة طرق من بينها تنظيم الموارد الإعدادية، وتحديد قدرات الخصوصية، وتحديد متطلبات الخصوصية، وإجراء تقييمات مخاطر الخصوصية، وإنشاء متطلبات تتبع مخاطر الخصوصية، ومراقبة مخاطر الخصوصية المتغيرة. وقد تم إدراج مراجع الفئات والفئات الفرعية لتسهيل استخدام النواة على نحو يدعم هذه الممارسات، وهذه المراجع مكتوبة بين أقواس.

تنظيم الموارد التحضيرية

يُساعد توافر الموارد المناسبة على تيسير اتخاذ قرارات مستنيرة بشأن مخاطر الخصوصية على جميع مستويات المؤسسة. من الناحية العملية، قد تُسند مسؤولية تطوير مختلف الموارد إلى عناصر مختلفة بالمؤسسة. لذلك، قد يجد أحد عناصر المؤسسة التي تعتمد على موارد معينة أن هذه الموارد غير متاحة أو أنها لا تتناول الخصوصية كما ينبغي. ويمكن للعنصر التابع، في هكذا ظروف، النظر في الغرض من المورد ليتمكن من تلقي المعلومات من مصادر أخرى، أو اتخاذ أفضل قرار ممكن باستخدام المعلومات المتاحة. إيجازاً لما سبق، تعد الموارد الجيدة مفيدة، ولكن لا ينبغي لأي أوجه قصور منع عناصر المؤسسة من اتخاذ أفضل قرار بشأن المخاطر وفق الإمكانيات المتاحة.

تضع الموارد التالية، وإن لم تكن شاملة، أساساً لاتخاذ قرارات أفضل.

- **التكليف بدور إدارة المخاطر (GV.PO-P3, GV.PO-P4)**

من شأن إنشاء وتمكين الفهم عبر المؤسسة حول هوية المسؤول عن إدارة مخاطر الخصوصية بالإضافة إلى مهام إدارة المخاطر الأخرى فيها أن يدعم التنسيق والمساءلة بشكل أفضل، وبالتالي تحسين اتخاذ القرار. بالإضافة إلى ذلك، قد يساعد تعدد وجهات النظر على تحسين عملية تحديد وتقييم مخاطر الخصوصية والاستجابة لها، وكذلك يمكن الاستعانة بفريق متنوع ومتعدد الوظائف لتحديد نطاق أكثر شمولاً من المخاطر التي تهدد خصوصية الأفراد، واختيار مجموعة أوسع من وسائل التخفيف من حدة تلك المخاطر. ويعتمد تحديد الأدوار التي ينبغي تضمينها في مناقشات إدارة المخاطر على سياق المؤسسة وبنيتها، دون إغفال أهمية التعاون بين برنامجي الخصوصية والأمن السيبراني للمؤسسة. وفي حالة تكليف فرد واحد بأكثر من دور، فينبغي تلافي أي تضارب محتمل في المصالح.

- **استراتيجية إدارة المخاطر المؤسسية (GV.RM-P)**

تساعد إستراتيجية إدارة المخاطر المؤسسية المؤسسات على مواءمة مهمتها وقيمتها مع درجة تحمل المخاطر المؤسسية والافتراضات والقيود والأولويات. ومن المحتمل تقديم بعض التنازلات للتعامل مع القيود المفروضة على الموارد حتى يُمكن تحقيق مهمة المؤسسة أو أهداف العمل، وكذلك إدارة مجموعة كبيرة من المخاطر. وينبغي أن يساعد تمكين الموظفين المشاركين في عملية إدارة مخاطر الخصوصية لتحسين فهم درجة تحمل مخاطر المؤسسة في توجيه القرارات المتخذة حول كيفية تخصيص الموارد وتحسين القرارات المتعلقة بالاستجابة للمخاطر.

- **أصحاب المصلحة الرئيسيون (GV.PO-P4, ID.DE-P)**

أصحاب المصلحة المعنيين بالخصوصية هم المهتمين أو المنشغلين بنتائج خصوصية النظام أو المنتج أو الخدمة. على سبيل المثال، من المحتمل أن تركز المخاوف القانونية على ما إذا كان النظام أو المنتج أو الخدمة يعمل بطريقة من شأنها أن تتسبب في عدم امتثال المؤسسة لقوانين أو لوائح الخصوصية أو اتفاقيات العمل ذات الصلة. وقد يشعر أصحاب الأعمال الذين يرغبون في زيادة الاستخدام إلى الحد الأقصى بالقلق بشأن فقدان الثقة في النظام/المنتج/الخدمة بسبب تدني درجة الخصوصية. يرغب الأفراد الذين تتم معالجة بياناتهم أو الذين يتفاعلون مع النظام/المنتج/الخدمة في عدم مواجهة مشكلات أو عواقب سلبية. لذا، سيسهل تكوين فكرة واضحة عن أصحاب المصلحة وأنواع نتائج الخصوصية التي يهتمون بها تصميم النظام/المنتج/الخدمة الذي يلبي احتياجات أصحاب المصلحة بشكل مناسب.

- **متطلبات الخصوصية على مستوى المؤسسة (GV.PO-P)**

متطلبات الخصوصية على مستوى المؤسسة هي وسيلة للتعبير عن الالتزامات القانونية وقيم الخصوصية والسياسات التي تعتزم المؤسسة الالتزام بها. ويعد فهم هذه المتطلبات أمراً أساسياً لضمان توافق تصميم النظام/المنتج/الخدمة مع التزاماته. ويمكن اشتقاق متطلبات الخصوصية هذه من مصادر مختلفة، منها مثلاً:

  - البيئة القانونية (مثل القوانين واللوائح والعقود).
  - سياسات المؤسسة أو قيمها الثقافية.
  - المعايير ذات الصلة.
  - مبادئ الخصوصية.

- **عناصر تصميم النظام/المنتج/الخدمة (ID.BE-P3)**

قد تتخذ أدوات التصميم أشكالاً مختلفة (مثل تصميم النظام أو مخططات تدفق البيانات)، والتي تساعد المؤسسة في تحديد كيف ستعمل أنظمتها/منتجاتها/خدماتها، الأمر الذي يجعلها قادرة على مساعدة برامج الخصوصية في فهم كيفية عمل الأنظمة/المنتجات/الخدمات بحيث يمكن تحديد وتنفيذ الضوابط أو الإجراءات التي تساعد على التخفيف من مخاطر الخصوصية بطرق تحافظ على الوظائف وتحمي أيضاً حماية الخصوصية.

- **خرائط البيانات** (ID.IM-P)

توضح خرائط البيانات معالجة البيانات وتفاعلات الأفراد مع الأنظمة والمنتجات والخدمات، كما تُظهر هذه الخرائط بيئة معالجة البيانات، وتشير إلى المكونات المستخدمة لمعالجة البيانات أو التي يتفاعل معها الأفراد، ومالكو المكونات أو مشغلوها، وإجراءات البيانات غير المترابطة وعناصر البيانات المحددة التي تتم معالجتها. علاوةً على ذلك، يمكن رسم خرائط البيانات بطرق مختلفة، وقد يختلف مستوى التفاصيل بناءً على احتياجات المؤسسة. ويُمكن تركيب خريطة البيانات فوق عناصر تصميم النظام/المنتج/الخدمة الموجودة للتيسير وسهولة الاتصال بين أفراد المؤسسة. كما هو موضح أدناه، تعد خريطة البيانات أداة مهمة في تقييم مخاطر الخصوصية.

تحديد إمكانيات الخصوصية

يمكن استخدام إمكانيات الخصوصية لوصف سمات أو مزايا النظام أو المنتج أو الخدمة التي تحقق نتيجة الخصوصية المرغوبة (على سبيل المثال، "تتيح الخدمة تصغير حجم البيانات"). وتُستخدم سرية أهداف أمن البيانات وسلامتها وإتاحتها إلى جانب متطلبات الأمان لتوجيه إمكانيات أمن النظام أو المنتج أو الخدمة. ويمكن تحديد إمكانيات الخصوصية بتحقيق مجموعة إضافية من أهداف هندسة الخصوصية كما يوضح الجدول 3، حيث قد تستخدم المؤسسة أيضاً أهداف هندسة الخصوصية كأداة عالية المستوى لتحديد الأولويات. ومن المؤشرات على زيادة مخاطر الخصوصية، ضعف إمكانية التنبؤ بالأنظمة أو المنتجات أو الخدمات أو إدارتها أو عدم اقترانها، وبالتالي ينبغي أن تجري هذه المؤسسة تقييماً أكثر شمولاً لمخاطر الخصوصية.

عند تحديد إمكانات الخصوصية، قد تنظر المؤسسة في أيهما أكثر أهمية - أهداف هندسة الخصوصية أم أهداف الأمن - لتحقيق مهمتها، أو احتياجات العمل، ودرجة تحمل المخاطر، ومتطلبات الخصوصية على مستوى المؤسسة (انظر تنظيم الموارد التحضيرية أعلاه). قد لا تتساوى جميع الأهداف في الأهمية، أو قد يكون من الضروري المفاضلة بينها. ورغم أن إمكانات الخصوصية توجه تقييم مخاطر الخصوصية من خلال دعم قرارات تحديد أولويات المخاطر، إلا أنه قد يتم أيضاً توجيه قدرات الخصوصية من خلال تقييم المخاطر وتعديلها لدعم إدارة مخاطر الخصوصية المحددة أو معالجة التغييرات في البيئة، بما في ذلك تغييرات تصميم النظام أو المنتج أو الخدمة.

جدول 3: أهداف هندسة الخصوصية وأهداف أمن الخصوصية[18]

	الهدف	التعريف	الوظائف ذات الصلة بالمبادئ وفقاً للهيكل الأساسي لإطار عمل الخصوصية
صية	إمكانية التنبؤ	تمكين الافتراضات الموثوقة من قبل الأفراد والمالكين والمشغلين حول البيانات ومعالجتها بواسطة نظام أو منتج أو خدمة.	التحديد–الخصوصية، والضبط–الخصوصية، والتحكم–الخصوصية، والتواصل–الخصوصية، والحماية–الخصوصية
	سهولة الإدارة	توفير القدرة على الإدارة الدقيقة للبيانات، بما في ذلك تعديلها وحذفها والكشف الاختياري عنها.	التحديد–الخصوصية، والضبط–الخصوصية، والتحكم–الخصوصية
	عدم الاقتران	تمكين معالجة البيانات أو الأحداث دون الاقتران بأفراد أو أجهزة تتجاوز المتطلبات التشغيلية للنظام.	التحديد–الخصوصية، والضبط–الخصوصية، والتحكم–الخصوصية
لأمن	السرية	الحفاظ على القيود المصرح بها على الوصول إلى المعلومات والكشف عنها، بما في ذلك وسائل حماية الخصوصية الشخصية ومعلومات الملكية.	التحديد–الخصوصية، والضبط–الخصوصية، والحماية–الخصوصية
	السلامة	الحماية من أي تعديل أو إتلاف غير سليم للمعلومات، بما في ذلك ضمان عدم إنكار المعلومات وأصالتها.	التحديد–الخصوصية، والضبط–الخصوصية، والحماية–الخصوصية
	الإتاحة	ضمان الوصول إلى البيانات واستخدامها في الوقت المناسب وبطريقة موثوقة	التحديد–الخصوصية، والضبط–الخصوصية، والحماية–الخصوصية

[18] أهداف هندسة الخصوصية مقتبسة من التقرير الداخلي للمعهد الوطني للمعايير والتكنولوجيا رقم 8062 [5]، أما أهداف الأمن فمقتبسة من المنشور الخاص للمعهد رقم 37-800، المراجعة 2 [7].

تعريف متطلبات الخصوصية

تحدد متطلبات الخصوصية الطريقة التي ينبغي أن يعمل بها النظام أو المنتج أو الخدمة لتلبية نتائج الخصوصية التي ينشدها أصحاب المصلحة (على سبيل المثال، "تم تكوين التطبيق بحيث يسمح للمستخدمين بتحديد عناصر بيانات محددة"). ولتحديد متطلبات الخصوصية، ينبغي وضع متطلبات الخصوصية على مستوى المؤسسة (انظر تنظيم الموارد التحضيرية أعلاه)، ومخرجات تقييم مخاطر الخصوصية، في الاعتبار. وتساعد هذه العملية المؤسسة على الإجابة عن سؤالين: (1) كيف *يمكن* أن يستفيد نظام أو منتج أو خدمة ما من معالجة البيانات والتفاعل مع الأفراد؟ و(2) ماذا الذي يجب أن يفعله النظام أو المنتج أو الخدمة؟ عندها يمكن للمؤسسة تخصيص الموارد لتصميم نظام أو منتج أو خدمة بطريقة تحقق المتطلبات المحددة. وفي نهاية المطاف يمكن أن يؤدي تحديد متطلبات الخصوصية إلى تطوير الأنظمة والمنتجات والخدمات التي تولي اهتمامها لخصوصية الأفراد، والتي تستند إلى قرارات مستنيرة بشأن المخاطر.

إجراء عمليات تقييم مخاطر الخصوصية

تتمكن المؤسسات، من خلال إجراء تقييم مخاطر الخصوصية، من تحديد مخاطر الخصوصية التي يسببها النظام أو المنتج أو الخدمة، وترتيبها بحسب الأولوية بما يكفل تمكين المؤسسة من اتخاذ قرارات مستنيرة حول كيفية الاستجابة للمخاطر (ID.RA-P، GV.RM-P). وقد تختلف منهجيات إجراء تقييم مخاطر الخصوصية، ولكن على المؤسسات مراعاة الخصائص التالية:[19]

- **نموذج المخاطر (ID.RA-P, GV.MT-P1)**

تحدد هذه النماذج عوامل المخاطر التي سيتم تقييمها، والعلاقات بين هذه العوامل.[20] وإذا لم تكن المؤسسة تستخدم نموذج مخاطر محدد مسبقاً، فعليها تحديد عوامل المخاطر التي ستقوم بتقييمها، وكذا العلاقات بين هذه العوامل. ولا يوجد نموذج واحد مقبول بشكل عام لمخاطر الخصوصية رغم أن لدى الأمن السيبراني نموذج مخاطر مستخدم على نطاق واسع ويستند إلى عوامل المخاطر المتمثلة في التهديدات والثغرات الأمنية والاحتمالية والأثر. وقد صمم المعهد الوطني للمعايير والتكنولوجيا نموذج لمخاطر الخصوصية لحساب المخاطر استناداً إلى احتمالية تنفيذ إجراءات البيانات المسببة للمشاكل مضروبة في أثر هذه الإجراءات، ونوضح أدناه عوامل المخاطر الثلاثة:

عوامل مخاطر الخصوصية:

إجراءات البيانات المسببة للمشاكل | الاحتمالية | الأثر

- يُقصد بإجراءات البيانات الإشكالية أي إجراء يتخذه النظام لمعالجة البيانات قد ينتج عنه مشكلة للأفراد. وتنظر المؤسسات في نوع المشاكل ذات الصلة بالأفراد. ويمكن أن تأتي المشاكل في أي صورة، وقد تأخذ تجربة الأفراد بعين الاعتبار.[21]

---

[19] وضع المعهد الوطني للمعايير والتكنولوجيا منهجية لتقييم مخاطر الخصوصية لمساعدة المؤسسات في تحديد وتقييم المخاطر والاستجابة لها. وهذه المنهجية مكونة من مجموعة من أوراق العمل ومتاحة على [3].

[20] انظر المنشور الخاص للمعهد الوطني للمعايير والتكنولوجيا رقم 30-800، المراجعة 1، Guide for Conducting Risk Assessments [دليل إجراء عمليات تقييم المخاطر] [12] صفحة 8.

[21] أنشأ المعهد، في إطار منهجية تقييم مخاطر الخصوصية، فهرس توضيحي لإجراءات البيانات المسببة للمشاكل والمشكلات ذات الصلة لدراستها [3]. وقد تنشئ مؤسسات أخرى مجموعات إضافية من المشكلات، أو ربما تشير إليها وكأن لها عواقب أو أضرار.

- الاحتمالية هي تحليل سياقي يُرجح أن يؤدي إجراء البيانات إلى خلق مشكلة لمجموعة تمثيلية من الأفراد. وقد يشمل هذا السياق عوامل تنظيمية (كالموقع الجغرافي، والتصور العام حول المؤسسات المشاركة فيما يتعلق بالخصوصية)، وعوامل النظام (كطبيعة وتاريخ تفاعلات الأفراد مع النظام، ووضوح عملية معالجة البيانات للأفراد والأطراف الثالثة)، أو العوامل الفردية (كالتركيبة السكانية للأفراد، أو اهتمامات أو تصورات الخصوصية، أو مدى حساسية البيانات).[22] وربما تساعد خريطة البيانات في هذا التحليل السياقي (انظر تنظيم الموارد التحضيرية).
- الأثر هو تحليل التكاليف في حالة حدوث المشكلة. وكما ذُكر في القسم 1.2، لا تواجه المؤسسات هذه المشكلات بشكل مباشر. علاوة على ذلك، تختلف تجربة كل فرد عن تجربة آخر، بالتالي، قد يصعب تقييم الأثر بدقة. ويجب أن تدرس المؤسسات أفضل الوسائل لاستيعاب أثر المشكلة على الأفراد من أجل تحديد أولويات مخاطر الخصوصية والاستجابة لها بالطريقة المناسبة.[23]

- **نهج التقييم**

نهج التقييم هو الآلية المتبعة لترتيب المخاطر التي المرتبة بحسب الأولوية. ويمكن تصنيف نُهج التقييم إلى ثلاث فئات (كمية أو شبه كمية أو نوعية)[24] [25]

- **ترتيب المخاطر حسب الأولوية** (ID.RA-P4)

تُعطي المؤسسات الأولوية للمخاطر لتسهيل التواصل حول كيفية الاستجابة لها حسب الأولوية،[26] نظراً للحدود المطبقة على موارد المؤسسة.

- **الاستجابة للمخاطر** (ID.RA-P5)

تتضمن نُهج الاستجابة، التخفيف من حدة المخاطر أو نقلها أو تقاسمها أو تجنبها أو قبولها كما هو موضح في القسم 1.2.2.[27]

تتبع عملية وضع متطلبات الخصوصية

بمجرد أن تحدد المؤسسة المخاطر التي يجب التخفيف منها، يكون في إمكانها تنقيح متطلبات الخصوصية ثم انتقاء وتنفيذ الضوابط (أي الضمانات الوقائية الفنية و/أو المادية و/أو السياسية) لتلبية متطلباتها.[28] قد تستخدم المؤسسة مجموعة متنوعة من المصادر لتحديد الضوابط، مثل منشور المعهد رقم 800-53، *Security and Privacy Controls*

[22] انظر منهجية تقييم مخاطر الخصوصية التي وضعها المعهد لمعلومات إضافية عن العوامل السياقية. انظر ورقة العمل رقم 2.

[23] يستخدم منهجية تقييم مخاطر الخصوصية التي وضعها المعهد التكاليف المؤسسية مثل تكاليف عدم الامتثال، وتكاليف الأعمال المباشرة، وتكاليف السمعة، وتكاليف الثقافة الداخلية، كأسباب تدفعها للنظر في كيفية تقييم الأثر على الأفراد. انظر ورقة العمل رقم 3، علامة تبويب "الأثر".

[24] انظر المنشور الخاص للمعهد رقم 800-30، المراجعة 1، Guide for Conducting Risk Assessments [دليل إجراء عمليات تقييم المخاطر] [12] ص. 14.

[25] تستخدم منهجية تقييم مخاطر الخصوصية التي وضعها المعهد نهجاً شبه كمي بمقياس من 1 إلى 10.

[26] تقدم منهجية تقييم مخاطر الخصوصية التي وضعها المعهد تمثيلات متنوعة لترتيب الأولوية، ومنها على سبيل المثال خريطة الحرارة. انظر [3] ورقة العمل رقم 3.

[27] تقدم منهجية تقييم مخاطر الخصوصية التي وضعها المعهد عملية للاستجابة لمخاطر الخصوصية ذات الأولوية. انظر ورقة العمل رقم 4.

[28] انظر المنشور الخاص للمعهد رقم 800-37، المراجعة 2 [7].

for Information Systems and Organizations [ضوابط الأمن والخصوصية لأنظمة المعلومات والمؤسسات].[29] بعد التنفيذ، تقوم المؤسسة بشكل متكرر بتقييم الضوابط للتأكد من فعاليتها في تلبية متطلبات الخصوصية وإدارة مخاطر الخصوصية. بهذه الطريقة، تنشئ المؤسسة إمكانية تتبع ضوابط ومتطلبات الخصوصية، وتوضح المساءلة بين أنظمتها ومنتجاتها وخدماتها وأهداف الخصوصية التنظيمية لديها.

متابعة التغيير

إدارة مخاطر الخصوصية ليست عملية ثابتة، حيث تلاحظ المؤسسات كيفية تأثر مخاطر الخصوصية لديها بالتغييرات التي تتم في بيئة أعمالها - بما في ذلك وضع القوانين واللوائح الجديدة والتقنيات الناشئة - والتغييرات المقابلة في أنظمتها ومنتجاتها وخدماتها، وتستخدم بشكل متكرر الممارسات المبينة في هذا الملحق لضبط عملياتها استناداً إلى تلك التغييرات. (GV.MT-P1)

[29] انظر المنشور الخاص للمعهد رقم 53-800، وتحديثاته [10].

الملحق (هـ): تعريفات مستويات التنفيذ

يتم تعريف كل مستوى من المستويات الأربعة الملخصة أدناه في إطار أربعة عناصر:

المستوى الأول: العناصر الجزئية

- **عملية إدارة مخاطر الخصوصية** - لم يتم إضفاء الطابع الرسمي على ممارسات إدارة مخاطر الخصوصية التنظيمية، وتتم إدارتها بطريقة مخصصة، وأحياناً بطريقة تفاعلية. وقد لا يتم تحديد أولويات أنشطة الخصوصية بشكل مباشر من خلال أولويات إدارة المخاطر التنظيمية أو تقييمات مخاطر الخصوصية أو مهام المؤسسة أو أهداف العمل.
- **برنامج متكامل لإدارة مخاطر الخصوصية** – إن الوعي بمخاطر الخصوصية على مستوى المؤسسة محدود، حيث تقوم المؤسسة بإدارة مخاطر الخصوصية على أساس غير منتظم، وحسب كل حالة على حدة، نظراً لاختلاف الخبرات أو المعلومات المكتسبة من مصادر خارجية. وقد لا تمتلك المؤسسة العمليات التي تمكنها من مشاركة المعلومات حول معالجة البيانات ومخاطر الخصوصية الناجمة عنها في المؤسسة.
- **العلاقات في منظومة معالجة البيانات** – ثمة فهم محدود لدور (أدوار) المؤسسة تجاه الكيانات الأخرى (مثل المشترين والموردين ومقدمي الخدمات وشركاء الأعمال والشركاء) في المنظومة الأكبر. ولا تمتلك المؤسسة عمليات لتحديد كيفية انتشار مخاطر الخصوصية في جميع أنحاء المنظومة أو لإبلاغ الكيانات الأخرى في المنظومة بمخاطر أو متطلبات الخصوصية.
- **القوى العاملة** – قد يكون استيعاب بعض الموظفين لمخاطر الخصوصية أو عمليات إدارة هذه المخاطر محدوداً، وقد لا يكون لديهم مسؤوليات خصوصية محددة. وإذا وفرت لهم المؤسسة التدريب على الخصوصية، فإنه يكون مخصصاً ولا يتم تحديث محتواه وفقاً لأفضل الممارسات.

المستوى الثاني: العناصر التي توجهها المخاطر

- **عملية إدارة مخاطر الخصوصية** – توافق الإدارة على ممارسات إدارة المخاطر، ولكن قد لا يتم تطبيق سياسة ذات صلة على مستوى المؤسسة. ويتم تحديد أولويات أنشطة الخصوصية بشكلٍ مباشرٍ من خلال أولويات إدارة المخاطر التنظيمية أو تقييمات مخاطر الخصوصية أو مهام المؤسسة أو أهداف المشروع التجاري.
- **برنامج متكامل لإدارة مخاطر الخصوصية** – ثمة وعي بمخاطر الخصوصية على مستوى المؤسسة، ولكن لم يتم وضع نهج شامل للمؤسسة لإدارة مخاطر الخصوصية. ويتم تبادل المعلومات حول معالجة البيانات ومخاطر الخصوصية الناجمة عنها داخل المؤسسة على أساس غير رسمي. وقد يتم مراعاة الخصوصية عند وضع الأهداف والبرامج التنظيمية على بعض مستويات المؤسسة وليس جميعها، ويتم تقييم مخاطر الخصوصية، لكن ذلك لا يتكرر أو يحدث عادةً.
- **العلاقات في منظومة معالجة البيانات** – ثمة فهم جزئي لدور (أدوار) المؤسسة تجاه الكيانات الأخرى (مثل المشترين والموردين ومقدمي الخدمات وشركاء الأعمال والشركاء) في المنظومة الأكبر. وتدرك المؤسسة مخاطر المنظومة المرتبطة بالمنتجات والخدمات التي تقدمها وتستخدمها، ولكنها لا تعمل بشكل متسق أو رسمي على مواجهة هذه المخاطر.
- **القوى العاملة** – تُسند إلى بعض الموظفين مسؤوليات خصوصية محددة، ولكن ربما يضطلعون بمسؤوليات غير متعلقة بالخصوصية أيضاً. ويتلقى موظفي الخصوصية بانتظام تدريبات على الخصوصية، رغم عدم وجود عملية متسقة لتحديث المحتوى التدريبي وفقاً لأفضل الممارسات.

المستوى الثالث: العناصر القابلة للتكرار

- **عملية إدارة مخاطر الخصوصية –** ثمة موافقة رسمية على ممارسات إدارة المخاطر في المؤسسة ومقدَّمة كإحدى سياسات المؤسسة. يتم تحديث ممارسات الخصوصية المؤسسية بانتظام بناءً على تطبيق عمليات إدارة المخاطر على التغييرات في المهمة أو أهداف العمل، والمخاطر المتغيرة، والسياسة، والمشهد التكنولوجي.
- **برنامج متكامل لإدارة مخاطر الخصوصية –** يتم تطبيق نهج على مستوى المؤسسة لإدارة مخاطر الخصوصية، حيث يتم تحديد وتنفيذ ومراجعة سياسات وعمليات وإجراءات على إطلاع بالمخاطر. وتتبع المؤسسة طرق متسقة للاستجابة بفعالية للتغيرات في المخاطر، وتراقب مخاطر الخصوصية على نحو مستمر ودقيق. ويتواصل كبار المسؤولين التنفيذيين في مجال الخصوصية والمجالات الأخرى بانتظام لمناقشة مخاطر الخصوصية، ويضمنون مراعاة الخصوصية في جميع عمليات المؤسسة.
- **العلاقات في منظومة معالجة البيانات –** تستوعب المؤسسة دورها (أدوارها) وتبعياتها وتوابعها في المنظومة الأكبر، وتسهم في توعية المجتمع على النطاق الأوسع بالمخاطر. وتدرك المنظمة مخاطر الخصوصية المرتبطة بالمنتجات والخدمات التي تقدمها وتستخدمها في المنظومة. بالإضافة إلى ذلك، عادةً ما تتخذ إجراءات رسمية للتعامل مع تلك المخاطر، كتنفيذ آليات مثل الاتفاقيات الخطية للإبلاغ بمتطلبات الخصوصية، وهياكل الحوكمة، وتنفيذ السياسة، ومتابعتها.
- **القوى العاملة –** لدى موظفي الخصوصية المتفانون المعرفة والمهارات اللازمة لأداء الأدوار والمسؤوليات المسندة إليهم، ويتلقى جميع الموظفين تدريب منتظم وحديث على الخصوصية.

المستوى الرابع: العناصر التكيفية

- **عملية إدارة مخاطر الخصوصية –** تقوم المؤسسة بتطويع ممارسات الخصوصية الخاصة بها بناءً على الدروس المستفادة من أحداث الخصوصية وتحديد مخاطر الخصوصية الجديدة. ومن خلال عملية التحسين المستمر التي تتضمن تقنيات وممارسات الخصوصية المتقدمة، تتكيف المؤسسة بفعالية مع السياسة المتغيرة والمشهد التكنولوجي، وتستجيب في الوقت المناسب وبطريقة فعالة لمخاطر الخصوصية المتطورة.
- **برنامج متكامل لإدارة مخاطر الخصوصية** – يتم تطبيق نهج على مستوى المؤسسة لإدارة مخاطر الخصوصية يعتمد على تنفيذ سياسات وعمليات وإجراءات واعية بالمخاطر، حتى ينجح في معالجة إجراءات البيانات المسببة للمشاكل. إن العلاقة بين مخاطر الخصوصية وأهداف المؤسسة مفهومة وواضحة، وينبغي وضعها في الاعتبار عند اتخاذ القرارات. ويتابع كبار المسؤولين التنفيذيين مخاطر الخصوصية كمتابعتهم لمخاطر الأمن السيبراني والمخاطر المالية والمخاطر المؤسسية الأخرى. وتعتمد ميزانية المؤسسة على فهم بيئة المخاطر الحالية والمتوقعة ودرجة تحمل المخاطر. وتقوم وحدات الأعمال بتنفيذ الرؤية التنفيذية وتحليل المخاطر على مستوى النظام في سياق تحمل مخاطر المؤسسة. وتعد إدارة مخاطر الخصوصية جزءاً من الثقافة التنظيمية، وتتطور من الدروس المستفادة إلى التوعية المستمرة بمعالجة البيانات ومخاطر الخصوصية الناجمة عنها. ويمكن للمؤسسة أن تحسب بسرعة وكفاءة التغييرات التي تطرأ على أهداف العمل/المهمة عند تحديد كيفية التعامل مع المخاطر والتواصل بشأنها.
- **العلاقات في منظومة معالجة البيانات –** تستوعب المؤسسة دورها (أدوارها) وتبعياتها وتوابعها في المنظومة الأكبر، وتسهم في توعية المجتمع على النطاق الأوسع بالمخاطر. وتستخدم المؤسسة معلومات في الوقت الفعلي أو شبه الفعلي لفهم مخاطر نظام الخصوصية المرتبطة بالمنتجات والخدمات التي تقدمها وتستخدمها، وتتخذ الإجراءات المناسبة وفقاً لذلك. كما تتواصل المؤسسة بشكل استباقي، عبر

الآليات الرسمية (مثل إبرام الاتفاقيات) والآليات غير الرسمية لإقامة علاقات قوية مع المنظومة، والحفاظ على تلك العلاقات.

- **القوى العاملة** – لدى المؤسسة مجموعات من المهارات المتخصصة ذات الصلة بالخصوصية في جميع أقسام هيكلها التنظيمي، ويساهم الموظفون أصحاب وجهات النظر المتنوعة في إدارة مخاطر الخصوصية. ويتم تزويد جميع الموظفين بتدريب منتظم وحديث ومتخصص بشأن الخصوصية. ويفهم الموظفون على جميع المستويات قيم الخصوصية المؤسسية ودورهم في الحفاظ عليها.