الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

# ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

# X.1058

(2017/03)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنة – إدارة الأمن

---

# تكنولوجيا المعلومات – التقنيات الأمنية – مدونة القواعد لحماية المعلومات المحدِّدة لهويّة الشخص

التوصية ITU-T X.1058

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

## شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

| | |
|---|---|
| الشبكات العمومية للبيانات | X.199–X.1 |
| التوصيل البيني للأنظمة المفتوحة | X.299–X.200 |
| التشغيل البيني للشبكات | X.399–X.300 |
| أنظمة معالجة الرسائل | X.499–X.400 |
| الدليل | X.599–X.500 |
| التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام | X.699–X.600 |
| إدارة التوصيل البيني للأنظمة المفتوحة (OSI) | X.799–X.700 |
| الأمن | X.849–X.800 |
| تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI) | X.899–X.850 |
| المعالجة الموزعة المفتوحة | X.999–X.900 |
| أمن المعلومات والشبكات | |
| الجوانب العامة للأمن | X.1029–X.1000 |
| أمن الشبكة | X.1049–X.1030 |
| **إدارة الأمن** | **X.1069–X.1050** |
| الخصائص البيومترية | X.1099–X.1080 |
| تطبيقات وخدمات آمنة | |
| أمن البث المتعدد | X.1109–X.1100 |
| أمن الشبكة المحلية | X.1119–X.1110 |
| أمن الخدمات المتنقلة | X.1139–X.1120 |
| أمن الويب | X.1149–X.1140 |
| بروتوكولات الأمن | X.1159–X.1150 |
| الأمن بين جهتين نظيرتين | X.1169–X.1160 |
| أمن معرفات الهوية عبر الشبكات | X.1179–X.1170 |
| أمن التلفزيون القائم على بروتوكول الإنترنت | X.1199–X.1180 |
| أمن الفضاء السيبراني | |
| الأمن السيبراني | X.1229–X.1200 |
| مكافحة الرسائل الاقتحامية | X.1249–X.1230 |
| إدارة الهوية | X.1279–X.1250 |
| تطبيقات وخدمات آمنة | |
| اتصالات الطوارئ | X.1309–X.1300 |
| أمن شبكات المحاسيس واسعة الانتشار | X.1339–X.1310 |
| التوصيات ذات الصلة بالبنية التحتية للمفاتيح العمومية | X.1349–X.1340 |
| أمن إنترنت الأشياء (IoT) | X.1369–X.1360 |
| أمن أنظمة النقل الذكية (ITS) | X.1379–X.1370 |
| تبادل معلومات الأمن السيبراني | |
| نظرة عامة عن الأمن السيبراني | X.1519–X.1500 |
| تبادل مواطن الضعف/الحالة | X.1539–X.1520 |
| تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية | X.1549–X.1540 |
| تبادل السياسات | X.1559–X.1550 |
| طلب المعلومات الحدسية والمعلومات الأخرى | X.1569–X.1560 |
| تعرف الهوية والاكتشاف | X.1579–X.1570 |
| التبادل المضمون | X.1589–X.1580 |
| أمن الحوسبة السحابية | |
| نظرة عامة على أمن الحوسبة السحابية | X.1601–X.1600 |
| تصميم أمن الحوسبة السحابية | X.1639–X.1602 |
| أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية | X.1659–X.1640 |
| تنفيذ أمن الحوسبة السحابية | X.1679–X.1660 |
| أمن أشكال أخرى للحوسبة السحابية | X.1699–X.1680 |

*لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.*

**المعيار الدولي ISO/IEC 29151**
**التوصية ITU-T X.1058**

# تكنولوجيا المعلومات – التقنيات الأمنية – مدونة القواعد لحماية المعلومات المحدِّدة لهويّة الشخص


## ملخص

يتزايد عدد المنظمات التي تعالج المعلومات المحدِّدة لهوية الشخص (PII)، وكذلك كمية المعلومات PII التي تتعامل معها هذه المنظمات. وتتزايد في الوقت نفسه التوقّعات الاجتماعية بشأن حماية المعلومات المحددّة لهوية الشخص وأمن البيانات المتعلقة بالأفراد. ويقوم عدد من البلدان بتعزيز قوانينه من أجل معالجة العدد المتزايد من الانتهاكات لبيانات ذات قيمة عالية.

تحدد هذه التوصية أهداف التحكم، والضوابط والمبادئ التوجيهية لتنفيذ الضوابط، لتلبية المتطلبات التي يحددها تقييم المخاطر المتصلة بحماية المعلومات المحددة لهوية الشخص وأثر هذه المخاطر. وتوصّف هذه التوصية بوجه خاص المبادئ التوجيهية القائمة على المعيار ISO/IEC 27002، مع مراعاة متطلبات معالجة المعلومات المحددة لهوية الشخص التي يمكن تطبيقها ضمن سياق بيئة (بيئات) المخاطر الأمنية لمعلومات المنظمة.



## التسلسل التاريخي

| الطبعة | التوصية | تاريخ الموافقة | لجنة الدراسات | معرف الهوية الفريد* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1058 | 2017-03-30 | 17 | 11.1002/1000/13182 |


## مصطلحات أساسية

مدونة قواعد الممارسات، تحكّم، توجيهات بشأن التنفيذ، المعلومات المحدِّدة لهويّة الشخص (PII).

---

* للنفاذ إلى توصية، يرجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

## تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

## ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

## حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

# جدول المحتويات

*الصفحة*

**مقدمة**

يتزايد عدد المنظمات التي تعالج المعلومات المحددة لهوية الشخص (PII)، وكذلك كمية المعلومات PII التي تتعامل معها هذه المنظمات. وتتزايد في الوقت نفسه التوقعات الاجتماعية بشأن حماية المعلومات المحددة لهوية الشخص وأمن البيانات المتعلقة بالأفراد. ويقوم عدد من البلدان بتعزيز قوانينه من أجل معالجة العدد المتزايد من الانتهاكات لبيانات ذات قيمة عالية.

ونظراً لتزايد عدد الانتهاكات للمعلومات المحددة لهوية الشخص (PII)، فسوف تكون المنظمات التي تجمع المعلومات PII أو تعالجها بحاجة متزايدة لتوجيهات بشأن الكيفية التي ينبغي بواسطتها حماية المعلومات PII من أجل تقليل المخاطر المتعلقة بحدوث انتهاكات للخصوصية، وتقليل أثر الانتهاكات على المنظمة المعنية أو الأفراد المعنيين. وتوفر هذه المواصفة هذه الإرشادات.

وتقدم هذه المواصفة توجيهات إلى مراقبي المعلومات PII بشأن مجموعة واسعة من الضوابط المتعلقة بأمن المعلومات وحماية المعلومات PII والمطبقة عادة في منظمات كثيرة مختلفة تتعامل مع حماية المعلومات PII. أما الأجزاء المتبقية من مجموعة المعايير ISO/IEC، المدرجة أدناه، فتقدم توجيهات أو متطلبات بشأن الجوانب الأخرى لمجمل عملية حماية المعلومات PII:

- المعيار ISO/IEC 27001، ويحدد عملية إدارة أمن المعلومات والمتطلبات المقترنة بها، والتي يمكن استخدامها كأساس لحماية المعلومات PII.
- المعيار ISO/IEC 27002، ويقدم مبادئ توجيهية بشأن معايير أمن معلومات المنظمة والممارسات الخاصة بإدارة أمن المعلومات بما في ذلك اختيار الضوابط وتنفيذها وإدارتها مع مراعاة بيئة (بيئات) المخاطر الأمنية لمعلومات المنظمة.
- المعيار ISO/IEC 27009، ويحدد المتطلبات لاستخدام المعيار ISO/IEC 27001 في أي قطاع محدد (مجال، أو مجال تطبيق أو قطاع من قطاعات السوق). ويشرح كيفية إدراج متطلبات إضافية لمتطلبات المعيار ISO/IEC 27001 وكيفية تحسين أي من هذه المتطلبات، وكيفية إدراج ضوابط أو مجموعات من الضوابط إلى جانب الملحق A بالمعيار ISO/IEC 27001.
- المعيار ISO/IEC 27018، ويقدم توجيهات للمنظمات التي تقوم بمعالجة المعلومات PII لدى تقديمها قدرات المعالجة كخدمات سحابية.
- المعيار ISO/IEC 29134 ويقدم مبادئ توجيهية بشأن تحديد المخاطر المتعلقة بالخصوصية وتحليلها وتقييمها، في حين أن المعيار ISO/IEC 27001 يقدم إلى جانب المعيار ISO/IEC 27005 منهجية لتحديد وتحليل وتقييم المخاطر المتعلقة بالخصوصية.

وينبغي أن يتم اختيار الضوابط على أساس المخاطر التي تحددت نتيجة تحليل للمخاطر يرمي إلى وضع نظام شامل ومتسق من الضوابط. وينبغي تكييف الضوابط مع سياق المعالجة الخاصة للمعلومات PII.

وتتضمن هذه المواصفة جزأين: (1) النص الرئيسي المكون من الفقرات 1 إلى 18، و(2) ملحق معياري. وتعكس هذه البنية ممارسة عادية لإعداد مكمّلات للمعيار ISO/IEC 27002 خاصة بقطاع معين.

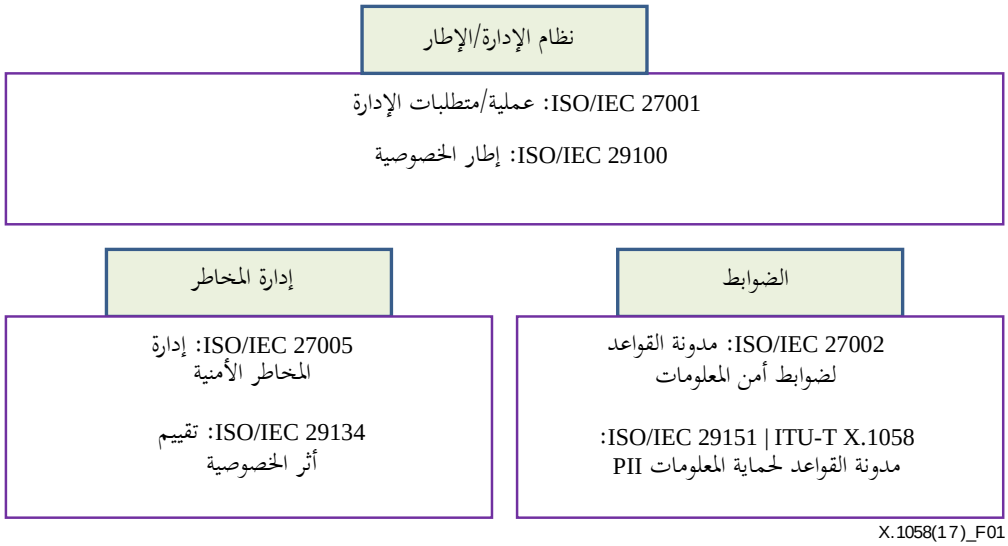
وتعكس بنية النص الرئيسي لهذه المواصفة، بما في ذلك عناوين الفقرات، النص الرئيسي للمعيار ISO/IEC 27002. وتوفر المقدّمة والفقرات من 1 إلى 4 معلومات أساسية عن استخدام هذه المواصفة. أما عناوين الفقرات من 5 إلى 18 فتعكس عناوين المعيار ISO/IEC 27002، ما يدل على أن هذه المواصفة مبنية على التوجيهات الواردة في المعيار ISO/IEC 27002، ولكنها ضوابط جديدة خاصة بحماية المعلومات PII. ولا يحتاج العديد من الضوابط الواردة في المعيار ISO/IEC 27002 إلى توسّع في سياق الضوابط الخاصة بحماية المعلومات PII. ومع ذلك تدعو الحاجة في بعض الحالات إلى توجيهات إضافية بشأن التنفيذ، ويرد ذلك تحت العنوان المناسب (ورقم الفقرة) من المعيار ISO/IEC 27002.

ويتضمن الملحق المعياري مجموعة موسّعة من الضوابط الخاصة بحماية المعلومات PII، تكمل تلك الواردة في المعيار ISO/IEC 27002. وقد قسمت هذه الضوابط الجديدة الخاصة بحماية المعلومات PII، مع التوجيهات المقترنة بها، إلى 12 فئة تناظر المبادئ الأحد عشر الخاصة بالخصوصية والواردة في المعيار ISO/IEC 29100، وهي:

- الموافقة والاختيار؛

- ومشروعية وتوصيف الغرض؛
- وتقييدات عملية الجمع؛
- والتقليل من البيانات إلى الحد الأدنى؛
- والاستخدام وتقييدات الاحتفاظ والكشف؛
- والدقة والجودة؛
- والانفتاح والشفافية والإشعارات؛
- والمشاركة الفردية والنفاذ؛
- والمساءلة؛
- وأمن المعلومات؛
- والامتثال للخصوصية.

ويبين الشكل 1 العلاقة بين هذه المواصفة ومجموعة المعايير ISO/IEC.




**الشكل 1 – العلاقة بين هذه المواصفة ومجموعة المعايير ISO/IEC**

تتضمن هذه المواصفة مبادئ توجيهية تستند إلى المعيار ISO/IEC 27002، وهي تكيف هذه المبادئ حسب الاقتضاء من أجل معالجة متطلبات الحماية التي تنجم عن معالجة المعلومات PII:

أ) في مختلف ميادين المعالجة مثل:

- الخدمات السحابية العامة،
- تطبيقات التواصل الاجتماعي،
- الأجهزة الموصولة بالإنترنت في المنزل،
- البحث والتحليل،
- استهداف المعلومات PII لأغراض إعلانية وغيرها،
- برامج تحليل البيانات الضخمة،
- معالجة العمالة،

- إدارة الأعمال في المبيعات والخدمة (تخطيط موارد المؤسسة، إدارة العلاقات مع الزبائن)؛

ب) في مواقع مختلفة مثل:

- منصة شخصية للمعالجة مقدمة لأحد الأفراد (مثل البطاقات الذكية، الهواتف الذكية وتطبيقاتها، العدادات الذكية، الأجهزة "الملبوسة")،
- داخل شبكات نقل وجمع البيانات (مثلاً حيث تُنشأ البيانات المتعلقة بموقع الهاتف المتنقل من الناحية التشغيلية بواسطة معالجة الشبكة، ما يمكن اعتباره من المعلومات المحدِّدة لهوية الشخص في بعض الولايات القضائية)،
- داخل البنية التحتية للمعالجة الخاصة بالمنظمة،
- منصة معالجة خاصة بطرف ثالث؛

ج) من أجل خصائص الجمع مثل:

- جمع البيانات لمرة واحدة (مثل التسجيل في خدمة)،
- الجمع المستمر للبيانات (مثلاً المراقبة المتكررة لمعلمات الصحة بواسطة أجهزة استشعار مركبة على جسم أحد الأشخاص أو في داخله، جمع متعدد للبيانات باستخدام بطاقات دفع دون اتصال، وأنظمة جمع بيانات العدادات الذكية، وما إلى ذلك).

**ملاحظة** – يمكن للجمع المستمر للبيانات أن يتضمن أو يسفر عن معلومات PII تتعلق بالسلوك أو الموقع أو غير ذلك. وفي هذه الحالات، ينبغي مراعاة استخدام الضوابط المتعلقة بحماية المعلومات PII التي تسمح بإدارة النفاذ والجمع بناء على الموافقة وتسمح لصاحب المعلومات المحددة لهوية الشخص بممارسة سيطرة مناسبة على هذا النفاذ والجمع.

**المعيار الدولي**
**توصية قطاع تقييس الاتصالات**

# تكنولوجيا المعلومات – التقنيات الأمنية – مدونة قواعد الممارسات لحماية المعلومات المحدِّدة لهويّة الشخص

## 1 مجال التطبيق

تحدد هذه التوصية | هذا المعيار الدولي أهداف التحكم، والضوابط والمبادئ التوجيهية لتنفيذ الضوابط، لتلبية المتطلبات التي يحددها تقييم المخاطر المتصلة بحماية المعلومات المحددة لهوية الشخص (PII) وأثر هذه المخاطر.

وتوصّف هذه التوصية | هذا المعيار الدولي بوجه خاص المبادئ التوجيهية القائمة على المعيار ISO/IEC 27002، مع مراعاة متطلبات معالجة المعلومات المحددة لهوية الشخص التي يمكن تطبيقها ضمن سياق بيئة (بيئات) المخاطر الأمنية لمعلومات المنظمة.

وتنطبق هذه التوصية | هذا المعيار الدولي على جميع أنواع وأحجام المنظمات التي تعمل كمراقب للمعلومات PII (كما هو محدد في المعيار (ISO/IEC 29100)، بما في ذلك الشركات العامة والخاصة والكيانات الحكومية والمنظمات التي لا تسعى إلى الربح التي تعالج المعلومات PII.

## 2 المراجع المعيارية

تحتوي التوصيات والمعايير الدولية التالية على أحكام اعتُبرت أحكاماً في هذه التوصية | المعيار الدولي بالإشارة إليها في النص. وكانت الطبعات المشار إليها سارية وقت نشر هذا النص. ولما كانت جميع التوصيات والمعايير تخضع للمراجعة، فإن الأطراف في أي اتفاقات تقوم على أساس هذه التوصية | المعيار الدولي مدعوة للنظر في إمكانية تطبيق آخر طبعة من التوصيات والمعايير التي ترد قائمة بها أدناه. ويحتفظ أعضاء اللجنة الكهرتقنية الدولية والمنظمة الدولية للتوحيد القياسي بسجلات بالمعايير الدولية الصالحة حالياً. ويحتفظ مكتب تقييس الاتصالات في الاتحاد الدولي للاتصالات بقائمة بتوصيات القطاع الصالحة حالياً.

– ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*.
– ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*.

## 3 التعاريف والأسماء المختصرة

### 1.3 التعاريف

لأغراض هذه التوصية | هذا المعيار الدولي، تنطبق المصطلحات والتعاريف الواردة في المعيار ISO/IEC 27000:2016 والمعيار ISO/IEC 29100 والمصطلحات والتعاريف التالية.

*ومنصة التصفح* الخاصة بالمنظمة الدولية للتوحيد القياسي *على الإنترنت*، *وموسوعة Electropedia* الخاصة باللجنة الكهرتقنية الدولية *ومصطلحات وتعاريف* الاتحاد الدولي للاتصالات عبارة عن قواعد بيانات للمصطلحات للاستخدام في التقييس.

**1.1.3 كبير موظفي الخصوصية (CPO)**: مسؤول كبير في الإدارة مكلّف بحماية المعلومات المحددة لهويات الأشخاص في منظمة معينة.

**2.1.3 منع التعرّف (de-identification process)**: عملية لفصل الارتباط بين مجموعة من البيانات المحددة للهوية وأساس هذه البيانات باستعمال تقنيات منع التعرف.

### 2.3 المختصرات

تنطبق المختصرات التالية لأغراض هذه المواصفة:

BCR قواعد عامة مُلزِمة *(Binding Corporate Rule)*

CCTV دارة تلفزيونية مغلقة *(Closed-Circuit Television)*

CPO كبير موظّفي الخصوصية *(Chief Privacy Officer)*

PBD الخصوصية عند التصميم *(Privacy By Design)*

PDA المساعِدات الرقمية الشخصية *(Personal Digital Assistant)*

PET تكنولوجيا تعزيز الخصوصية *(Privacy Enhancing Technology)*

PIA تقييم أثر الخصوصية *(Privacy Impact Assessment)*

PII المعلومات المحدِّدة لهوية الشخص *(Personally Identifiable Information)*

RFID تعرف الهوية بالترددات الراديوية *(Radio Frequency Identification)*

USB الناقل التسلسلي العام *(Universal Serial Bus)*

## 4 نظرة عامة

### 1.4 هدف حماية المعلومات المحدِّدة لهوية الشخص (PII)

توفر هذه المواصفة مجموعة من الضوابط الخاصة بحماية المعلومات المحددة لهوية الشخص (PII). والهدف من حماية المعلومات PII هو تمكين المنظمات من وضع مجموعة من الضوابط في إطار برنامجها الشامل لحماية المعلومات PII. ويمكن استخدام مجموعة الضوابط هذه ضمن إطار للحفاظ على الامتثال للقوانين والأنظمة المتعلقة بالخصوصية وتحسينه، وإدارة المخاطر المتعلقة بالخصوصية وتلبية توقعات أصحاب المعلومات PII أو الهيئات التنظيمية أو المستهلكين، وفقاً لمبادئ الخصوصية الواردة في المعيار ISO/IEC 29100.

### 2.4 متطلبات حماية المعلومات PII

ينبغي أن تحدد المنظمة متطلباتها المتعلقة بحماية المعلومات PII. وتطبق مبادئ الخصوصية الواردة في المعيار ISO/IEC 29100 لتحديد هذه المتطلبات. وهناك ثلاثة مصادر رئيسية لمتطلبات حماية المعلومات PII وهم:

- المتطلبات القانونية والنظامية والتنظيمية والتعاقدية المتعلقة بحماية المعلومات PII بما في ذلك، على سبيل المثال، المتطلبات المتعلقة بالمعلومات PII التي يتعين على المنظمة وشركائها التجاريين والمتعاقدين معها ومقدّمي خدماتها الامتثال لها؛
- تقييم المخاطر (أي المخاطر الأمنية والمخاطر المتعلقة بالخصوصية)، عبر إجراء تقييم للمخاطر، على المنظمة وعلى صاحب المعلومات PII، مع مراعاة الاستراتيجية والأهداف العامة لأعمال المنظمة؛
- سياسات المؤسسة: قد تختار إحدى المنظمات أيضاً على أساس طوعي تجاوز المعايير المستمدة من المتطلبات السابقة.

وينبغي للمنظمات أن تراعي أيضاً المبادئ (أي مبادئ الخصوصية المحددة في المعيار ISO/IEC 29100) والأهداف ومتطلبات العمل المتعلقة بمعالجة المعلومات PII والتي وضعت لدعم عملياتها.

وينبغي أن يتم اختيار الضوابط الخاصة بحماية المعلومات PII (بما في ذلك الضوابط الأمنية) على أساس تقييم المخاطر. وتساعد نتائج تقييم أثر الخصوصية (PIA)، كما هو محدد مثلاً في المعيار ISO/IEC 29134، في توجيه وتحديد الإجراءات والأولويات العلاجية المناسبة لإدارة المخاطر التي تتعرض لها حماية المعلومات PII وتنفيذ الضوابط التي تم اختيارها للحماية من هذه المخاطر.

وقد توفر مواصفات تقييم أثر الخصوصية كما وردت في المعيار ISO/IEC 29134 توجيهات بشأن تقييم مخاطر الخصوصية، بما في ذلك المشورة بشأن تقييم المخاطر، وخطة معالجة المخاطر، وتحمّل المخاطر، واستعراض المخاطر.

### 3.4 الضوابط

يمكن لتقييم مخاطر الخصوصية أن يساعد المنظمات في تحديد المخاطر الخاصة بانتهاك الخصوصية الناتجة عن المعالجة غير المشروعة لصاحب المعلومات PII المشارك في إحدى العمليات المتوخاة أو بنزع حقوقه. وينبغي للمنظمات أن تحدد وتنفذ الضوابط الكفيلة بمعالجة المخاطر التي حددها إجراء تقييم المخاطر. وينبغي بعد ذلك توثيق الضوابط والمعالجات، بصورة مستقلة من الناحية المثالية وفي سجل منفصل للمخاطر. ويمكن لأنماط معينة من معالجة المعلومات PII أن تسمح بضوابط محددة لا تكون الحاجة إليها واضحة إلا عند إجراء تحليل دقيق لإحدى العمليات المتوخاة

### 4.4 اختيار الضوابط

يمكن اختيار الضوابط من هذه المواصفة (الذي يشمل بالإحالة الضوابط الواردة في المعيار ISO/IEC 27002، ما ينشئ مجموعة موحدة من الضوابط المرجعية). ويمكن أيضاً إذا استدعى الأمر اختيار الضوابط من مجموعات أخرى من الضوابط، أو يمكن تصميم ضوابط جديدة تلبي احتياجات محددة حسب الاقتضاء.

ويعتمد اختيار الضوابط على قرارات تنظيمية قائمة على المعايير المتعلقة بخيارات معالجة المخاطر وعلى النهج العام لإدارة المخاطر، والمطبقة على المنظمة، وعلى مستهلكيها وموزّديها عن طريق اتفاقات تعاقدية، كما ينبغي أن يخضع لجميع التشريعات واللوائح الوطنية والدولية المعمول بها.

كما يعتمد اختيار الضوابط وتنفيذها على دور المنظمة في توفير البنى التحتية والخدمات. فقد تكون للكثير من المنظمات المختلفة دور في توفير البنى التحتية أو الخدمات. وفي بعض الظروف، قد تكون الضوابط التي تم اختيارها استثنائية بالنسبة لمنظمة معينة. وفي حالات أخرى، قد يكون هناك مشاركة في دور تنفيذ الضوابط. وينبغي للاتفاقات التعاقدية أن تحدد بوضوح مسؤوليات جميع المنظمات المشاركة في تقديم أو استعمال الخدمات في مجال حماية المعلومات PII.

ويمكن استخدام الضوابط الواردة في هذه المواصفة كمرجع بالنسبة للمنظمات التي تعالج المعلومات PII، وهي معدّة لكي تطبق في جميع المنظمات التي تعمل كمراقب للمعلومات PII. وينبغي للمنظمات التي تعمل كمراقب للمعلومات PII أن تقوم بذلك وفقاً لتعليمات مراقب المعلومات PII. وينبغي أن يكون مراقبو المعلومات PII قادرين على تنفيذ جميع الضوابط الضرورية المدرجة في اتفاق معالجة المعلومات PII طبقاً للغرض من هذه المعالجة ويجوز لمراقبي المعلومات PII الذين يستخدمون خدمات الحوسبة السحابية كوسيلة لمعالجة المعلومات PII أن يستعرضوا المعيار ISO/IEC 27018 من أجل تحديد الضوابط ذات الصلة الواجب تنفيذها.

ويرد في الفقرات من 5 إلى 18 شرح مفصل للضوابط الواردة في هذه المواصفة، إلى جانب توجيهات بشأن التنفيذ. ويمكن تبسيط التنفيذ إذا أخذت متطلبات حماية المعلومات PII في الاعتبار عند تصميم نظام معلومات المنظمة وخدماتها وعملياتها. وهذا الاعتبار هو بمثابة عنصر من عناصر المفهوم الذي يطلق عليه غالباً اسم "الخصوصية عند التصميم (PBD)". ويمكن الاطلاع على المزيد من المعلومات بشأن اختيار الضوابط والخيارات الأخرى المتعلقة بمعالجة المخاطر في المعيار ISO/IEC 29134. وهناك مراجع أخرى ذات صلة مدرجة في البيبليوغرافيا.

### 5.4 وضع المبادئ التوجيهية الخاصة بالمنظمة

يمكن اعتبار هذه المواصفة نقطة انطلاق لوضع المبادئ التوجيهية الخاصة بالمنظمة. ولا تنطبق جميع الضوابط والمبادئ التوجيهية الواردة في هذه التوصية | هذا المعيار الدولي على جميع المنظمات.

وعلاوة على ذلك، قد يكون هناك حاجة إلى ضوابط ومبادئ توجيهية إضافية غير مدرجة في هذه التوصية | هذا المعيار الدولي. وعندما توضع وثائق تتضمن ضوابط ومبادئ توجيهية إضافية، قد يكون من المفيد إدراج إحالات مرجعية إلى فقرات في هذه المواصفة، عند الاقتضاء، لتسهيل تحقّق المدققين والشركاء التجاريين من الامتثال.

### 6.4 اعتبارات بشأن دورة الحياة

للمعلومات المحدِّدة لهوية الشخص (PII) دورة حياة طبيعية، منذ استحداثها أو إنشائها وحتى التخلّص المحتمل منها (مثلاً إتلافها بشكل آمن)، مروراً بجمعها وتخزينها واستعمالها ونقلها. ومع أن قيمة المعلومات PII والمخاطر بشأنها قد تتغير خلال دورة حياتها، إلا أن حمايتها تظل من الأمور الهامة إلى حد ما في جميع المراحل والسياقات التي تتخلل دورة حياتها.

ولأنظمة المعلومات أيضاً دورات حياة يتم في إطارها تصور هذه الأنظمة وتحديد خصائصها وتصميمها وإعدادها واختبارها وتنفيذها واستخدامها وصيانتها وإخراجها من الخدمة والتخلص منها في نهاية المطاف. وينبغي أن تؤخذ حماية المعلومات PII في الاعتبار أيضاً في كل مرحلة من هذه المراحل. ويوفر وضع أنظمة جديدة وإدخال تغييرات على الأنظمة القائمة فرصاً سانحة للمنظمات لتحديث الضوابط الأمنية والضوابط الخاصة بحماية المعلومات PII مع أخذ الأحداث العارضة والمخاطر الحالية والمتوقعة على أمن المعلومات والخصوصية في الاعتبار.

### 7.4 هيكل هذه المواصفة

يتضمن القسم المتبقي من هذه المواصفة جزأين معياريين رئيسيين.

يتضمن الجزء الأول من هذه المواصفة، المؤلف من الفقرات 5 إلى 18، توجيهات إضافية بشأن التنفيذ ومعلومات أخرى عن بعض الضوابط القائمة ذات الصلة الواردة في المعيار ISO/IEC 27002. ويستخدم النسق الخاص بهذا الجزء عناوين الفقرات ذات الصلة في المعيار ISO/IEC 27002 من أجل توفير إحالات مرجعية إلى هذا المعيار الدولي.

ويتضمن الجزء الثاني مجموعة محددة من الضوابط الخاصة بحماية المعلومات PII موصفة في الملحق A. وهو يستخدم النسق ذاته المستخدم في المعيار ISO/IEC 27002 والذي يحدد أهداف الضوابط (نص داخل إطار) يليها واحد أو أكثر من الضوابط التي يمكن تطبيقها. وتنظّم مواصفات الضوابط على النحو التالي:

**المراقبة**

يحدد النص تحت هذا العنوان البيان الخاص بالمراقبة الذي يحقق هدفها.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

يقدم النص تحت هذا العنوان معلومات أكثر تفصيلاً لدعم تنفيذ المراقبة وتحقيق أهدافها. وقد لا تكون التوجيهات الواردة في هذه المواصفة مناسبة تماماً أو كافية في جميع الحالات، وقد لا تلبي متطلبات المراقبة الخاصة بالمنظمة. وبالتالي قد يكون من المناسب استخدام ضوابط بديلة أو إضافية، أو أشكال أخرى من معالجة المخاطر (تجنب المخاطر أو نقلها).

**معلومات أخرى بشأن حماية المعلومات PII**

يقدم النص تحت هذا العنوان المزيد من المعلومات التي قد يتعين أخذها في الاعتبار، من قبيل الاعتبارات القانونية والإحالات المرجعية إلى معايير أخرى.

## 5 السياسات المتعلقة بأمن المعلومات

### 1.5 توجيهات الإدارة بشأن أمن المعلومات

#### 1.1.5 مقدمة

ينطبق الهدف المحدد في الفقرة 1.5 من المعيار ISO/IEC 27002:2013.

### 2.1.5 السياسات الخاصة بأمن المعلومات

تنطبق الفقرة 1.1.5 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي أن تشمل السياسات الخاصة بأمن المعلومات بيانات مناسبة للتدابير الأمنية لحماية المعلومات PII. وترد التفاصيل المتعلقة بحماية المعلومات PII في الفقرة 4.1.18 من المعيار ISO/IEC 27002:2013

وعند وضع سياسة أمن المعلومات وتنفيذها واستعراضها، ينبغي أن تنظر المنظمات في متطلبات حماية الخصوصية الواردة في المعيار ISO/IEC 29100.

وينبغي للمنظمات تحديد عناصر حماية المعلومات PII غير المتعلقة بالأمن باعتبارها سياسة منفصلة بشأن الخصوصية. انظر التوجيهات الواردة في الفقرة 2.A.

### 3.1.5 استعراض السياسات الخاصة بأمن المعلومات

تنطبق الفقرة 2.1.5 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها المحددة في المعيار ISO/IEC 27002.

## 6 تنظيم أمن المعلومات

### 1.6 التنظيم الداخلي

### 1.1.6 مقدمة

ينطبق الهدف المحدد في الفقرة 1.6 من المعيار ISO/IEC 27002.

### 2.1.6 دور أمن المعلومات ومسؤولياته

تنطبق الفقرة 1.1.6 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

من الضروري تعريف الأدوار والمسؤوليات المتعلقة بحماية المعلومات PII بوضوح وتوثيقها بشكل صحيح وتداولها بشكل مناسب. وعلى وجه التحديد:

أ ) ينبغي أن تقع مسؤولية حماية المعلومات PII على عاتق أحد كبار المسؤولين المحددين بشكل واضح داخل المنظمة [يشار إليه أحياناً باسم كبير موظفي الخصوصية (CPO)]؛

ب) ينبغي أن يكلّف شخص محدد أو أشخاص محددون بوضوح، (أي وظيفة حماية المعلومات PII)، بمسؤولية التنسيق مع وظائف أمن المعلومات داخل المنظمة؛

ج) ينبغي أن تتضمن مواصفات الوظائف الخاصة بجميع الأشخاص المشاركين في معالجة المعلومات PII (بما في ذلك المستعملون وموظفو الدعم) شروط مناسبة متعلقة بحماية المعلومات PII.

وينبغي أن تعمل الوظيفة المحددة لحماية المعلومات PII بشكل وثيق مع الوظائف الأخرى الخاصة بمعالجة المعلومات PII، ومع وظيفة أمن المعلومات التي تنفذ متطلبات أمنية تشمل تلك الناجمة عن القوانين الخاصة بحماية المعلومات PII، وكذلك مع الوظيفة القانونية التي تساعد في تفسير القوانين واللوائح والشروط التعاقدية وفي التعامل مع انتهاكات البيانات.

وينبغي للمنظمة أن تدرس الحاجة إلى مجلس أو لجنة عابرة للوظائف مكوّنة من كبار الأعضاء في الوظائف التي تعالج المعلومات PII وأن تنشئ هذا المجلس أو هذه اللجنة. وبما أن حماية المعلومات PII هي وظيفة متعددة التخصصات، ففي وسع هذا المجلس أن يساعد بشكل استباقي في تحديد الفرص المتاحة لإجراء تحسينات، وتحديد المخاطر والمجالات الجديدة لإجراء عمليات تقييم أثر الخصوصية، والتخطيط لاتخاذ إجراءات وقائية وتدابير لكشف الانتهاكات والعمل ضدها، وما إلى ذلك. ويوصى بضرورة أن يجتمع هذا المجلس بصورة دورية وأن يرأسه الشخص المسؤول عن حماية المعلومات PII كما هو محدد في الفقرة ( أ ).

وينبغي لمراقب المعلومات PII أن يطلب من معالج (معالجي) المعلومات PII التابع (التابعين) له تعيين جهة اتصال لكي توجه إليها الأسئلة المتعلقة بمعالجة المعلومات PII بموجب عقد معالجة هذه المعلومات.

وينبغي للأفراد المسؤولين عن وظائف حماية المعلومات رفع التقارير إلى كبير موظفي الخصوصية من أجل ضمان أن يتمتعوا بالمستوى الكافي من السلطة مما يسمح لهم بالاضطلاع بمسؤولياتهم.

### 3.1.6 الفصل بين الواجبات

تنطبق الفقرة 2.1.6 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي أن تكون الواجبات ومجال المسؤوليات في حماية المعلومات PII مستقلة عن تلك الخاصة بأمن المعلومات. ومع التسليم بأهمية أمن المعلومات في حماية المعلومات PII، فمن المهم أن تكون الواجبات ومجال المسؤوليات في الأمن وفي حماية المعلومات PII مستقلة بعضها عن بعض قدر الإمكان. وينبغي تيسير التنسيق والتعاون بين المسؤولين عن أمن المعلومات PII وعن حماية المعلومات PII إذا كان ذلك ضرورياً أو مفيداً لحماية المعلومات PII.

وينبغي للمنظمات أن تعتمد مبدأ الفصل بين الواجبات عند تخصيص حقوق النفاذ لمعالجة المعلومات PII، ولا سيما المعالجة التي تنطوي على درجة عالية من المخاطر.

ينبغي أن يكون النفاذ إلى المعلومات PII التي تجري معالجتها والنفاذ إلى ملفات التسجيل المتعلقة بتلك المعالجة واجبات منفصلة.

وينبغي الفصل بين النفاذ إلى المعلومات المتعلقة بجمع المعلومات PII للإجابة على طلبات أصحاب المعلومات PII وبين جميع أشكال النفاذ الأخرى إلى المعلومات PII. وينبغي أن يقتصر النفاذ على الذين تشمل واجباتهم الإجابة على طلبات أصحاب المعلومات PII.

### 4.1.6 الاتصال بالسلطات

تنطبق الفقرة 3.1.6 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي أن يكون لدى المنظمات، عند الاقتضاء، إجراءات قائمة تحدد متى ينبغي الاتصال بالسلطات (بما في ذلك سلطات حماية البيانات) للإبلاغ مثلاً عن انتهاكات للخصوصية أو عن تفاصيل عملية المعالجة، ومن هي الجهة التي تقوم بذلك.

### 5.1.6 الاتصال بمجموعات الاهتمام الخاص

تنطبق الفقرة 4.1.6 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 6.1.6 أمن المعلومات في إدارة المشاريع

تنطبق الفقرة 5.1.6 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي أن يحثّ الشروع بأي مشروع جديد على إجراء تحليل أولي لتحديد ما إذا كان يتعين إجراء تقييم لأثر الخصوصية أم لا. ويلاحظ أن مصطلح "مشروع" يشمل جميع الأحداث العارضة التي تقوم فيها المنظمة بتنفيذ أو تعديل ما هو جديد أو قائم من تكنولوجيا أو منتج أو خدمة أو برنامج أو نظام معلومات أو عملية أو مشروع.

ويمكن الاطلاع على المزيد من التوجيهات في تقييم أثر الخصوصية الوارد في المعيار ISO/IEC 29134.

## 2.6 الأجهزة المتنقلة والعمل عن بُعد

### 1.2.6 مقدمة

ينطبق الهدف المحدد في الفقرة 2.6 من المعيار ISO/IEC 27002:2013.

### 2.2.6 السياسة المتعلقة بالأجهزة المتنقلة

تنطبق الفقرة 1.2.6 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات المحددة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن تقيّد تماماً النفاذ إلى المعلومات PII من الأجهزة المحمولة والمتنقلة، من قبيل الحواسيب المحمولة والهواتف المتنقلة والأجهزة الموصولة بناقل تسلسلي عام (USB) والمساعدات الرقمية الشخصية (PDA)، التي قد تكون معرضة عموماً لمخاطر تفوق المخاطر التي تتعرض لها الأجهزة غير المحمولة (مثل الحواسيب المكتبية في مرافق المنظمة)، وذلك طبقاً لتقييم المخاطر.

وينبغي للمنظمات أن تقيّد تماماً النفاذ من بُعد إلى المعلومات PII في الحالات التي لا يمكن فيها تجنّب النفاذ عن بُعد، وأن تضمن أن تكون الاتصالات بالنفاذ عن بُعد مجفّرة ورسائلها مستيقنة وسلامتها محمية.

### 3.2.6 العمل عن بُعد

تنطبق الفقرة 2.2.6 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

# 7 أمن الموارد البشرية

## 1.7 قبل التوظيف

### 1.1.7 مقدمة

ينطبق الهدف المحدد في الفقرة 1.7 من المعيار ISO/IEC 27002:2013.

### 2.1.7 الفرز

تنطبق الفقرة 1.1.7 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 3.1.7 شروط وأحكام التوظيف

تنطبق الفقرة 2.1.7 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات المحددة في المعيار ISO/IEC 27002.

## 2.7 أثناء التوظيف

### 1.2.7 مقدمة

ينطبق الهدف المحدد في الفقرة 2.7 من المعيار ISO/IEC 27002:2013.

### 2.2.7 مسؤوليات الإدارة

تنطبق الفقرة 1.2.7 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات المحددة في المعيار ISO/IEC 27002.

### 3.2.7 الوعي والتثقيف والتدريب بشأن أمن المعلومات

تنطبق الفقرة 2.2.7 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات المحددة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي وضع تدابير لتوعية الموظفين ذوي الصلة بالعواقب المحتملة التي تترتب على مراقب المعلومات PII (مثلاً العواقب القانونية، أو خسارة الأعمال التجارية، أو الإضرار بالعلامة التجارية أو بالسمعة) وعلى الموظف (مثلاً العواقب التأديبية) وعلى صاحب المعلومات PII (مثلاً العواقب الجسدية والمادية والعاطفية) من جراء انتهاك الخصوصية أو القواعد والإجراءات الأمنية، لا سيما أولئك الذين يتصدون لمعالجة المعلومات PII.

وكما هو الحال بالنسبة للوعي والتثقيف والتدريب بشأن أمن المعلومات، ينبغي للمنظمات أن توفّر ما هو مناسب من تدريب وتثقيف ووعي فيما يتعلق بحماية المعلومات PII ومعالجتها.

### 4.2.7 عملية التأديب

تنطبق الفقرة 3.2.7 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات المحددة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن تضع سياسة رسمية بشأن التأديب. وينبغي في حالات انتهاكات الخصوصية إبلاغ هذه السياسة بوضوح إلى الأشخاص المتضررين. كما ينبغي أن تنفذ المنظمات هذه السياسة في جميع حالات انتهاكات الخصوصية.

## 3.7 إنهاء التوظيف وتغييره

### 1.3.7 مقدمة

ينطبق الهدف المحدد في الفقرة 3.7 من المعيار ISO/IEC 27002:2013.

### 2.3.7 مسؤوليات إنهاء التوظيف أو تغييره

تنطبق الفقرة 1.3.7 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

# 8 إدارة الأصول

## 1.8 المسؤولية عن الأصول

### 1.1.8 مقدمة

ينطبق الهدف المحدد في الفقرة 1.8 من المعيار ISO/IEC 27002:2013.

### 2.1.8 جرد الأصول

تنطبق الفقرة 1.1.8 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن تضع جرداً بالأصول وأن تحتفظ به وتحدّثه باستخدام المعلومات التي يوفرها مثلاً تقرير تقييم أثر الخصوصية (PIA) إن وجد، على النحو المحدد في المعيار ISO/IEC 29134. وينبغي أن يشمل ذلك جميع أصول المعلومات PII وجميع الأنظمة التي تعالج المعلومات PII.

وعند إعداد عملية الجرد والاحتفاظ به، ينبغي للمنظمات أن تستخلص من عمليات تقييم أثر الخصوصية عناصر المعلومات التالية المتعلقة بأنظمة المعلومات التي تقوم بمعالجة المعلومات PII. والقائمة التالية مقدمة كمثال – وقد يكون هناك إضافة أو طرح لبعض العناصر في القوائم النهائية المطبقة:

أ ) الاسم ومختصر الاسم لكل نظام محدد؛

ب) وأنواع المعلومات PII التي تعالجها هذه الأنظمة؛

ج) وتصنيف (انظر الفقرة 2.2.8) جميع أنواع المعلومات PII، سواء كعناصر معلومات فردية أو عناصر مدمجة في أنظمة المعلومات هذه؛

د ) ومستوى الأثر المحتمل، على صاحب المعلومات PII وعلى المنظمة، لأي انتهاك للمعلومات PII؛

هـ ) والغاية (الغايات) من جمع المعلومات PII؛

و ) وما إذا كانت معالجة المعلومات PII تتم بتعاقد خارجي مع معالج المعلومات PII؛

ز ) وما إذا كانت المعلومات PII قد أرسلت إلى مراقبين آخرين للمعلومات PII، وفي هذه الحالة، إلى أي جهة (أو أي جماعة متلقية)؛

ح) وفترة الاحتفاظ بالمعلومات PII؛

ط) والمنطقة الجغرافية التي جمعت فيها المعلومات PII أو عولجت؛

ي) وما إذا تم نقل المعلومات PII عبر الحدود.

وينبغي للمنظمات أن تقدم إلى الشخص المسؤول عن حماية المعلومات PII تحديثات منتظمة لجردة المعلومات PII دعماً لوضع ضوابط أمنية مناسبة لجميع أنظمة المعلومات الجديدة أو المحدَّثة التي تعالج المعلومات PII.

### 3.1.8 ملكية الأصول

تنطبق الفقرة 2.1.8 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات المحددة في المعيار ISO/IEC 27002.

### 4.1.8 الاستخدام المقبول للأصول

تنطبق الفقرة 3.1.8 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن توفر الحماية للأصول التي تدعم المعلومات PII من النفاذ غير المرخّص، أو التعديل غير المرخّص، أو الإزالة غير المرخّصة، أو الفقدان أو الإتلاف، أو المعالجة الخاطئة وغير المشروعة وما إلى ذلك.

### 5.1.8 ملكية الأصول

تنطبق الفقرة 4.1.8 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات المحددة في المعيار ISO/IEC 27002.

## 2.8 تصنيف المعلومات

### 1.2.8 مقدمة

ينطبق الهدف المحدد في الفقرة 2.8 من المعيار ISO/IEC 27002:2013.

### 2.2.8 تصنيف المعلومات

تنطبق الفقرة 1.2.8 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن تصنّف جميع المعلومات التي تتضمن معلومات PII باستخدام فئة تصنيف سارية (تسمى مجموعة معلومات في المعيار ISO/IEC 27002) أو فئات تصنيف جديدة يتم استحداثها. وينبغي لفئات التصنيف الجديدة أن تشمل، على سبيل الذكر وليس الحصر، فئات عامة من قبيل المعلومات PII الحساسة والمعلومات PII غير الحساسة. وقد يشمل مخطط التصنيف أيضاً فئات أكثر تحديداً من قبيل المعلومات الصحية الشخصية (PHI) والمعلومات المالية الشخصية (PFI). وإذا استحدثت المنظمات فئات تصنيف جديدة، فإنه ينبغي تحديد مستويات الحماية الخاصة بها. وينبغي أن تعتمد الفئات الفعلية المستخدمة على أشياء مثل المتطلبات المحددة في التشريعات واللوائح المتصلة بحماية البيانات، والالتزامات القانونية الأخرى (التعاقدية مثلاً)، وطبيعة المعلومات وحساسيتها، والمخاطر التي تنطوي على ضرر والتي قد تنشأ في حال وقوع انتهاك.

ويمكن لبعض المعلومات PII التي يمكن تصنيفها بأنها غير حساسة في بلد ما أن تعتبر حساسة في مكان آخر، رهناً بالقوانين المعمول بها المتعلقة بحماية البيانات.

وقد يحتاج تصنيف أحد عناصر المعلومات PII إلى إعادة تقييم وتعديل عند اقترانه بنعت واحد أو أكثر من النعوت الإضافية. وينبغي إنفاذ المبادئ التوجيهية والإجراءات المناسبة.

### 3.2.8 توسيم المعلومات

تنطبق الفقرة 2.2.8 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

عندما لا تدرج أي منظمة معلومات PII ضمن فئة من فئات التصنيف، ينبغي أن تتأكد المنظمة من أن الأشخاص الخاضعين لمسؤوليتها على دراية بتعريف المعلومات PII وكيفية تمييز ما إذا كانت أي معلومات تعتبر معلومات PII.

### 4.2.8 التعامل مع الأصول

تنطبق الفقرة 3.2.8 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

إذا سمحت المنظمات للأشخاص الخاضعين لإدارتها بحذف وسم معلومات خاص بفئة التصنيف المتعلقة بالمعلومات PII، ينبغي للمنظمات أن تجعل هؤلاء الشخاص يتعاملون مع جميع المعلومات المحتوية على معلومات PII بوصفها معلومات من فئة التصنيف المخصصة.

## 3.8 معالجة الوسائط

### 1.3.8 مقدمة

ينطبق الهدف المحدد في الفقرة 3.8 من المعيار ISO/IEC 27002:2013.

### 2.3.8 إدارة الوسائط القابلة للنقل

تنطبق الفقرة 1.3.8 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

يجوز لبعض الولايات القضائية أن تطلب وسائط قابلة للنقل تحتوي على المعلومات PII المقرر تجفيرها. وسواء فرضت القوانين ذلك أم لا، يوصى بعملية التجفير للحدّ من مخاطر تسرب المعلومات PII.

وإذا كانت سرية البيانات أو سلامتها تشكل اعتبارات هامة، ينبغي استخدام تقنيات التجفير لحماية المعلومات PII على الوسائط القابلة للنقل. وينبغي إجراء تقييم للمخاطر من أجل تحديد المستوى المطلوب للحماية ما يساعد بدوره في تحديد النمط اللازم لخوارزمية التجفير المقرر استخدامها وقوتها وجودتها.

ويرد في الفقرة 1.10 توجيهات إضافية بشأن استخدام ضوابط التجفير.

### 3.3.8 التخلص من الوسائط

تنطبق الفقرة 2.3.8 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي أن تكون إجراءات التخلص الآمن من الوسائط التي تحتوي على المعلومات PII متناسبة مع حساسية المعلومات ومستوى الأثر الناجم عن المعالجة غير الملائمة لهذه المعلومات. ويجوز لبعض الولايات القضائية أن تفرض معايير بشأن الإجراءات المستخدمة للتخلص من الوسائط التي تحتوي على المعلومات PII أو على أنواع محددة من المعلومات PII (مثل البيانات الصحية، البيانات المالية، وغيرها).

### 4.3.8 نقل الوسائط المادية

تنطبق الفقرة 3.3.8 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

عندما تستخدم الوسائط المادية في نقل المعلومات، ينبغي اتخاذ التدابير اللازمة لتسجيل الوسائط المادية الداخلة والخارجة التي تحتوي على المعلومات PII، بما في ذلك نوع الوسائط المادية وأرقام التعريف (مثل الأرقام التسلسلية أو أرقام وسم الجردات) والمرسل/المستلم المرخّص والتاريخ والوقت وعدد الوسائط المادية وأنماط المعلومات PII التي تحتويها، ولكشف فقدان الوسائط المادية. وينبغي أيضاً توثيق الغرض من النقل ومداه، والشخص المسؤول عن الترخيص بشأنه، والأساس القانوني/التعاقدي للنقل. وينبغي أيضاً مراعاة الإشارة الصريحة إلى مبدأ التقليل من البيانات إلى الحد الأدنى.

# 9 التحكم في النفاذ

## 1.9 متطلبات أعمال التحكم في النفاذ

### 1.1.9 مقدمة

ينطبق الهدف المحدد في الفقرة 1.9 من المعيار ISO/IEC 27002:2013.

### 2.1.9 سياسة التحكم في النفاذ

تنطبق الفقرة 1.1.9 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 3.1.9 النفاذ إلى الشبكات وخدمات الشبكات

تنطبق الفقرة 2.1.9 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

## 2.9 إدارة نفاذ المستعملين

### 1.2.9 مقدمة

ينطبق الهدف المحدد في الفقرة 2.9 من المعيار ISO/IEC 27002:2013.

### 2.2.9 تسجيل وإلغاء تسجيل المستعملين

تنطبق الفقرة 1.2.9 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للإجراءات المتعلقة بتسجيل المستعملين وإلغاء تسجيلهم وإدارة دورة حياتهم أن توفر تدابير لمعالجة تعرض التحكم بنفاذ المستعملين للخطر من قبيل المساس بكلمات المرور أو بالبيانات الأخرى الخاصة بتسجيل المستعملين أو تعرضها للخطر (كأن تكون مثلاً نتيجة إفصاح غير مقصود).

### 3.2.9 تزويد المستعملين بالنفاذ

تنطبق الفقرة 2.2.9 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن تمنح المستعملين الحق المناسب للنفاذ إلى أنظمة المعلومات التي تعالج المعلومات PII وفقاً لمبدأ تقليل البيانات إلى أدنى حد الوارد في المعيار ISO/IEC 29100.

وينبغي للمنظمات أن تقصر النفاذ إلى أنظمة المعلومات التي تعالج المعلومات PII على العدد الأدنى من الأفراد اللازم لتنفيذ الأهداف المحددة لهذه المعالجة وفقاً لمبدأ تقليل البيانات إلى أدنى حد الوارد في المعيار ISO/IEC 29100.

وينبغي للمنظمات أن تعتمد أساليب استيقان محكمة لمعلومات PII خاصة ولمعالجة الخاصة للمعلومات PII (مثلاً البيانات الصحية).

### 4.2.9 إدارة حقوق النفاذ المميز

تنطبق الفقرة 3.2.9 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

تؤدي المعالجة الواسعة النطاق للمعلومات PII (مثلاً، الاستعلام على دفعات، والتعديل على دفعات، والتصدير على دفعات، والحذف على دفعات) إلى زيادة مخاطر وقوع انتهاك واسع النطاق. وينبغي للمنظمات أن تولي عناية خاصة عند تخصيص حقوق النفاذ لهذه العمليات المميزة. ولمنع إساءة استعمال المعلومات PII، ينبغي تخصيص حقوق النفاذ المميز لمعالجة المعلومات PII (لا سيما المعالجة التي تنطوي على درجة عالية من المخاطر) على أساس حصري تماماً. كما ينبغي أن تخصّص بطريقة تساعد على الحد من مخاطر التواطؤ بين شخصين أو أكثر. وينبغي أن يسجل منح هذه الحقوق واستعمالها في ملفات التسجيل ذات الصلة. وينبغي أن تكون جميع الموافقات على النفاذ لفترة محددة. وينبغي أن تستعرض المنظمات هذه الموافقات بصورة منتظمة وحسب الاقتضاء، وأن تجدد وتلغي وتنهي مدة الموافقات حسب الاقتضاء.

**5.2.9 إدارة معلومات الاستيقان السرية من المستعملين**

تنطبق الفقرة 4.2.9 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**6.2.9 استعراض حقوق نفاذ المستعملين**

تنطبق الفقرة 5.2.9 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**7.2.9 إزالة حقوق النفاذ أو تعديلها**

تنطبق الفقرة 6.2.9 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**3.9 مسؤوليات المستعملين**

**1.3.9 مقدمة**

ينطبق الهدف المحدد في الفقرة 3.9 من المعيار ISO/IEC 27002:2013.

**2.3.9 استخدام معلومات الاستيقان السرية**

تنطبق الفقرة 1.3.9 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**4.9 التحكم بالنفاذ إلى الأنظمة والتطبيقات**

**1.4.9 مقدمة**

ينطبق الهدف المحدد في الفقرة 4.9 من المعيار ISO/IEC 27002:2013.

**2.4.9 تقييد النفاذ إلى المعلومات**

تنطبق الفقرة 1.4.9 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

قبل السماح للأشخاص كالمشغّلين والمديرين باستعمال لغات الاستعلام التي تمكن من استرجاع المعلومات PII بشكل مكثّف ومؤتمت من قواعد البيانات التي تحتوي على المعلومات PII، ينبغي أن تستعرض المنظمات الحاجة إلى استخدام هذه اللغات لدى معالجة المعلومات PII.

وإذا كان استخدام لغات الاستعلام متسقاً مع متطلبات الحماية، ينبغي للمنظمات أن تتخذ تدابير تقنية لاستخدام هذه اللغات بالحد الأدنى الضروري لتحقيق الغرض أو الأغراض المحددة.

وقد يعني ذلك، على سبيل المثال، أن القيود على النفاذ تحصر استخدام لغة الاستعلام في بضعة مجالات حساسة ومحددة مسبقاً من السجلات.

وعندما يطلب الأشخاص النفاذ إلى مجالات ليسوا مخولين عادة بالنفاذ إليها (المجال التشغيلي مثلاً)، ينبغي تنفيذ آليات محكمة للموافقة. وينبغي للمنظمات أن تحتفظ بسجل بجميع هذه الموافقات.

### 3.4.9 إجراءات الدخول الآمن

تنطبق الفقرة 2.4.9 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

عندما يتمكن أصحاب المعلومات PII من طلب حسابات من مراقب المعلومات PII، يتعين على المراقب اتخاذ تدابير دخول آمن بالنسبة لهذه الحسابات، وذلك تبعاً لنتائج تحليل المخاطر.

### 4.4.9 نظام إدارة كلمات المرور

تنطبق الفقرة 3.4.9 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 5.4.9 استخدام برامج الانتفاع المميزة

تنطبق الفقرة 4.4.9 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 6.4.9 التحكم في النفاذ إلى شفرة مصدر البرنامج

تنطبق الفقرة 5.4.9 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

## 10 التجفير

### 1.10 ضوابط التجفير

#### 1.1.10 مقدمة

ينطبق الهدف المحدد في الفقرة 1.10 من المعيار ISO/IEC 27002:2013.

#### 2.1.10 السياسة بشأن استخدام ضوابط التجفير

تنطبق الفقرة 1.1.10 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

#### 3.1.10 إدارة المفاتيح

تنطبق الفقرة 2.1.10 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

## 11 الأمن المادي والبيئي

### 1.11 المناطق الآمنة

#### 1.1.11 مقدمة

ينطبق الهدف المحدد في الفقرة 1.11 من المعيار ISO/IEC 27002:2013.

**2.1.11 الحدود الخارجية للأمن المادي**

تنطبق الفقرة 1.1.11 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**3.1.11 ضوابط الدخول المادي**

تنطبق الفقرة 2.1.11 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**4.1.11 تأمين المكاتب والغرف والمرافق**

تنطبق الفقرة 3.1.11 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**5.1.11 الحماية من التهديدات الخارجية والبيئية**

تنطبق الفقرة 4.1.11 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**6.1.11 العمل في المناطق الآمنة**

تنطبق الفقرة 5.1.11 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**7.1.11 مناطق التسليم والتحميل**

تنطبق الفقرة 6.1.11 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**2.11 المعدّات**

**1.2.11 مقدمة**

ينطبق الهدف المحدد في الفقرة 2.11 من المعيار ISO/IEC 27002:2013.

**2.2.11 اختيار أماكن المعدات وحمايتها**

تنطبق الفقرة 1.2.11 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**3.2.11 مرافق الدعم**

تنطبق الفقرة 2.2.11 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**4.2.11 أمن الكابلات**

تنطبق الفقرة 3.2.11 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**5.2.11 صيانة المعدات**

تنطبق الفقرة 4.2.11 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**6.2.11 إزالة الأصول**

تنطبق الفقرة 5.2.11 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**7.2.11 أمن المعدات والأصول خارج المباني**

تنطبق الفقرة 6.2.11 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 8.2.11 التخلص الآمن من المعدات أو إعادة استعمالها

تنطبق الفقرة 7.2.11 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

لأغراض التخلص الآمن أو إعادة الاستعمال، ينبغي أن تتلف المعدات التي تحتوي على وسائط تخزين يمكن أن تحتوي على معلومات PII أو ينبغي إتلاف المعلومات PII أو محوها أو الكتابة فوقها باستخدام تقنيات معتمدة، وفقاً لإجراءات محددة جيداً وموثقة، وذلك لجعل المعلومات PII الأصلية غير قابلة للاسترجاع بدلاً من مجرد استخدام وظيفة المحو أو التنسيق العادية. وبالنسبة للمعدات التي تحتوي على وسائط خزن يمكن أن تحتوي على معلومات PII مجفرة، قد يكون إتلاف مفاتيح فك التجفير أو حاملي المفاتيح (مثل البطاقات الذكية) كافياً.

### 9.2.11 معدات المستعملين غير المراقبة

تنطبق الفقرة 8.2.11 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 10.2.11 سياسة المكتب النظيف والشاشة النظيفة

تنطبق الفقرة 9.2.11 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

## 12 أمن العمليات

### 1.12 الإجراءات والمسؤوليات التشغيلية

### 1.1.12 مقدمة

ينطبق الهدف المحدد في الفقرة 1.12 من المعيار ISO/IEC 27002:2013.

### 2.1.12 توثيق إجراءات التشغيل

تنطبق الفقرة 1.1.12 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 3.1.12 إدارة التغيير

تنطبق الفقرة 2.1.12 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 4.1.12 إدارة القدرات

تنطبق الفقرة 3.1.12 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 5.1.12 الفصل بين بيئات التطوير والاختبار والتشغيل

تنطبق الفقرة 4.1.12 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي أن تكون بيئات التطوير والاختبار والتشغيل منفصلة من الناحية المنطقية، ومن الناحية المادية إذا أمكن. وينبغي تنفيذ ضوابط النفاذ المناسبة لضمان اقتصار النفاذ على الأفراد المخولين بشكل صحيح. وإذا اقتضت شبكات أو أجهزة الاختبار أو التطوير النفاذ إلى شبكة التشغيل، ينبغي تنفيذ ضوابط نفاذ مُحكمة.

وينبغي للمنظمة أن تجري تقييماً لمخاطر استعمال وسائط وأجهزة قابلة للنقل تحتوي على معلومات PII وذات قدرات لاسلكية بغض النظر عن البيئة التي ستستخدم فيها.

وينبغي عدم استخدام المعلومات PII لأغراض التطوير أو الاختبار من دون إخفاء مسبق للهوية إلا إذا سمح القانون بذلك أو بعد الحصول على موافقة صريحة من صاحب المعلومات PII.

### 2.12 الحماية من البرمجيات الضارّة

#### 1.2.12 مقدمة

ينطبق الهدف المحدد في الفقرة 2.12 من المعيار ISO/IEC 27002:2013.

#### 2.2.12 الضوابط ضد البرمجيات الضارة

تنطبق الفقرة 1.2.12 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 3.12 الخزن الاحتياطي

#### 1.3.12 مقدمة

ينطبق الهدف المحدد في الفقرة 3.12 من المعيار ISO/IEC 27002:2013.

#### 2.3.12 الخزن الاحتياطي للمعلومات

تنطبق الفقرة 1.3.12 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي أن تضع أنظمة المعلومات التي تعالج المعلومات PII آليات إضافية أو بديلة على شكل أدوات خزن احتياطية خارج المبنى لحماية المعلومات PII من الضياع وضمان استمرار عمليات معالجة هذه المعلومات وتوفير القدرة على استعادة عمليات معالجة المعلومات PII بعد وقوع حدث معوّق، إذا كان ذلك ضرورياً قطعاً.

**ملاحظة** – تنقضي فترة معينة بين الخزن الاحتياطي وعمليات الاستعادة. فربما لا تعود المعلومات PII التي خزنت بشكل احتياطي محدّثة عند تقييمها من أجل استعادتها. وقد تؤدي العمليات التي تستند إلى معلومات PII متقادمة إلى نتائج غير صحيحة وتطرح مخاطر تتعلق بالخصوصية.

### 4.12 التسجيل والمراقبة

#### 1.4.12 مقدمة

ينطبق الهدف المحدد في الفقرة 4.12 من المعيار ISO/IEC 27002:2013.

#### 2.4.12 تسجيل الأحداث

تنطبق الفقرة 1.4.12 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي، حيثما أمكن، تسجيل المعلومات PII التي تم النفاذ إليها في سجل الأحداث، وماذا جرى لهذه المعلومات (قراءتها مثلاً أو طباعتها أو إضافتها أو تعديلها أو حذفها)، ومتى تم النفاذ إليها والجهة التي قامت به، وخاصة لأنواع معينة من المعلومات PII

(مثل البيانات الصحية). وفي الحالات التي يشارك عدد من مقدمي الخدمات في تقديم خدمة، قد تكون هناك أدوار متنوعة أو مشاركة في تنفيذ هذه التوجيهات.

وينبغي وضع عملية لاستعراض سجل الأحداث وفق نسق دوري محدد وموثق لتحديد المخالفات واقتراح جهود للمعالجة.

وينبغي أن يحدد مراقب المعلومات PII إجراءات تتعلق بإمكانية وكيفية وموعد إتاحة معلومات السجل أو إمكانية استعمالها من المدير الإداري لأغراض من قبيل المراقبة الأمنية وتشخيص العمليات.

### 3.4.12 حماية معلومات السجل

تنطبق الفقرة 2.4.12 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

قد تتضمن معلومات السجل المسجلة لأغراض المراقبة الأمنية وتشخيص العمليات معلومات محددة لهوية الشخص (PII). وينبغي وضع تدابير من قبيل التحكم في النفاذ (انظر الفقرة 3.2.9) لضمان عدم استعمال معلومات السجل إلا للأغراض المقصودة. وينبغي وضع تدابير لضمان سلامة ملفات التسجيل.

### 4.4.12 سجلات المدير الإداري والمشغّل

تنطبق الفقرة 3.4.12 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن تراقب النفاذ المميّز (عن طريق مدراء ومشغلي الأنظمة مثلاً) إلى المعلومات PII ومعالجتها لاحقاً من قبل أولئك الأشخاص. وينبغي أن تشكل هذه المراقبة جزءاً من المراقبة الكلية لأنظمة المعلومات التي تعالج المعلومات PII.

وينبغي أن تحدد المنظمات الأنشطة التي تعتبرها غير طبيعية وأن تنفذ إجراءات مؤتمتة للإبلا غ عن هذا النشاط إلى الأشخاص ذوي الصلة داخل المنظمة.

### 5.4.12 مزامنة الميقاتيات

تنطبق الفقرة 4.4.12 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

## 5.12 التحكم في برامج التشغيل

### 1.5.12 مقدمة

ينطبق الهدف المحدد في الفقرة 5.12 من المعيار ISO/IEC 27002:2013.

### 2.5.12 تركيب البرامج في أنظمة التشغيل

تنطبق الفقرة 1.5.12 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

## 6.12 إدارة مواطن الضعف التقنية

### 1.6.12 مقدمة

ينطبق الهدف المحدد في الفقرة 6.12 من المعيار ISO/IEC 27002:2013.

#### 2.6.12 إدارة مواطن الضعف التقنية

تنطبق الفقرة 1.6.12 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

#### 3.6.12 القيود على تركيب البرمجيات

تنطبق الفقرة 2.6.12 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 7.12 اعتبارات بشأن التدقيق في أنظمة المعلومات

#### 1.7.12 مقدمة

ينطبق الهدف المحدد في الفقرة 7.12 من المعيار ISO/IEC 27002:2013.

#### 2.7.12 ضوابط التدقيق في أنظمة المعلومات

تنطبق الفقرة 1.7.12 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

## 13 أمن الاتصالات

### 1.13 إدارة أمن الشبكات

#### 1.1.13 مقدمة

ينطبق الهدف المحدد في الفقرة 1.13 من المعيار ISO/IEC 27002:2013.

#### 2.1.13 ضوابط الشبكة

تنطبق الفقرة 1.1.13 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

#### 3.1.13 أمن خدمات الشبكة

تنطبق الفقرة 2.1.13 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

#### 4.1.13 الفصل بين الشبكات

تنطبق الفقرة 3.1.13 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 2.13 نقل المعلومات

#### 1.2.13 مقدمة

ينطبق الهدف المحدد في الفقرة 2.13 من المعيار ISO/IEC 27002:2013.

#### 2.2.13 سياسات وإجراءات نقل المعلومات

تنطبق الفقرة 1.2.13 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي وضع تدابير مناسبة لتقليل مخاطر تسرّب المعلومات PII أثناء نقلها. ويمكن حلّ ذلك بتنفيذ التشفير وتدابير أولية أخرى قد تشمل منع التعرّف أو الحجب أو التمويه.

### 3.2.13 الاتفاقات بشأن نقل المعلومات

تنطبق الفقرة 2.2.13 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 4.2.13 الرسائل الإلكترونية

تنطبق الفقرة 3.2.13 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 5.2.13 الاتفاقات بشأن السرية أو عدم الكشف

تنطبق الفقرة 4.2.13 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن تحدد الشروط التي تجري بموجبها معالجة خارجية للمعلومات PII. وينبغي أن تكون هذه الشروط جزءاً من اتفاق مناسب (كالعقد مثلاً أو اتفاق عدم الكشف).

## 14 حيازة الأنظمة وتطويرها وصيانتها

### 1.14 المتطلبات الأمنية لأنظمة المعلومات

#### 1.1.14 مقدمة

ينطبق الهدف المحدد في الفقرة 1.14 من المعيار ISO/IEC 27002:2013.

#### 2.1.14 تحليل وتوصيف متطلبات أمن المعلومات

تنطبق الفقرة 1.1.14 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي إجراء تقييم لأثر الخصوصية عند تطوير أنظمة المعلومات التي تعالج المعلومات PII أو إدخال تعديلات هامة عليها. ويمكن الاطلاع على توجيهات بشأن عمليات تقييم أثر الخصوصية في المعيار ISO/IEC 29134. وينبغي استخدام نتائج تقييم أثر الخصوصية لتحديد الضوابط التي تعالج المخاطر التي تم تحديدها أثناء عملية تقييم أثر الخصوصية.

#### 3.1.14 تأمين خدمات التطبيقات على الشبكات العمومية

تنطبق الفقرة 2.1.14 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

#### 4.1.14 حماية المعاملات في خدمات التطبيقات

تنطبق الفقرة 3.1.14 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 2.14 الأمن في عمليات التطوير والدعم

#### 1.2.14 مقدمة

ينطبق الهدف المحدد في الفقرة 2.14 من المعيار ISO/IEC 27002:2013.

**2.2.14 سياسة التطوير الآمن**

تنطبق الفقرة 1.2.14 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**3.2.14 إجراءات التحكم بتغييرات النظام**

تنطبق الفقرة 2.2.14 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**4.2.14 الاستعراض التقني للتطبيقات بعد إدخال تغييرات على منصة التشغيل**

تنطبق الفقرة 3.2.14 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**5.2.14 القيود على إدخال تغييرات على حزم البرمجيات**

تنطبق الفقرة 4.2.14 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**6.2.14 مبادئ هندسة الأنظمة الآمنة**

تنطبق الفقرة 5.2.14 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**7.2.14 بيئة التطوير الآمن**

تنطبق الفقرة 6.2.14 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**8.2.14 التطوير بتعاقد خارجي**

تنطبق الفقرة 7.2.14 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**9.2.14 اختبار أمن الأنظمة**

تنطبق الفقرة 8.2.14 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

**10.2.14 اختبار قبول الأنظمة**

تنطبق الفقرة 9.2.14 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي أن يشمل اختبار قبول الأنظمة أيضاً اختبار متطلبات حماية الخصوصية.

**3.14 بيانات الاختبار**

**1.3.14 مقدمة**

ينطبق الهدف المحدد في الفقرة 3.14 من المعيار ISO/IEC 27002:2013.

**2.3.14 حماية بيانات الاختبار**

تنطبق الفقرة 1.3.14 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات بشأن تنفيذ حماية المعلومات PII**

ينبغي في العادة عدم استخدام البيانات التشغيلية التي تحتوي على معلومات PII في التطوير أو الاختبار. فقد يؤدي استخدام معلومات PII حقيقية في هذه البيئات إلى زيادة مخاطر انتهاك سرية المعلومات. وينبغي للمنظمات أن تستخدم بدلاً من ذلك بيانات مركبة أو أن تتخذ تدابير "لإخفاء" (مثلاً حجب أو تمويه أو منع تعرّف) أي معلومات PII قيد الاستعمال.

# 15 العلاقات مع المورّدين

## 1.15 أمن المعلومات في العلاقات مع المورّدين

### 1.1.15 مقدمة

ينطبق الهدف المحدد في الفقرة 1.15 من المعيار ISO/IEC 27002:2013.

### 2.1.15 سياسة أمن المعلومات في العلاقات مع المورّدين

تنطبق الفقرة 1.1.15 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

عندما تحتاج منظمة معينة إلى استعمال خدمات معالج للمعلومات PII، ينبغي إجراء تقييم لمعالجي المعلومات PII على أساس الخبرة والثقة والقدرة على تلبية متطلبات حماية المعلومات PII المنصوص عليها في التشريعات واللوائح المعمول بها أو في العقود أو الاتفاقات القانونية الأخرى.

وينبغي أن يكون لدى المنظمة التي تعمل كمراقب للمعلومات PII عقد مكتوب مبرم مع المنظمة التي تقوم بدور معالج للمعلومات PII. وينبغي أن يُسند العقد بوضوح أدوار ومسؤوليات مراقب المعلومات PII ومعالج المعلومات PII وأن يتضمن البنود الملائمة المتعلقة بحماية المعلومات PII لكي يتحمل معالج المعلومات PII مسؤولية المعالجة التي يقوم بها.

وينبغي أن ينص العقد المبرم مع مراقب المعلومات PII على الأمور التالية على الأقل:

- إعلان ملائم بشأن حجم المعالجة وطبيعتها والغرض منها بحسب العقد؛
- واجبات الدعم التي يقوم بها معالج المعلومات PII بشأن منح أصحاب المعلومات PII القدرة على النفاذ إلى المعلومات PII الخاصة بهم واستعراضها ومعالجة الشكاوى التي يطرحها أصحاب المعلومات PII (انظر الفقرة 10.A)؛
- التدابير التنظيمية الأخرى التي يجب اتخاذها لتلبية المتطلبات القانونية أو التنظيمية؛
- تخويل مراقب المعلومات PII إجراء عمليات تدقيق في مقرّ معالج المعلومات PII؛
- متطلبات الإبلاغ في حالات انتهاكات البيانات أو المعالجة غير المرخصة أو الإخفاق في أداء الشروط والأحكام التعاقدية، بما في ذلك تحديد جهات الاتصال لدى الطرفين؛
- طريقة تقديم التعليمات من مراقب المعلومات PII إلى معالج المعلومات PII؛
- التدابير المطبقة عند إنهاء العقد، ولا سيّما فيما يتعلق بالحذف الآمن للمعلومات PII في المقر أو إعادة المعلومات PII والوسائط المادية.

وينبغي لمراقب المعلومات PII أن يضمن عدم قيام معالجي المعلومات PII بأي تعاقد خارجي آخر لأغراض المعالجة (أي استخدام معالجين خارجيين) بدون الموافقة المسبقة لمراقب المعلومات PII. وينبغي لمراقب المعلومات المذكور أن يتقيد بجميع التشريعات واللوائح ذات الصلة فيما يتعلق بذلك.

وينبغي لمراقب المعلومات PII أن يضمن عدم قيام معالجي المعلومات PII بمعالجة هذه المعلومات لأغراض غير تلك المحددة في العقد أو في اتفاق قانوني آخر.

وينبغي لمراقب المعلومات PII أن يضمن قيام معالجي المعلومات PII بالتخلص منها وفقاً لسياسات مراقب المعلومات PII أو لأي توجيه آخر (مثلاً متطلبات تحددها الوكالة).

### 3.1.15 معالجة الأمن في الاتفاقات مع المورّدين

تنطبق الفقرة 2.1.15 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 4.1.15 سلسلة توريد تكنولوجيا المعلومات والاتصالات

تنطبق الفقرة 3.1.15 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

## 2.15 إدارة تقديم خدمات المورّد

### 1.2.15 مقدمة

ينطبق الهدف المحدد في الفقرة 2.15 من المعيار ISO/IEC 27002:2013.

### 2.2.15 مراقبة خدمات المورّد واستعراضها

تنطبق الفقرة 1.2.15 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 3.2.15 إدارة التغييرات التي تدخل على خدمات المورّد

تنطبق الفقرة 2.2.15 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

# 16 إدارة حوادث أمن المعلومات

## 1.16 إدارة حوادث أمن المعلومات وإدخال تحسينات عليها

### 1.1.16 مقدمة

ينطبق الهدف المحدد في الفقرة 1.16 من المعيار ISO/IEC 27002:2013.

### 2.1.16 المسؤوليات والإجراءات

تنطبق الفقرة 1.1.16 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي أن تكون المنظمات قادرة على توفير (ومستعدة لتقديم) استجابة فعالة ومنظمة لحوادث الخصوصية. وينبغي بالتالي أن تضع المنظمات خطّة للاستجابة لحوادث الخصوصية وأن تعمل على تنفيذها.

وينبغي أن تشمل خطة الاستجابة لحوادث الخصوصية ما يلي:

أ ) تعريف حادث الخصوصية ونطاق الاستجابة له؛

ب) إنشاء فريق استجابة لحوادث الخصوصية عابر للوظائف يقوم بإعداد وتنفيذ واختبار واستعراض خطة الاستجابة لحوادث الخصوصية (ينبغي أن تكون الإدارة العليا في المنظمة مسؤولة عن الموافقة على الخطة)؛

ج) وأدوار ومسؤوليات وسلطات محددة بوضوح لجميع أعضاء فريق الاستجابة لحوادث الخصوصية؛

د ) وإجراءات لتوضيح الأسس القانونية للتعاون مع المنظمات الخارجية (الوطنية والدولية) في حالة وقوع حدث عابر للحدود؛

هـ ) وإجراءات لضمان قيام جميع الأشخاص الخاضعين للسياسة الداخلية بشأن الخصوصية (مثلاً الموظفون والمتعاقدون وما إلى ذلك) بإبلاغ موظفي أمن المعلومات والشخص المكلف بحماية المعلومات PII (يشار إليه أحياناً باسم كبير موظفي الخصوصية) فوراً عن أي حادث يتعلق بالخصوصية وفقاً لتوجيهات إدارة الحوادث في المنظمة؛

و ) و(مهام) تقييم أثر الحادث من أجل تحديد طبيعة ومدى أي ضرر محتمل أو فعلي على الأشخاص المتضررين (كالحرج أو الإزعاج أو عدم الإنصاف) أو على المنظمة؛

ز ) وعملية لتحديد التدابير التي يتعين اتخاذها للتخفيف من الضرر المحدد أعلاه والحد من احتمال تكراره؛

ح) وإجراءات لتحديد ما إذا كان إخطار الأشخاص المتضررين والكيانات المعنية الأخرى (الهيئات التنظيمية مثلاً) مطلوباً، وتوقيت هذا الإشعار وشكله، وتوفير هذا الإشعار عند الاقتضاء.

ويجوز للمنظمات أن تختار إدماج خططها بشأن الاستجابة لحوادث الخصوصية مع خططها بشأن الاستجابة للحوادث الأمنية أو إبقائها منفصلة. وينبغي لحادث في أمن المعلومات أن يحثّ مراقب المعلومات PII على إجراء استعراض لمعرفة ما إذا كان قد وقع انتهاك للبيانات يطال المعلومات PII، وذلك كجزء من العملية المتعلقة بإدارة حوادث أمن المعلومات الخاصة به.

وقد لا يحث حادث أمن المعلومات على إجراء هذا الاستعراض. وقد يشمل حادث أمن المعلومات، على سبيل الذكر وليس الحصر، هجمات ترمي إلى حجب الخدمات (pings) وغيرها من الهجمات المبثوثة على جدران الحماية أو المخدّمات الطرفية، وهجمات مسح المنافذ المفتوحة، وهجمات الحرمان من الخدمة، واستشفاف الرزم. ولا يؤدي حادث أمن المعلومات بالضرورة إلى حدوث اختراق للمعلومات PII أو للمعدات أو المرافق التي تعالج هذه المعلومات.

### 3.1.16 الإبلاغ عن حوادث أمن المعلومات

تنطبق الفقرة 2.1.16 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

#### توجيهات التنفيذ بشأن حماية المعلومات PII

عندما تنتهك سرية المعلومات PII، لا يمكن حماية حقوق ومصالح صاحب هذه المعلومات من دون اتخاذ تدابير فورية.

ويجوز للولايات القضائية أن تفرض متطلبات محددة (في التشريعات أو اللوائح مثلاً) تتصل بالإبلاغ أو الإخطار عن حوادث الأمن التي تتعلق بالمعلومات PII (كالمعالجة غير المرخصة، والانتهاك). وعند حصول حادث أمني متعلق بالمعلومات PII، ينبغي إبلاغ السلطات ذات الصلة بأسرع ما يمكن بتفاصيل الحادث، بما في ذلك الاستجابة المقترحة للمنظمات (التي قد يخضع الإفصاح عنها لبعض التقييدات). وقد تشمل هذه السلطات هيئات حماية البيانات ووكالات إنفاذ القانون والأشخاص المتضررين من الحادث.

وإذا حدث انتهاك للخصوصية، ينبغي للمنظمات أن توفر لأصحاب المعلومات PII النفاذ إلى سبل علاجية ملائمة وفعَّالة، من قبيل تصحيح المعلومات أو حذف المعلومات غير الصحيحة.

### 4.1.16 الإبلاغ عن مواطن الضعف الأمنية

تنطبق الفقرة 3.1.16 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 5.1.16 تقييم حوادث أمن المعلومات والبتّ بشأنها

تنطبق الفقرة 4.1.16 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

#### 6.1.16 الاستجابة لحوادث أمن المعلومات

تنطبق الفقرة 5.1.16 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

#### 7.1.16 التعلم من حوادث أمن المعلومات

تنطبق الفقرة 6.1.16 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

#### 8.1.16 جمع الأدلة

تنطبق الفقرة 7.1.16 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

## 17 جوانب أمن المعلومات في إدارة استمرار الأعمال

### 1.17 استمرار أمن المعلومات

#### 1.1.17 مقدمة

ينطبق الهدف المحدد في الفقرة 1.17 من المعيار ISO/IEC 27002:2013.

#### 2.1.17 تخطيط استمرار أمن المعلومات

تنطبق الفقرة 1.1.17 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

#### 3.1.17 تنفيذ استمرار أمن المعلومات

تنطبق الفقرة 2.1.17 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

#### 4.1.17 التحقق من استمرار أمن المعلومات واستعراضه وتقييمه

تنطبق الفقرة 3.1.17 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 2.17 التكرار

#### 1.2.17 مقدمة

ينطبق الهدف المحدد في الفقرة 2.17 من المعيار ISO/IEC 27002:2013.

#### 2.2.17 توافر مرافق معالجة المعلومات

تنطبق الفقرة 1.2.17 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

## 18 الامتثال

### 1.18 الامتثال للمتطلبات القانونية والتعاقدية

#### 1.1.18 مقدمة

ينطبق الهدف المحدد في الفقرة 1.18 من المعيار ISO/IEC 27002:2013.

### 2.1.18 تحديد المتطلبات القانونية والتعاقدية المعمول بها

تنطبق الفقرة 1.1.18 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي أن تحدد المنظمات القوانين واللوائح التي تخضع لها والمتعلقة بحماية المعلومات PII. وفي حال تحديد هذه القوانين واللوائح، ينبغي للمنظمات عندئذ اتخاذ التدابير اللازمة بشأنها. والحالتان التاليتان مثالان على هذه المتطلبات:

أ ) عندما تكون الحماية الإضافية لبعض فئات المعلومات PII (مثل معرّف الهوية الوطني، أو رقم جواز السفر، أو رقم بطاقة الائتمان) مطلوبة، ينبغي استخدام تقنيات التجفير مثل التشفير. وينبغي مراعاة نوع وقوة وجودة خوارزمية التجفير اللازمة. وينبغي أن يتم اختيار خوارزميات التجفير من قوائم الخوارزميات المعتمدة فقط.

ويرد توصيف وسيلة التحكم الأمنية المتعلقة بهذا المتطلب في الفقرة 2.1.10.

ب) قد تفرض الولايات القضائية حداً أدنى من تواتر عمليات الخزن الاحتياطي للبيانات، بما في ذلك المعلومات PII وحداً أدنى من تواتر عمليات استعراض الخزن الاحتياطي وإجراءات الاستعادة.

ويرد توصيف وسيلة التحكم الأمنية المتعلقة بهذا المتطلب في الفقرة 2.3.12.

وينبغي أن تجري المنظمات عمليات تقييم أثر الخصوصية وتنفذ الخطط الناتجة المتعلقة بمعالجة الخصوصية لضمان امتثال الخدمات والبرامج المتعلقة بمعالجة المعلومات PII لمتطلبات حماية الخصوصية. ويمكن الاطلاع على المزيد من التوجيهات في المعيار ISO/IEC 29134.

وينبغي أن تضع المنظمات برامج تدقيق تساعد في التحقق من امتثال معالجة المعلومات PII لمتطلبات حماية الخصوصية ذات الصلة. وينبغي أن يحدد البرنامج تواتر عمليات التدقيق المقرر إجراؤها.

ويجوز أن تجرى عمليات التدقيق بواسطة المنظمة (مثلاً من خلال مكون تدقيق داخلي) أو عن طريق طرف ثالث مستقل.

**معلومات أخرى بشأن حماية المعلومات PII**

في حين أن مراقب المعلومات PII هو المسؤول في النهاية عن ضمان الامتثال في بعض الولايات القضائية، إلا أنه ينبغي للجهات الفاعلة المشاركة في معالجة المعلومات PII أن تتبع نهجاً استباقياً في تحديد متطلبات حماية الخصوصية ذات الصلة الناجمة عن عوامل قانونية أو عوامل أخرى.

ويوفر العقد المبرم بين مراقب المعلومات PII ومعالج المعلومات PII آلية للتأكد من قيام معالج المعلومات PII بدعم الامتثال وإدارته. وينبغي أن يدعو العقد إلى خضوع الامتثال لتدقيق مستقل، مقبول من معالج المعلومات PII، مثلاً عن طريق تنفيذ الضوابط ذات الصلة في هذه المواصفة، والمعيار ISO/IEC 27002، والمعيار ISO/IEC 27018.

### 3.1.18 حقوق الملكية الفكرية

تنطبق الفقرة 2.1.18 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 4.1.18 حماية السجلات

تنطبق الفقرة 3.1.18 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 5.1.18 الخصوصية وحماية المعلومات المحدّدة لهوية الشخص

تنطبق الفقرة 4.1.18 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 6.1.18 تنظيم ضوابط التجفير

تنطبق الفقرة 5.1.18 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

## 2.18 عمليات استعراض أمن المعلومات

### 1.2.18 مقدمة

ينطبق الهدف المحدد في الفقرة 2.18 من المعيار ISO/IEC 27002:2013.

### 2.2.18 الاستعراض المستقل لأمن المعلومات

تنطبق الفقرة 1.2.18 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002. كما تنطبق التوجيهات الإضافية التالية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

إذا كانت عمليات التدقيق التي تجريها فرادى الأطراف المهتمة غير عملية أو قد تزيد المخاطر الأمنية، ينبغي للمنظمات أن توفر للأطراف المهتمة المحتملة، قبل الدخول في تعاقد، أدلة مستقلة تفيد بأن أمن المعلومات منفذ ويعمل وفقاً لسياسات وإجراءات مراقب المعلومات PII. وينبغي عادة أن يشكل التدقيق المستقل ذو الصلة الذي يختاره مراقب المعلومات PII طريقة مقبولة لتلبية مصالح الأطراف المهتمة في استعراض عمليات المعالجة التي يجريها مراقب المعلومات PII طالما توفرت الشفافية الكافية.

### 3.2.18 الامتثال لسياسات الأمن ومعاييره

تنطبق الفقرة 2.2.18 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

### 4.2.18 استعراض الامتثال التقني

تنطبق الفقرة 3.2.18 تحت عنوان "المراقبة" وتوجيهات التنفيذ المقترنة بها وغيرها من المعلومات الواردة في المعيار ISO/IEC 27002.

# الملحق A

# مجموعة ضوابط موسعة لحماية المعلومات المحدِّدة لهوية الشخص

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية | هذا المعيار الدولي)

## 1.A اعتبارات عامة

يقدم هذا الملحق تعاريف لأهداف جديدة وضوابط جديدة وتوجيهات جديدة بشأن التنفيذ تؤلف جميعها مجموعة موسّعة من الضوابط لتلبية المتطلبات المحددة لحماية المعلومات المحدّدة لهوية الشخص (PII).

وترتكز التوجيهات الواردة في هذه المواصفة على التوجيهات الواردة في المعيار ISO 29100:2011 وتفترض أن تلك التوجيهات قد نُفّذت.

وتصف الفقرة 2.A سياسات عامة لتوفير الحماية للمعلومات PII بينما تعبّر الفقرات التالية عن المبادئ المتعلقة بالخصوصية الواردة في المعيار ISO 29100.

## 2.A السياسات العامة لاستخدام المعلومات PII وحمايتها

| |
|---|
| الهدف: توفير التوجيه والدعم لإدارة حماية المعلومات PII وفقاً لمتطلبات الأعمال والقوانين واللوائح ذات الصلة. |

### المراقبة

ينبغي للمنظمات المشاركة في حماية المعلومات PII أن تضع سياسة عامة لاستعمال المعلومات PII وحمايتها.

### توجيهات التنفيذ بشأن حماية المعلومات PII

ينبغي أن تشمل السياسات الخاصة بالخصوصية بيانات مناسبة (في سياسات مستقلة متعلقة بالخصوصية أو كإضافات للسياسات القائمة) تتعلق بدعم الامتثال للتشريعات والشروط التعاقدية والسياسات الداخلية الأخرى المتعلقة بحماية المعلومات PII والالتزام بإدارته.

وقد لا تشمل السياسات المتعلقة بالخصوصية والأمن المواضيع نفسها، وإن كانت وثيقة الارتباط بعضها ببعض. وينبغي أن تتصدى السياسات المتعلقة بالخصوصية والسياسات المتعلقة بأمن المعلومات لمسائل سرية المعلومات وسلامتها وتوافرها، وبالإضافة إلى ذلك ينبغي للسياسات المتعلقة بالخصوصية أن تعالج مواضيع من قبيل الموافقة ونفاذ الأفراد.

ويقدم المعيار ISO/IEC 29100 توجيهات بشأن تنفيذ إطار للخصوصية. وينبغي لسياسة حماية المعلومات PII:

- أن تكون ملائمة لغرض (أغراض) المنظمة؛
- وأن تكون شفّافة فيما يتعلق بجمع المنظمة للمعلومات PII ومعالجتها لها؛
- وأن توفر الإطار لتحديد أهداف حماية المعلومات PII؛
- وأن تحدد قواعد اتخاذ القرارات في مسائل حماية المعلومات PII؛
- وأن تحدد معايير بشأن تحمّل مخاطر الخصوصية (انظر أيضاً الفقرة 1.3.6 من المعيار ISO/IEC 29134)؛
- وأن تتضمن تعهداً بتلبية متطلبات حماية الخصوصية المعمول بها؛
- وأن تتضمن التزاماً بالتحسين المتواصل؛
- وأن تبلّغ إلى الجميع داخل المنظمة؛
- وأن تكون متاحة للأطراف المهتمة، حسب الاقتضاء.

## 3.A الموافقة والخيار

### 1.3.A الموافقة

| |
|---|
| الهدف: جعل أصحاب المعلومات PII مشاركين فاعلين في عملية اتخاذ القرار فيما يتعلق بمعالجة المعلومات PII الخاصة بهم، ما لم تحدد التشريعات واللوائح خلاف ذلك، عبر ممارسة موافقة طوعية مستنيرة وذات مضمون وعن علم. |

**المراقبة**

ينبغي أن توفر المنظمات لأصحاب المعلومات PII الوسائل اللازمة لممارسة موافقة طوعية مستنيرة وذات مضمون وعن علم ومن دون لبس، باستثناء الحالات التي لا يتمكن فيها صاحب المعلومات PII من رفض الموافقة طوعاً أو حين تسمح القوانين النافذة تحديداً بمعالجة المعلومات PII من دون موافقة صاحبها.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تحدد الوسائل العملية الواجب تنفيذها للحصول على موافقة أصحاب المعلومات PII وتحليل الحالات التي لم تعد فيها الوسائل العملية التي تم اختيارها فاعلة وتحديد الحلول البديلة إذا لزم الأمر، وذلك لضمان الحصول على الموافقة قبل بدء أي معالجة؛

ب) وتوفر الوسائل، متى كان ذلك مجدياً وملائماً أو متى كان مطلوباً من الناحية القانونية، لأصحاب المعلومات PII لإعطاء الموافقة لضمان الحصول عليها قبل بدء المعالجة – وتشمل المعالجة جمع المعلومات PII وتخزينها وتعديلها واسترجاعها ومداولتها وعدم الكشف عنها ومنع تعرّفها وإخفاء هويتها ونشرها أو إتاحتها بأي شكل آخر وحذفها أو إتلافها؛

ج) وتحفظ سجل الموافقة عندما يعطى الموافقة وكيل قانوني (مثلاً نيابة عن طفل أو أشخاص معاقين قانونياً)؛

د ) وتبلغ أصحاب المعلومات PII عند الضرورة بجميع حالات نقل المعلومات PII إلى أطراف ثالثة وتوفر الوسائل المناسبة لأصحاب هذه المعلومات لإعطاء موافقتهم على عمليات النقل هذه؛

هـ ) وتحصل، متى كان ذلك مجدياً وملائماً أو متى كان مطلوباً من الناحية القانونية، على موافقة أصحاب المعلومات PII قبل أي عمليات استعمال جديدة أو الكشف عن معلومات PII جرى جمعها سابقاً، وتضمن الحصول على الموافقة قبل بدء أي معالجة أخرى؛

و ) وتتأكد من الحصول على الموافقة بطريقة مستنيرة وشفافة فيما يتعلق بأغراض المعالجة وتضمن أن الحصول عليها هو لغرض محدد؛

ز ) وتنشر الوعي وتحقق الموافقة، على سبيل المثال، من خلال إشعارات عامة محدّثة؛

ح) وتوفر آلية لأصحاب المعلومات PII لتعديل نطاق موافقتهم – وينبغي الاستجابة لأي تعديل في الموافقة في الوقت المناسب وينبغي تعديل المعالجة أو إيقافها وفقاً لإعادة النظر في الموافقة؛

ط) وتضمن تقيّد الموافقة بجميع المتطلبات القانونية المعمول بها، بما في ذلك، عند الاقتضاء، متطلبات الموافقة الصريحة بالنسبة للمعلومات PII الحساسة؛

ي) وتسمح، متى كان ذلك ملائماً، بالموافقة الضمنية، عندما يكون أصحاب المعلومات PII على وعي واضح بالمعالجة ولم يعترضوا عليها، حيث يمكن أن يدل هذا التصرف على موافقة؛

ك) وتبلغ مسبقاً بجميع عمليات المعالجة قبل تنفيذها؛

ل) وتؤكد هوية صاحب المعلومات PII الذي يعطي الموافقة على المعالجة، أو هوية وكيل مرخص لصاحب المعلومات PII – وينبغي أن تبقى المعلومات المطلوبة للتحقّق بالحد الأدنى الذي لا غنى عنه لهذا الغرض، وأن لا يحتفظ بها إلا للفترة الزمنية الضرورية وأن يتم التخلص منها بأمان عندما تنتفي الحاجة إليها.

**معلومات أخرى بشأن حماية المعلومات PII**

رهناً بالتشريعات الوطنية النافذة، ينبغي للمنظمات أن تحصل على الموافقة من خلال اختيار القبول أو القبول الضمني. ومع أن اختيار القبول هو الطريقة المفضلة، إلا أنه ليس مجدياً دائماً. ويتطلب اختيار القبول أن يقوم أصحاب المعلومات PII بعمل إيجابي للسماح للمنظمات بجمع المعلومات PII أو استعمالها. وعند الحصول على الموافقة باستخدام وسائط إلكترونية، ينبغي أن تحدد المنظمة ما إذا كان اختيار القبول ملائماً أو إذا كان هناك حاجة للتثنية على اختيار القبول.

ويمكن أن تفترض المنظمات بآليات اختيار الرفض أن صاحب المعلومات PII قد وافق ضمناً على معالجة المعلومات PII الخاصة به ما لم يقم بعمل إيجابي يفيد بخلاف ذلك.

ويستدل عادة على الموافقة الضمنية من خلال أفعال الشخص أو عدم وجودها، أو من خلال ظروفه الخاصة. ومن الأمثلة على الموافقة الضمنية: عندما يقدم المستهلك عنوان الشحن إلى شركة البيع الإلكتروني بالتجزئة، فتستخدم شركة البيع المعلومات فقط لأغراض تسليم البضائع إلى المستهلك الشاري.

وينبغي للمنظمات أن توفر الوسائل العملية الواجب تنفيذها للحصول على موافقة منفصلة من أصحاب المعلومات PII لدى جمع أرقام التعريف الوطنية (مثلاً رقم الضمان الاجتماعي، رقم تسجيل الإقامة، رقم جواز السفر).

ويجوز للمنظمة مثلاً أن تقدم خيارات مفصلة خاصة بأصحاب المعلومات PII فيما إذا كانوا يرغبون في الاتصال بهم لأي مجموعة منوعة من الأغراض. وفي هذه الحالة، تضع المنظمات آليات للموافقة لضمان امتثال عمليات المنظمة لخيارات أصحاب المعلومات PII قدر المستطاع.

وقد تكون الموافقة إلكترونية أو ورقية رهناً بالمتطلبات التنظيمية النافذة والاعتبارات العملية.

وعندما تنقل المعلومات PII من منظمة أخرى أو إليها، ينبغي للمنظمات أن تضع عملية لتحديث سجلاتها لكي تعكس تحديثات المحتوى وتغيرات الموافقة (مثلاً تعديل، إبطال) التي يقوم بها أصحاب المعلومات PII وتضمن انتقال هذه التحديثات/التغيرات إلى المنظمات التي تتشارك معها في المعلومات PII. وينبغي أن يجمع من صاحب المعلومات PII أدنى قدر من المعلومات اللازمة التي تضمن تحديث السجلات الصحيحة ومشاركتها مع المنظمات الأخرى. وينبغي للمنظمات أن تقوم بصورة دورية باستعراض عملياتها لضمان عدم معالجة معلومات PII غير ضرورية.

### 2.3.A الخيار

| |
|---|
| الهدف: إتاحة الخيار إلى أصحاب المعلومات PII، متى كان ذلك ملائماً ومجدياً، بعدم السماح بمعالجة المعلومات PII الخاصة بهم، أو رفض الموافقة أو سحبها، أو الاعتراض على نمط محدد من المعالجة، وتوضيح الآثار المترتبة على منح الموافقة أو رفضها إلى صاحب المعلومات PII. |

**المراقبة**

ينبغي أن تزود المنظمات أصحاب المعلومات PII بآليات واضحة وبارزة وسهلة الفهم وجلية وميسورة التكلفة لممارسة الخيارات فيما يتعلق بمعالجة المعلومات PII الخاصة بهم ما لم يكن صاحب المعلومات غير قادر على سحب الموافقة بحرية أو حين تسمح القوانين النافذة تحديداً بمعالجة المعلومات PII من دون موافقة صاحب هذه المعلومات.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تضمن أن باستطاعة أصحاب المعلومات PII الذين يمارسون خياراً فيما يتعلق بمعالجة المعلومات PII الخاصة بهم القيام بذلك قبل إجراء أي معالجة؛

ب) ولا تحجب الخدمة عن صاحب المعلومات PII الذي يمتنع عن تقديم معلومات PII لا تتصل بتلك الخدمة؛

ج) وتحدد، عندما تنص على ذلك التشريعات أو اللوائح ذات الصلة، الوسائل العملية التي ستنفّذ لتمكين أصحاب المعلومات PII من ممارسة حقهم في الاعتراض على معالجة المعلومات PII الخاصة بهم. وينبغي إعطاء أصحاب المعلومات PII وسائل عدة يمارسون من خلالها هذا الحق (مثلاً البريد العادي، البريد الإلكتروني، الهاتف)؛

د ) وتقر باستلام إفادة الاعتراض ضمن الأطر الزمنية المحددة في القانون أو كما هو محدد في سياسة المنظمة؛

هـ ) وتحلل الحالات التي لم تعد فيها الوسائل العملية فاعلة، وإذا لزم الأمر وضع حلول احتياطية للسماح لأصحاب المعلومات PII بالاستمرار في ممارسة حقهم في الاعتراض في الوقت المناسب؛

و ) وتضمن أن تكون المعلومات PII مصنفة وموسومة ومخزنة بطريقة تسهّل ممارسة حق الاعتراض وتضمن إمكانية ممارسة أصحاب المعلومات PII لحقهم في الاعتراض في الوقت المناسب وبدون تكلفة؛

ز ) وتؤكد هوية صاحب المعلومات PII الذي يعطي الموافقة على المعالجة، أو هوية وكيل مرخص لصاحب المعلومات PII – وينبغي أن تبقى المعلومات المطلوبة للتحقّق بالحد الأدنى الذي لا غنى عنه لهذا الغرض، وأن لا يحتفظ بها إلا للفترة الزمنية الضرورية وأن يتم التخلص منها بأمان عندما تنتفي الحاجة إليها.

ح) وتضمن، إذا كانت الأسس المشروعة مطلوبة لممارسة حق الاعتراض، أن يقدم أصحاب المعلومات PII الذين يمارسون حقهم في الاعتراض الأسس المشروعة للاعتراض – وينبغي لأي رفض للامتثال للاعتراض أن يبين بالتفصيل الأسباب التي تدفع مراقب المعلومات PII إلى اعتبار هذه الأسس غير مشروعة؛

ط) وتضمن أن تكون جميع المنظمات التي تشاركت معها في المعلومات PII مدركة للاعتراضات التي يقدمها صاحب المعلومات PII وأنها تلتزم بأي اعتراضات صالحة؛

ي) وتمكّن أصحاب المعلومات PII، حيثما أمكن، من الاعتراض على بعض جوانب معالجة المعلومات PII بدلاً من الاضطرار إلى قبول المعالجة أو الاعتراض عليها بمجملها.

**معلومات أخرى بشأن حماية المعلومات PII**

في الكثير من الحالات، ورهناً بالقوانين النافذة، قد لا يكون من الضروري أو العملي توفير آلية لممارسة خيارات عند جمع معلومات متاحة علناً. فعلى سبيل المثال، لن يكون من الضروري توفير آلية لكي يتيح أصحاب المعلومات PII خيارات عند الاستحصال على أسمائهم وعناوينهم من سجل عام أو صحيفة.

## 4.A مشروعية وتوصيف الغرض

### 1.4.A مشروعية الغرض

| |
|---|
| الهدف: ضمان امتثال غرض (أغراض) معالجة المعلومات PII للقوانين النافذة واعتماده على أسس قانونية مسموح بها. |

**المراقبة**

ينبغي للمنظمات أن تنفذ تدابير ملائمة لضمان امتثال المعلومات PII للقوانين النافذة واعتمادها على أسس قانونية مسموح بها.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تحدد ما إذا كان من الممكن إجراء المعالجة المقترحة على أساسٍ مشروع خلاف الموافقة (مثلاً إنفاذ القانون، أو السلامة العامة، أو التزام قانوني، أو مصلحة مشروعة لمراقب المعلومات PII؛

ب) وتحدد ما إذا كانت المعالجة المقترحة تدار على أساسٍ مشروع (مثلاً إنفاذ القانون، أو السلامة العامة، أو التزام قانوني) يمنع صاحب المعلومات PII من ممارسة خياراته فيما يتعلق بمعالجة المعلومات PII؛

**ملاحظة** – عند جمع المعلومات PII أو معالجتها على صعيد دولي، قد تختلف الحاجة للموافقة والطريقة المناسبة للمعالجة باختلاف الأطر القانونية المعمول بها.

ج) وتحدد السلطة القانونية (الأسس) التي تسمح بمعالجة المعلومات PII، سواء بشكل عام أو دعماً لبرنامج محدد أو لنظام للمعلومات؛

د ) وتضع إجراءات تكفل أن المعالجة تتم وفقاً لجميع اللوائح المعمول بها وأن تفسيرها يتم من جانب سلطات مختصة. وينبغي مراعاة السياق العام للمعالجة لدى تحديد مشروعية الغرض منها. ويشمل ذلك طبيعة العلاقة القائمة بين مراقب المعلومات PII وأصحاب المعلومات PII، والتطورات العلمية والتكنولوجية، والتغيرات في المواقف الاجتماعية والثقافية.

وينبغي للمنظمات أن تضع إجراءات تضمن عدم معالجة المعلومات PII بطريقة تنتهك أو يمكن أن تنتهك أي التزامات قانونية، بما في ذلك الأحكام التنظيمية أو القانون العام أو الشروط التعاقدية.

وفي الحالات التي يكون فيها لعمال المنظمة مجلس أو نقابة، قد تتطلب القوانين النافذة التشاور مع هذه الهيئات لدى تحديد مشروعية الغرض في حالة الموظفين.

وينبغي لمسؤولي البرامج أن يتشاوروا مع الشخص المكلّف بحماية المعلومات PII (يشار إليه أحياناً باسم كبير موظفي الخصوصية) أو من يعادله ومع المستشار القانوني فيما يتعلق بسلطة أي برنامج أو نشاط لجمع المعلومات PII. وينبغي أن تكون السلطة التي تجمع المعلومات PII موثّقة.

### 2.4.A توصيف الغرض

| |
|---|
| الهدف: تحديد الأغراض التي تجمع من أجلها المعلومات PII في غضون فترة لا تتجاوز موعد جمع المعلومات PII وحصر الاستعمال اللاحق لتحقيق الأغراض الأصلية. |

**المراقبة**

ينبغي أن تبلّغ المنظمات صاحب المعلومات PII الذي تعتزم أن تجمع المعلومات PII منه بالغرض (الأغراض) التي تجمع لأجلها المعلومات والغرض (الأغراض) التي ستعالج من أجلها. وينبغي أن يتم التبليغ إبّان أو قبل جمع المعلومات PII وقبل معالجتها لأي غرض (أغراض) لم يبلغ به مسبقاً صاحب المعلومات PII.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن تبلّغ صاحب المعلومات PII بالغرض (الأغراض) قبل جمع المعلومات أو استعمالها للمرة الأولى لأغراض جديدة، وأن تستخدم لهذا التحديد لغة تكون واضحة ومكيّفة للظروف على نحو ملائم، وأن تعطي توضيحات كافية بشأن الحاجة إلى معالجة المعلومات PII الحساسة.

وغالباً ما تجيز اللغة القانونية صراحة عمليات جمع واستخدام محددة للمعلومات PII. وعندما تكتب اللغة القانونية بشكل عام وتكون بالتالي خاضعة للتأويل، ينبغي للمنظمات أن تضمن، بالتشاور مع كبير موظفي الخصوصية والمستشار القانوني، وجود علاقة واضحة بين الترخيص العام لجمع المعلومات PII والجمع المحدد لها.

وبمجرد تحديد الأغراض الخاصة، ينبغي وصف الأغراض بوضوح في وثائق الامتثال المتعلقة بالخصوصية أو الاستمارات التي تستخدمها المنظمات لجمع المعلومات PII. إضافة إلى ذلك، ولتجنب عمليات جمع أو استعمال غير مرخصة، ينبغي للموظفين الذين يتعاملون مع المعلومات PII أن يتلقوا تدريباً على سلطات المنظمة المعنية بجمع المعلومات.

وينبغي للمنظمات أن:

أ ) تحدد المعلومات PII المفيدة لكل عملية تجارية؛

ب) وتفصّل المعلومات PII المفيدة لكل عملية بطريقة منطقية؛

ج) وتدير مختلف حقوق النفاذ وفقاً للعمليات التجارية (بما في ذلك إدارة المرتّبات، وإدارة طلبات الإجازات، والتطور الوظيفي) وتنشئ بيئة مخصصة لتكنولوجيا المعلومات في الأنظمة التي تعالج المعلومات PII الأكثر حساسية؛

د ) وتؤكد بانتظام على أن المعلومات PII مفصولة فعلياً وأنه لم تتم إضافة المتلقين والعلاقات البينية إليها.

### 5.A القيود على الجمع

الهدف: تقييد جمع المعلومات PII بحيث تبقى ضمن حدود القوانين النافذة وفي إطار ما هو ضروري حصراً للأغراض المحددة.

**المراقبة**

ينبغي أن تنفذ المنظمات تدابير ملائمة لتقييد جمع أنماط وكمية المعلومات PII بالعناصر الدنيا للأغراض الواردة في الإشعار (انظر 1.9.A) وبحيث تبقى ضمن حدود القوانين واللوائح المعمول بها.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تحصر جمع المعلومات PII بالعناصر الدنيا للأغراض الواردة في الملاحظة (انظر 1.9.A) والتي أعطى صاحب المعلومات PII موافقته بشأنها؛

ب) ولا تجمع المعلومات PII الحساسة إلا إذا كان جمع هذه المعلومات مرخّصاً قانوناً أو تم الحصول على موافقة بشأنه؛

ج) وتقيّد كمية المعلومات التي تجمعها بشكل غير مباشر من صاحب المعلومات PII أو عنه (مثلاً من خلال سجلات الإنترنت، وسجلات النظام).

وينبغي للمنظمات أن تحدد الغرض (الأغراض) من معالجة المعلومات PII، وتحدد المعلومات PII الضرورية لتحقيق هذه الأغراض، وتحدد المعلومات التي ليست بحاجة إلى جمعها وتؤكد أن المعلومات الضرورية فقط هي التي يجري جمعها.

وينبغي للمنظمات أن تنظر بعناية إلى المعلومات PII التي يتعين جمعها لتحقيق غرض معين قبل البدء بعملية الجمع. وينبغي للمنظمات أن لا تجمع المعلومات PII دون تمييز.

وينبغي للمنظمات أن تستعرض بصورة دورية الغرض (الأغراض) التي تجمع من أجلها المعلومات PII لضمان أن تظل هذه المعلومات صالحة. كما ينبغي لها أن تستعرض بصورة دورية المعلومات PII التي تقوم بجمعها للتأكد من أنها ما زالت بالحد الأدنى الضروري لهذ الغرض (لهذه الأغراض).

وينبغي للمنظمات أن لا تجمع المعلومات PII الحساسة، مثل رقم الهوية الوطني، إلا إذا كان جمع هذه المعلومات مرخّصاً قانوناً أو نال موافقة صريحة.

**معلومات أخرى بشأن حماية المعلومات PII**

يجوز لبعض الولايات القضائية أن تحدد فئات معينة من المعلومات PII (مثلاً الأصل العرقي، أو الآراء السياسية، أو المعتقدات الدينية أو غيرها، أو البيانات الشخصية عن الصحة، أو الحياة الجنسية، أو الإدانات القانونية وما إلى ذلك) بأنها حساسة. ويجوز لهذه الولايات القضائية أن تفرض قيوداً أو شروطاً على جمع هذا النوع من المعلومات PII وينبغي للمنظمات أن تأخذ هذه القيود أو الشروط في الاعتبار عند البتّ بشأن نوع المعلومات المقرر جمعها.

### 6.A التقليل من البيانات إلى الحد الأدنى

الهدف: تقليل المعلومات PII التي تتم معالجتها إلى ما هو ضروري للمصالح المشروعة التي يسعى إليها مراقب المعلومات PII وحصر الكشف عن المعلومات PII بأدنى عدد من أصحاب المصلحة في الخصوصية.

**المراقبة**

ينبغي أن تنفذ المنظمات تدابير ملائمة لتقليل المعلومات PII التي تجري معالجتها إلى ما هو ضروري قطعاً للمصالح المشروعة لمراقب المعلومات PII (مثلاً، قد تسعى إحدى المنظمات إلى زيادة أو توسيع عملياتها التجارية بطريقة تزيد بشكل مشروع من كمية المعلومات PII التي تعالجها وتخزنها).

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تضمن اعتماد مبدأ "الحاجة إلى المعرفة"، أي عدم منح النفاذ إلا للمعلومات PII التي تكون ضرورية للقيام بالواجبات الرسمية في إطار الغرض المشروع لمعالجة المعلومات PII؛

ب) وتستخدم أو تمنح كخيارات مبدئية، حيثما أمكن، التفاعلات والمعاملات التي لا تنطوي على تعرّف هوية أصحاب المعلومات PII؛

ج) وتحد من إمكانية الربط مع المعلومات PII المجمّعة؛

د ) وتجري تقييماً أولياً للمعلومات PII التي تحتفظ بها المنظمة وتضع جدولاً زمنياً لاستعراض تلك المعلومات وتتقيد به للتأكد من أن المعلومات PII المحددة في الإشعار هي التي تم جمعها فقط، وأن المعلومات PII لا تزال ضرورية لتحقيق الأغراض التجارية الراهنة؛

هـ ) وتحصر إرسال الوثائق الإلكترونية التي تتضمن معلومات PII بالعدد الأدنى من أصحاب المصلحة الذين يحتاجون إليها في عملهم؛

و ) وتحدد المعلومات PII التي ينبغي إخفاء هويتها أو منع تعرّفها بناء على السياق والشكل الذي تخزن به هذه المعلومات (مثلاً حقول في قاعدة بيانات أو مقتطفات من نصوص) والمخاطر التي تم تحديدها؛

ز ) وتمنع تعرّف البيانات التي تتطلب منع التعرّف هذا بناء على شكل البيانات التي يتعين منع تعرّفها (مثلاً قواعد البيانات وسجلات نصية) والمخاطر التي تم تحديدها؛

ح) حذف المعلومات PII والتخلص منها عندما ينقضي الغرض من معالجتها ما دام لا يوجد أي متطلب قانوني للاحتفاظ بها أو عندما يكون من العملي القيام بذلك؛

ط) وتنظر في إمكانية استخدام تكنولوجيات تعزّز الخصوصية (PET) وفي نوع هذه التكنولوجيات.

وقد تكون المجموعة الدنيا من عناصر المعلومات PII اللازمة لدعم عملية محددة لأعمال المنظمة مجموعة فرعية من معلومات PII التي خُوّلت المنظمة جمعها.

وينبغي أن تصنف المعلومات PII إلى معلومات إلزامية ومعلومات اختيارية للجمع. وينبغي ألا تجمع المنظمات إلا المعلومات الإلزامية المطلوبة لتوفير خدمة وأن تحصل على خيار القبول الملائم من أصحاب المعلومات PII لدى جمع المعلومات الاختيارية. وينبغي ألا تمتنع المنظمات عن تقديم الخدمة إذا امتنع أصحاب المعلومات عن إعطاء المعلومات PII الاختيارية.

وينبغي لكبير موظفي الخصوصية والمستشار القانوني أن يطالبا مسؤولي البرنامج بتبرير المعالجة المقترحة للمعلومات PII للتأكد من أنها تمثل الحد الأدنى الضروري لنظام المعلومات أو النشاط لتحقيق الغرض المرخص قانوناً.

**الملاحظة 1** – إخفاء الهوية، كما هو معرّف في المعيار ISO/IEC 29100، هو عملية يتم بواسطتها تغيير المعلومات PII بشكل نهائي وبطريقة لا يمكن معها التعرف على صاحب المعلومات PII بصورة مباشرة أو غير مباشرة، سواء من مراقب المعلومات PII وحده أو بالتعاون مع أي طرف آخر. وتنطوي هذه العملية بالضرورة على فقدان (نهائي) للمعلومات. وفي بعض الحالات، يمكن تحقيق الهدف المنشود بمجرد حذف جزء من البيانات.

**الملاحظة 2** – من المخطط أن يكون هناك معيار دولي في المستقبل موضوعه وصف تقنيات منع تعرّف بيانات تعزيز الخصوصية، التي يتعين استعمالها لوصف وتصميم تدابير منع التعرّف وفقاً لمبادئ الخصوصية الواردة في المعيار ISO/IEC 29100. وكقاعدة عامة، للاستنتاج بأن عملية منع التعرف تتقيد بالقوانين، ينفذ عدم التعرف مثلاً بواسطة حذف النعوت أو تعميمها، إلى جانب تدابير تنظيمية أو تقنية قوية.

**الملاحظة 3** – عند معالجة المعلومات PII لغرض معين، يتم التقليل من مدى المعلومات PII المعالجة بحيث تخدم الهدف المقصود فقط، دون كشف معلومات عن صاحب المعلومات PII بصورة مفرطة، مثلاً إذا كانت المنطقة الجغرافية للمجيب على مسح استقصائي متعلق بالحركة مطلوبة، يجب النظر في جمع المعالم القريبة فقط بدلاً من العنوان الدقيق.

**الملاحظة 4** – أثناء تحليل بيانات مجهولة الهوية عندما تكون النتائج مجموعة صغيرة من البيانات، يمكن في أغلب الأحيان الكشف عن هوية أصحاب المعلومات PII. وبالتالي يشكل عدم صدور النتيجة ممارسة جيدة عندما يكون عدد السجلات أقل من عدد عتبي – مثلاً 10 سجلات. ويتعين تحديد قيمة العتبة استناداً إلى نمط توزيع البيانات.

وينبغي للمنظمات أن تقلل المخاطر الأمنية وتلك الخاصة بالخصوصية إلى الحد الأدنى وأن تقلل جرد المعلومات PII عند الاقتضاء. وينبغي لها أن تقوم باستعراض أولي واستعراضات لاحقة لما في حوزتها من معلومات PII لكي تضمن، قدر المستطاع عملياً، أن كُدَس البيانات هذه دقيقة ومهمة ومحدّثة وكاملة.

كما ينبغي للمنظمات أن توجه عملها لتقليل ما في حوزتها من معلومات PII إلى الحد الأدنى الضروري للأداء المناسب لغرض موثق من أغراض الأعمال التنظيمية. وينبغي للمنظمات أن تضع وتعمم جدولاً زمنياً للاستعراضات الدورية لكدس بياناتها لاستكمال الاستعراض الأولي.

وبإجراء عمليات تقييم دورية، تتمكن المنظمات من تقليل المخاطر، وتضمن جمع البيانات المحددة في الإشعار فقط، وتضمن أن البيانات المجمعة ما زالت مهمة وضرورية.

## 7.A الاستخدام وتقييدات الاحتفاظ والكشف

### 1.7.A الاستخدام وتقييدات الاحتفاظ والكشف

| |
|---|
| الهدف: تقييد استخدام وكشف المعلومات PII لأغراض محددة وصريحة ومشروعة، وعدم الاحتفاظ بالمعلومات PII لفترة تزيد عن الفترة الضرورية لتحقيق الأغراض المذكورة أو للتقيد بالقوانين النافذة. |

**المراقبة**

ينبغي للمنظمات أن تنفذ تدابير ملائمة لتقييد معالجة المعلومات PII لأغراض مشروعة ومقصودة، وعدم الاحتفاظ بالمعلومات PII لفترة تزيد عن الفترة الضرورية لتحقيق الأغراض المذكورة أو للتقيد بالقوانين النافذة.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تقيد استخدام المعلومات PII والاحتفاظ بها والكشف عنها (بما في ذلك نقلها) بما هو ضروري لتحقيق أغراض محددة وصريحة ومشروعة؛

ب) وتشكّل أنظمة المعلومات الخاصة بها بحيث تسجل تاريخ جمع المعلومات PII أو استحداثها أو تحديثها ومتى يجب حذفها أو أرشفتها وفق برنامج زمني معتمد للاحتفاظ بالسجلات.

**توجيهات التنفيذ بشأن الاستعمال في حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تحجز (أي تؤرشف وتؤمّن وتستثني من المعالجة اللاحقة) أي معلومات PII عند انتهاء مدة الأغراض المذكورة وإذا كان الاحتفاظ بها مطلوباً بموجب القوانين النافذة؛

ب) وتستخدم التقنيات أو الأساليب المناسبة لضمان الحذف الآمن للمعلومات PII أو إتلافها (بما في ذلك السجلات الأصلية والنسخ والسجلات المحفوظة)؛

ج) ولا تستخدم المعلومات PII إلا للأغراض التي تمت الموافقة عليها مع صاحب المعلومات PII أو التي كشف عنها إبّان جمعها أو قبل ذلك، وأن تحصل على الموافقة عند الضرورة قبل أي معالجة لأي غرض جديد؛

د ) وتقيّد نفاذ الأطراف الخارجية لأنظمة المنظمة والمعلومات PII بما هو ضروري قطعاً ومرخص به رسمياً. وإذا كان هذا النفاذ ضرورياً للأعمال بالفعل، ينبغي اتباع إجراءات الموافقة المناسبة؛

هـ ) وتتأكد من أن أنظمة الأطراف الخارجية التي سمح بربطها بأنظمة المنظمة قد نفّذت ضمانات ملائمة قبل السماح لها بالربط؛

و ) وتستعرض بصورة دورية الضمانات التي تنفذها الأطراف الثالثة لضمان الاستمرار بتلبية متطلبات أمن المنظمة – وإذا تبين بنتيجة هذا الاستعراض أن الضمانات غير كافية، ينبغي فك ربط الأطراف الثالثة إلى أن يحين وقتُ تثبت فيه هذه الأطراف أن الضمانات الكافية قد استعيدت؛

ز ) وتنفّذ آلية مناسبة للاستيقان من النفاذ عند النفاذ إلى المعلومات PII من واجهات بعيدة – ويتعين تسجيل سجلات النفاذ إلى المعلومات PII؛

ح) وتقدم إشعاراً للجمهور بالتغييرات الحاصلة في حيازة المعلومات PII التي جمعت أثناء عملية المراقبة الأمنية.

**توجيهات التنفيذ بشأن الاحتفاظ في حماية المعلومات PII**

قد تكون هناك ظروف يؤدي فيه الشرط القانوني للاحتفاظ بالمعلومات PII إلى الاحتفاظ بها لأبعد مما هو مطلوب لأغراض تجارية محددة. وينبغي للمنظمات أن:

أ ) لا تحتفظ بالمعلومات PII إلا للفترة الزمنية المرخص بها لتحقيق الغرض المحدد (الأغراض المحددة) في الإشعار كما ينص عليه القانون وحذف المعلومات PII فوراً عند انتهاء فترة الاحتفاظ؛

ب) وتنفذ، في الحالة التي يطلب فيها الاحتفاظ بالمعلومات PII لمدة أطول مما هو مطلوب لأغراض تجارية محددة، تدابير من قبيل منع التعرّف لحماية المعلومات PII؛

ج) وتحدّد فترات للاحتفاظ بالمعلومات PII تكون محدودة الوقت وملائمة لغرض المعالجة؛

د ) وتثبت أن نظام المعلومات يستطيع كشف انتهاء فترة الاحتفاظ؛

هـ ) وتضمن أن فترات الاحتفاظ المتفق عليها مطبقة وأن التخلص من المعلومات PII يتم وفقاً لفترات الاحتفاظ؛

و ) وتضع وظائف مؤتمتة تحذف المعلومات PII عند انتهاء فترات الاحتفاظ بها – وينبغي أن يحصل الحذف فوراً أو في أقرب موعد عملي ممكن؛

ز ) وتحدد ما الذي ينبغي منع تعرّفه استناداً إلى السياق والشكل الذي خزنت فيه المعلومات (بما في ذلك حقول في قواعد البيانات أو مقتطفات من نصوص) والمخاطر التي تم تحديدها؛

ح) وتمنع تعرف البيانات التي يلزم منع تعرفها استناداً إلى شكل البيانات التي يلزم منع تعرفها (بما في ذلك قواعد البيانات والسجلات النصية) والمخاطر التي تم تحديدها؛

ط) وتختار الأدوات (بما في ذلك الحذف الجزئي والتظليل وتظليل المفاتيح والمؤشر) التي تحتاج إليها لحماية المعلومات PII إذا تعذر منع تعرّف تلك البيانات.

**توجيهات التنفيذ بشأن عدم الكشف في حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) لا تكشف المعلومات PII لأطراف خارجية من دون علم صاحب البيانات وموافقته المسبقة إلا إذا كان هذا الكشف مسموحاً وفقاً للتشريعات ذات الصلة – وقد لا تُطلب معرفة وموافقة صاحب المعلومات PII إذا كان الكشف لأطراف داخلية (الموظفين مثلاً) يقتضي معرفتها بها؛

ب) وتوفر آلية محكمة للحماية عند نقل المعلومات PII، بما في ذلك تجفير البيانات وحماية سلامتها.

وينبغي التخلص من المعلومات PII الخاصة بالموظف (أي حذفها بشكل آمن أو أرشفتها) وفقاً للتشريعات واللوائح المعمول بها، وكذلك وفقاً لسياسات التخلص في المنظمة، وموافقة الموظف عند الاقتضاء.

### 2.7.A المحو الآمن للملفات المؤقتة

| |
|---|
| الهدف: توفير تدابير تقنية للملفات المؤقتة الواجب حذفها خلال الفترة المحددة. |

**المراقبة**

ينبغي التخلص من الملفات والوثائق المؤقتة التي قد تحتوي على معلومات PII خلال فترة محددة وموثقة.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

قد تنشئ أنظمة المعلومات في سياق عملها العادي ملفات مؤقتة تحتوي على معلومات PII. ومع أن هذه الملفات تكون خاصة بالأنظمة والتطبيقات، لكنها قد تحتوي على منظومة ملفات ذات قدرة تراجعية وعلى ملفات مؤقتة مرتبطة بتحديث قواعد البيانات وعمل برمجيات التطبيقات الأخرى. ولا يوجد عادة حاجة إلى الملفات المؤقتة بعد إكمال مهمة معالجة المعلومات المتصلة بها، إلا أنه قد تحدث ظروف لا تحذف فيها هذه الملفات بصورة أوتوماتية. كما أن المدة التي تبقى فيها هذه الملفات قيد الاستعمال ليست دائماً محددة ولكن ينبغي لإجراء "جمع المخلفات" أن يحدد الملفات المؤقتة ذات الصلة والفترة التي مضت على عدم استعمالها.

وينبغي لأنظمة المعلومات التي تعالج المعلومات PII أن تجري تدقيقاً دورياً لضمان حذف الملفات المؤقتة التي تجاوزت أعمارها فترة محددة.

### 3.7.A الإبلاغ عن كشف المعلومات PII

| |
|---|
| الهدف: ضمان أن يقوم معالج المعلومات PII بإبلاغ مراقب المعلومات PII بأي طلب ملزم قانوناً للكشف عن المعلومات PII. |

**المراقبة**

ينبغي أن يقضي العقد المبرم بين مراقب المعلومات PII ومعالج المعلومات PII بأن يقوم المعالج بإبلاغ المراقب، وفقاً للإجراءات والفترات الزمنية المتفق بشأنها في العقد، بأي طلب ملزم قانوناً للكشف عن المعلومات PII بواسطة سلطة إنفاذ القانون أو أي سلطة أخرى، إلا إذا حظر القانون هذا الكشف.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن تنفذ تدابير (مثلاً الالتزامات التعاقدية) لضمان أن:

أ ) يتشاور معالجو المعلومات PII مع مراقب المعلومات PII ذي الصلة قبل قبول أي طلبات ملزمة قانوناً للكشف عن المعلومات PII، إلا إذا حظر القانون ذلك؛

ب) وأن يقبل معالجو المعلومات PII طلبات متفق عليها بالعقد لكشف المعلومات PII، على النحو الذي يأذن به مراقب المعلومات PII، إلا إذا حظر القانون ذلك.

### 4.7.A تسجيل عمليات الكشف عن المعلومات PII

| |
|---|
| الهدف: ضمان تسجيل عمليات الكشف عن المعلومات PII إلى أطراف ثالثة. |

**المراقبة**

ينبغي أن تسجّل عمليات الكشف عن المعلومات PII إلى أطراف ثالثة، بما في ذلك المعلومات PII التي تم كشفها، وإلى أي جهة، وفي أي وقت ولأي غرض.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

يمكن أن تكشف المعلومات PII خلال السير العادي للعمليات. وينبغي تسجيل عمليات الكشف هذه. كما ينبغي تسجيل أي عمليات كشف إضافية إلى أطراف ثالثة، من قبيل العمليات التي تنجم عن التحقيقات القانونية أو عمليات التدقيق الخارجية. وينبغي أن تتضمن السجلات مصدر الكشف ومصدر السلطة التي يتم كشف المعلومات إليها.

### 5.7.A الكشف عن معالجين للمعلومات PII بعقد خارجي

الهدف: ضمان أن يكشف معالجو المعلومات PII لمراقب المعلومات PII عن استخدامهم لأي متعاقدين خارجيين.

**المراقبة**

ينبغي أن يكشف معالج المعلومات PII لمراقب المعلومات PII عن المتعاقدين الخارجيين الذين يستخدمهم لمعالجة المعلومات PII قبل أي استخدام لهم.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي أن يُحدَّد في العقد المبرم بين معالج المعلومات PII ومراقب المعلومات PII الأحكام المتعلقة باستخدام متعاقدين خارجيين لمعالجة المعلومات PII. وينبغي أن يحدِّد العقد عدم تكليف متعاقدين خارجيين بالعمل إلا بترخيص مسبق من مراقب المعلومات PII. وينبغي لمعالج المعلومات PII أن يبلغ مراقب المعلومات PII في الوقت المناسب بأي تغييرات مزمعة في هذا الخصوص لكي يتمكن مراقب المعلومات PII من الاعتراض على هذه التغييرات أو إنهاء الموافقة.

وينبغي أن تشمل المعلومات التي يتم الكشف عنها ما يفيد باستخدام تعاقد خارجي وأسماء المتعاقدين الخارجيين المعنيين، ولكن من دون تفاصيل خاصة بالأعمال. كما ينبغي أن تشمل المعلومات التي يتم الكشف عنها البلدان التي يستطيع المتعاقدون الخارجيون معالجة البيانات فيها والوسائل التي يلزمون بها للوفاء بتعهدات معالج المعلومات PII أو بما يتجاوزها.

وفي الحالة التي يتبين فيها أن الكشف العلني عن المعلومات المتعلقة بالمتعاقدين الخارجيين يؤدي إلى زيادة المخاطر الأمنية بما يتجاوز الحدود المقبولة، ينبغي أن يتم الكشف بموجب اتفاق عدم الكشف أو بناءً على طلب مراقب المعلومات PII. وينبغي أن يكون مراقب المعلومات PII على علم بأن المعلومات بشأن المتعاقدين الخارجيين الجاري استعمالها متاحة.

### 8.A الدقة والجودة

الهدف: ضمان أن تكون المعلومات PII المعالجة دقيقة وكاملة ومحدّثة وذات صلة بالغاية من استعمالها.

**المراقبة**

ينبغي للمنظمات أن تنفذ تدابير ملائمة لضمان أن تكون المعلومات PII المجمّعة من صاحب المعلومات PII، بطريقة مباشرة أو غير مباشرة، بالجودة المناسبة.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

يقصد بتحقيق جودة البيانات أن المعلومات PII التي تجري معالجتها دقيقة بالدقة الوافية، وكاملة، ومحدّثة، وكافية وذات صلة بالغاية من استعمالها.

وينبغي للمنظمات أن:

أ ) تضع إجراءات لجمع المعلومات PII تسهم في ضمان الدقة والجودة؛

ب) وتجمع المعلومات PII بطريقة تجعل أي تعديل فيها قابلاً للكشف بعد تركها المصدر المعتمد؛

ج) وتؤكد قدر المستطاع عملياً لدى جمع المعلومات PII أو استحداثها دقة المعلومات PII وأهميتها واكتمالها وتوقيتها المناسب؛

د ) وتضمن موثوقية المعلومات PII التي تجمع من مصدر غير صاحب المعلومات PII قبل معالجتها؛

هـ ) وتتحقق، باستعمال الوسائل المناسبة، من صلاحية وصحة طلبات التصحيح التي يتقدم بها صاحب المعلومات PII، حيثما يكون من الملائم القيام بذلك؛

و ) وتدقّق بصورة دورية في أي معلومات PII غير دقيقة أو متقادمة تستخدم في برامجها أو أنظمتها، وتعمل على تصحيحها عند الضرورة؛

ز ) وتحدد مبادئ توجيهية تضمن وتعظّم دقة المعلومات المنشورة واكتمالها وكفايتها وأهميتها. وينبغي للمنظمات أن تتخذ خطوات معقولة لتأكيد دقة المعلومات PII. وقد تشمل هذه الخطوات، على سبيل المثال، تنقيح العناوين أثناء جمعها أو إدخالها في أنظمة المعلومات والتأكد من صلاحيتها باستخدام واجهات مؤتمتة لبرمجة تطبيقات البحث والتدقيق من العناوين (API).

وعندما تكون المعلومات PII ذات طبيعة حساسة بشكل كاف (مثلاً عند استعمالها في التأكيد على المدخول السنوي لدافع الضرائب بالنسبة لربح متكرر)، ينبغي للمنظمات أن تضمّن أنظمة المعلومات الخاصة بها آليات معينة وتحدد إجراءات مقابلة تتعلق بوتيرة تحديث المعلومات وبالطريقة التي يتم بها هذا التحديث.

وللتقليل قدر المستطاع من مدى عدم دقة البيانات، ينبغي أن يقوم صاحب المعلومات PII بإدخال المعلومات PII مباشرة في نظام المعلومات دون الحاجة إلى شخص آخر لتدوينها. ولكن في الحالة التي لا يمكن فيها تفادي تدوين المعلومات PII، ينبغي للمنظمات أن تنظر في تمكين صاحب المعلومات PII من إقرار صلاحية المعلومات PII المدوّنة. ومن شأن ذلك أن يسهم في تصحيح الأخطاء قبل وقوع أي ضرر ناجم عن معالجة معلومات PII غير دقيقة.

**معلومات أخرى بشأن حماية المعلومات PII**

قد تستند أنواع التدابير المتخذة لحماية جودة البيانات إلى طبيعة المعلومات PII وسياقها، وكيفية استخدامها، وطريقة الحصول عليها. وينبغي أن تكون التدابير المتخذة لإثبات صحة المعلومات PII الحساسة أشمل من تلك المستخدمة لإثبات صحة المعلومات PII الأقل حساسية. وقد يكون اتخاذ خطوات إضافية ضرورياً لإثبات صحة المعلومات PII المأخوذة من مصادر خلاف أصحاب المعلومات PII أو من ممثلين مرخص لهم لأصحاب المعلومات PII.

## 9.A الانفتاح والشفافية والإشعارات

### 1.9.A إشعار الخصوصية

| |
|---|
| الهدف: التأكد من أن إشعارات الخصوصية تتضمن المستوى المناسب من التفاصيل، وأنها مكتوبة بلغة بسيطة وسهلة الفهم. |

**المراقبة**

ينبغي للمنظمات أن تنفذ تدابير ملائمة لتزويد أصحاب المعلومات PII بالإشعارات المناسبة لأغراض معالجة المعلومات PII.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تقدّم لأصحاب المعلومات PII إشعاراً نافذاً بشأن:

1) أنشطتها التي تؤثر على الخصوصية بما في ذلك، على سبيل الذكر وليس الحصر، جمعها للمعلومات PII وتقاسمها وحمايتها والتخلص الآمن منها؛

2) والسلطة التي تجمع المعلومات PII؛

3) والخيارات، إن وجدت، المتاحة لأصحاب المعلومات PII فيما يتعلق بكيفية استعمالات المنظمة للمعلومات PII ونتائج ممارسة أو عدم ممارسة هذه الخيارات؛

4) والقدرة على الاعتراض على المعالجة؛

ب) وتوفر آليات الإشعار والموافقة المصمّمة خصيصاً لتلبية الاحتياجات التشغيلية؛

ج) وتراجع إشعاراتها لتبيان التغيرات في الممارسة أو السياسة التي تؤثر على المعلومات PII أو التغيرات في أنشطتها التي تؤثر على الخصوصية، قبل حدوث التغيير أو في أقرب وقت ممكن عملياً بعده؛

د ) وتضمن أن يكون الإشعار كاملاً ومناسباً للجمهور المستهدف استناداً إلى طبيعة المعلومات PII، والوسائل العملية التي تم اختيارها لتقديم الإشعار، وطبيعة العلاقة بين مراقب المعلومات PII وصاحب المعلومات PII؛

هـ ) وتقدم المعلومات بطريقة واضحة يمكن أن يفهمها شخص غير مطلع على تكنولوجيات المعلومات أو الإنترنت أو المصطلحات القانونية؛

و ) وتضمن تقديم التبليغ قبل جمع المعلومات PII أو أثناءه؛

ز ) وتتأكد من عدم جمع المعلومات PII قبل تقديم إشعار بذلك؛

ح) وتحدّد حلولاً بديلة إذا لم تعد الوسائل العملية فاعلة؛

ط) وتوفر، إذا أمكن، وسيلة تبين بواسطتها أن التبليغ قد تمّ؛

ي) وتنشر، عندما يُقدّم إشعار الخصوصية بوسائل مادية، هذه المعلومات على لافتة ينبغي أن يراها أصحاب المعلومات PII، أو تطلب توقيع إشعار أو وثيقة؛

ك) وتوفر سياسة لتقديم الوسم والعلامة اللازمة لاطلاع أصحاب المعلومات PII عن استخدام التكنولوجيا ذات الصلة [أي نظام التلفزيون مغلق الدارة (CCTV)، الشبكة WiFi، تعرف الهوية بواسطة التردد الراديوي (RFID)].

وينبغي قدر المستطاع أن يكون الإشعار معروضاً بشكل بارز في نقطة جمع المعلومات (مثلاً على الموقع الشبكي للمنظمة أو في موقع مادي) دون أن يكون صاحب المعلومات PII مضطراً لطلبه تحديداً.

### 2.9.A الانفتاح والشفافية

| |
|---|
| الهدف: تزويد أصحاب المعلومات PII بمعلومات واضحة ويسهل الوصول إليها عن سياسات مراقب المعلومات PII وإجراءاته وممارساته فيما يتعلق بالتعامل مع المعلومات PII. |

**المراقبة**

ينبغي للمنظمات أن تنفذ تدابير ملائمة لتزويد أصحاب المعلومات PII بالمعلومات الملائمة عن سياساتها وإجراءاتها وممارساتها في معالجة المعلومات PII فيما يتعلق بالتعامل مع المعلومات PII.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تزود أصحاب المعلومات PII بمعلومات واضحة ويسهل الوصول إليها عن سياسات مراقب المعلومات PII وإجراءاته وممارساته فيما يتعلق بالتعامل مع المعلومات PII؛

ب) وتفصح عن الخيارات والوسائل التي يقدمها مراقب المعلومات PII لأصحاب هذه المعلومات فيما يتعلق بالغرض من تقييد معالجة معلوماتهم والنفاذ إليها وتصحيحها وإزالتها؛

بالإضافة إلى ذلك، ينبغي للمنظمات أن تصف:

أ ) المعلومات PII التي تجمعها المنظمة للأغراض التي تجمع تلك المعلومات من أجلها؛

ب) كيفية استعمال المعلومات PII داخل المنظمة؛

ج) ما إذا كانت المنظمة تتبادل المعلومات PII مع كيانات خارجية، وفئات تلك الكيانات، وأغراض هذا التبادل؛

د ) ما إذا كان لأصحاب المعلومات PII القدرة على الموافقة على استعمالات محددة للمعلومات PII أو تبادلها وكيفية ممارسة هذه الموافقة؛

هـ ) طول المدة التي يتم خلالها الاحتفاظ بالمعلومات PII؛

و ) ما إذا كانت المنظمة تبيع المعلومات PII أو تحيل البيانات إلى منظمات تحليل البيانات لمعالجتها والتفاصيل التي تسري على مخاطر المعلومات PII؛

ز ) كيفية حصول أصحاب المعلومات PII على النفاذ إلى هذه المعلومات بغية إجراء تعديل عليها أو تصحيحها حسب الاقتضاء؛

ح) المعلومات المناسبة عن كيفية حماية المعلومات PII؛

ط) ضمان أن يكون لصاحب المعلومات PII القدرة على النفاذ إلى المعلومات عن أنشطته المتعلقة بالخصوصية والقدرة على التواصل مع كبير موظفي الخصوصية؛

ي) توفير المعلومات المتعلقة بانتهاكات الخصوصية التي نجمت أو يمكن أن تنجم عن انتهاك خصوصية طالبي المعلومات PII إلى جانب الأفعال المصاحبة التي قد يقوم بها طالب المعلومات للتخفيف من حدة المخاطر الإضافية الناجمة عن الانتهاك.

وينبغي للمنظمات أن تستخدم أيضاً آليات مختلفة لاطلاع الجمهور على الممارسات التي تعتمدها بشأن بالخصوصية بما في ذلك، على سبيل الذكر وليس الحصر، تقارير تقييم أثر الخصوصية وتقارير بشأن الخصوصية وصفحات الإنترنت المتاحة للجمهور وتوزيع البريد الإلكتروني والمدونات والمنشورات الدورية (مثل النشرات الإخبارية الفصلية). وينبغي للمنظمات أيضاً أن توفر عناوين البريد الإلكتروني أو خطوط هاتف التي تمكّن الجمهور من إبداء التعليقات أو توجيه الأسئلة إلى المكاتب المعنية بالخصوصية فيما يتعلق بالممارسات بشأنها.

## 10.A مشاركة ونفاذ أصحاب المعلومات PII

### 1.10.A نفاذ أصحاب المعلومات PII

| |
|---|
| الهدف: إعطاء أصحاب المعلومات PII القدرة على النفاذ إلى المعلومات PII الخاصة بهم واستعراضها والتحقق من دقتها واكتمالها. |

**المراقبة**

ينبغي للمنظمات أن تنفذ تدابير ملائمة لتزويد أصحاب المعلومات PII بالقدرة على النفاذ إلى المعلومات PII الخاصة بهم والتمكن من تصويبها أو حذفها.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تحدد الوسائل العملية التي سوف يجري تنفيذها للسماح لأصحاب المعلومات PII بممارسة حقهم في النفاذ (حيثما تسمح بذلك التشريعات النافذة). وينبغي أن يكون الأشخاص قادرين على ممارسة حقهم في الوقت المناسب، وبشكل واضح وميسور المنال لصاحب المعلومات PII وشبيه بالوسيلة المستخدمة في جمع المعلومات PII بالأساس (مثلاً، بالبريد العادي أو بالبريد الإلكتروني)؛

ب) وتحلّل الحالات التي لا تعود فيها الوسيلة العملية التي تم اختيارها فاعلة وتضع حلولاً احتياطية عند الضرورة؛

ج) وتوفر لأصحاب المعلومات PII القدرة على النفاذ إلى المعلومات PII الخاصة بهم بشكلها المحفوظ في المنظمة من أجل تقييم دقتها وطلب إجراء تصحيحات عند الضرورة؛

د ) وتقدم الردود، قدر الإمكان، بشكل مكافئ للشكل الذي قدم فيه الطلب (مثلاً إذا قدّم الطلب بالبريد العادي ينبغي أن تعطى الإجابة بالبريد العادي)؛

هـ ) وتنشر القواعد واللوائح التي تنظم كيف يمكن لأصحاب المعلومات PII أن يطلبوا النفاذ إلى السجلات المحفوظة في النظام؛

و ) وتسمح لأصحاب المعلومات PII بالتحقق من دقة واكتمال المعلومات PII بصورة مباشرة أو غير مباشرة وإدخال تعديلات عليها أو تصحيحها أو إزالتها حسبما يكون مناسباً وممكناً في السياق المحدد؛

ز ) وتحدد إجراءات لتمكين أصحاب المعلومات PII من ممارسة حقوقهم بطريقة بسيطة وسريعة وتتسم بالكفاءة، ولا يترتب عليها تأخير غير مبرر (مثلاً ينبغي أن تقدم الردود وفقاً للتشريعات أو اللوائح المعمول بها أو كما هو محدد في سياسة المنظمة) أو كلفة غير مبررة؛

ح) وتحدد عملية لاطلاع أصحاب المعلومات PII الذين يقدمون طلبات بشأن حالة طلبهم والمعالجة اللازمة (مثلاً بالبريد العادي أو الإلكتروني مع الإشارة إلى استلام الطلب والتاريخ الذي يمكن استلام الرد فيه) – وفي حالة المحفوظات، قد يكون هناك بعض المجال فيما يتعلق بتاريخ الإجابة إذا أطلع مراقبُ المعلومات PII صاحبَ المعلومات PII الذي قدّم الطلب على المدة الزمنية اللازمة لمعالجة الطلب وقدم له مهلة معقولة للإجابة؛

ط) وتضمن، في حدود ما يسمح به القانون، إمكانية ممارسة حقّ النفاذ بصورة دائمة؛

ي) وتتأكد من عدم تقييم المعلومات PII إلا من الشخص الذي تتعلق به المعلومات أو من وكيل مأذون له لذلك الشخص – وقد يقتضي ذلك أن يعرّف الأشخاص الذين يطلبون النفاذ عن أنفسهم وأن يتم الاستيقان منهم بطريقة مرضية – وقد تكون متطلبات هذا التعرّف والاستيقان محددة في التشريعات أو اللوائح المعمول بها؛

ك) وتحدد، في الحالة التي يطلب فيها تعرّف مقدمي الطلبات والاستيقان منهم، وما لم تنص التشريعات أو اللوائح على خلاف ذلك، الشكل المناسب للتعرّف والاستيقان – وينبغي للمنظمات أن لا تطلب إلا الحد الأدنى من المعلومات الضروري لضمان التعرّف الصحيح – وينبغي أن تكون هذه المعلومات مؤمنة وأن لا يتم الاحتفاظ بها إلا للفترة الضرورية من الوقت؛

ل) وتكفل عدم إرسال المعلومات PII إلا لصاحب المعلومات وأنها أرسلت بطريقة آمنة؛

م ) وتضمن إمكانية تقديم جميع المعلومات التي قد يطلبها صاحب المعلومات PII مع الاستمرار بحماية المعلومات PII الخاصة بأصحاب معلومات آخرين؛

ن) وتتواصل بواسطة إشعارات تتعلق بالخصوصية إذا كانت تعتزم جباية رسوم على النفاذ، كما قد تسمح به القوانين في بعض الولايات القضائية؛

س) وتطلب من أي معالج للمعلومات PII أن يدعم مراقب المعلومات PII في تسهيل ممارسة أصحاب المعلومات PII لحقوقهم في النفاذ إلى بياناتهم أو تصحيحها أو حذفها.

يمنح النفاذ أصحاب المعلومات PII القدرة على استعراض المعلومات PII الخاصة بهم والمحفوظة في أنظمة وسجلات المنظمة. ويشمل النفاذ إلى البيانات في الوقت المناسب وبشكل مبسط ورخيص الثمن. وقد تختلف عمليات المنظمة المتعلقة بإتاحة النفاذ إلى السجلات باختلاف الموارد أو المتطلبات القانونية أو عوامل أخرى.

### 2.10.A المشاركة وسبل الانتصاف

| |
|---|
| الهدف: تزويد معالجي المعلومات PII والأطراف الثالثة التي كُشفت إليها البيانات الشخصية بأي تعديل أو تصحيح أو إزالة لهذه المعلومات. |

**المراقبة**

ينبغي للمنظمات أن تنفذ تدابير ملائمة لتزويد أصحاب المعلومات PII بالقدرة على تصحيح أو تعديل أو حذف المعلومات PII التي تحتفظ بها المنظمات، ما لم تحظر ذلك التشريعات أو اللوائح ذات الصلة. كما ينبغي للمنظمات أن تضع آلية تبلّغ بها معالجي المعلومات بالتصحيحات أو التعديلات أو عمليات الحذف، وقدر المستطاع الأطراف الثالثة التي كشفت إليها المعلومات PII.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تضمن بأن يتمكن صاحب المعلومات PII دوماً من ممارسة حقه في التصحيح؛

ب) وتحلل الحالات التي لا تعود فيها الوسيلة العملية التي تم اختيارها فاعلة وتحدد حلولاً احتياطية عند الضرورة؛

ج) وتضمن أن باستطاعة أصحاب المعلومات PII ممارسة حقهم في التصحيح ضمن الحدود التي تسمح بها التشريعات أو اللوائح ذات الصلة؛

د ) وتضمن دقّة التصحيحات المطلوبة؛

هـ ) وتكفل حصول أصحاب المعلومات PII الذين يقدمون الطلبات على تأكيد باستلام الطلبات؛

و ) وتضمن إطلاع الأطراف الثالثة التي ربما أرسلت إليها المعلومات PII على التصحيحات التي أجريت؛

ز ) وتقدم لأصحاب المعلومات PII إمكانية النفاذ فقط إلى المعلومات PII التي يتعين تصحيحها أو حذفها أو تعديلها.

### 3.10.A إدارة الشكاوى

| |
|---|
| الهدف: وضع إجراءات فعالة لمعالجة وإنصاف الشكاوى الداخلية التي يقدمها أصحاب المعلومات PII. |

**المراقبة**

ينبغي للمنظمات أن تنفذ تدابير ملائمة لمعالجة الشكاوى الواردة من أصحاب المعلومات PII بكفاءة.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن تضع عملية لإدارة الشكاوى وتحتفظ بجهة اتصال لتلقي شكاوى أصحاب المعلومات PII أو الاهتمام بشواغلهم والرد على أسئلتهم بشأن الممارسات المتعلقة بالخصوصية في المنظمة.

وينبغي للمنظمات أن توفر آليات لتقديم الشكاوى تكون بمتناول أصحاب المعلومات PII بسهولة، وتتضمن جميع المعلومات الضرورية لتقديم الشكاوى (بما في ذلك معلومات الاتصال بكبير موظفي الخصوصية أو أي موظف آخر معين لتلقي الشكاوى) وتكون سهلة الاستعمال.

وينبغي لعمليات إدارة الشكاوى في المنظمة أن تشمل آليات للتتبّع تكفل استعراض جميع الشكاوى الواردة ومعالجتها بصورة ملائمة وفي الوقت المناسب. كما ينبغي أن تشمل عملية إدارة الشكاوى إجراءات تصحيحية يفعّلها مقدم الشكوى.

**معلومات أخرى بشأن حماية المعلومات PII**

يمكن للشكاوى والشواغل والأسئلة التي يقدمها أصحاب المعلومات PII أن تكون بمثابة مصدر قيّم لمساهمات خارجية تحسّن في نهاية المطاف نماذج التشغيل واستعمالات التكنولوجيا وممارسات معالجة البيانات والضمانات المتعلقة بالخصوصية والأمن.

## 11.A المساءلة

### 1.11.A الإدارة

| |
|---|
| الهدف: إقامة إدارة تتسم بالكفاءة في معالجة المعلومات PII. |

**المراقبة**

ينبغي للمنظمات أن تنفذ تدابير ملائمة لإقامة إدارة تتسم بالكفاءة فيما يتعلق بمعالجة المعلومات PII.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تعيّن شخصاً تقع على عاتقه مسؤولية إقامة إدارة على مستوى المنظمة ككل وتنفيذها والحفاظ عليها ووضع برنامج للخصوصية لضمان الامتثال لجميع القوانين واللوائح النافذة فيما يتعلق بمعالجة المعلومات PII بواسطة البرامج وأنظمة المعلومات – ويمكن أن يطلق على الشخص المعيّن اسم كبير موظفي الخصوصية – وكخيار بديل، يمكن أن يتولى المسؤولية عضو مخصص في مجلس الإدارة يدعمه موظف مخصص يمكن التعاقد معه من الخارج؛

ب) وتضمن أن تتوفر لدى الشخص المعيّن الخبرة الضرورية للإشراف على معالجة المعلومات PII؛

ج) وتضمن أن يشارك الشخص المعيّن في جميع القضايا المتصلة بحماية المعلومات PII وأن يكون بوسعه رفع تقارير إلى الإدارة العليا مباشرة في الوقت المناسب؛

د ) وتزود الشخص المعيّن بالموظفين والأماكن والمعدّات والموارد الأخرى اللازمة لتنفيذ مهامه؛

هـ ) وتضع عملية لمراقبة القوانين والسياسة المتعلقة بالخصوصية فيما يتعلق بالتغيرات التي تؤثر على برنامج حماية المعلومات PII؛

و ) وتضع وتنشر وتنفذ سياسات وإجراءات تشغيلية خاصة بحماية المعلومات PII تنظم هذه الحماية والضوابط الأمنية المتعلقة بالبرامج أو أنظمة المعلومات أو التكنولوجيات المعنية بالمعلومات PII؛

ز ) وتحدّث الخطط والسياسات والإجراءات المتعلقة بحماية المعلومات PII بصورة دورية؛

ح) وتراقب بصورة دورية أداء المنظمة في حماية المعلومات PII. وينبغي أن يقوم ممثل عن الإدارة العليا أو عضو في مجلس الإدارة بتنظيم ذلك مع إحاطة كاملة بجوانب معينة من قبيل القياسات الكمية والمخاطر والانتهاكات – ومع أن هناك ضرورة لهذا الاستعراض بحد ذاته، إلا أنه ينبغي أن يتم بصورة دورية دون حاجة إلى دوافع.

### 2.11.A تقييم الآثار ذات الصلة بالخصوصية

| |
|---|
| الهدف: وضع عملية لتقييم الآثار ذات الصلة بالخصوصية وإجراء تقييم للمخاطر ذات الصلة بالخصوصية عند الضرورة. |

**المراقبة**

إذا كانت إحدى المنظمات تعمل على معالجة المعلومات PII، ينبغي للمنظمات أن تحدد العمليات الضرورية لإجراء تقييم للمخاطر ذات الصلة بالخصوصية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

يجري تقييم المخاطر ذات الصلة بالخصوصية عادة من جانب منظمة تأخذ على عاتقها القيام به جدياً وتعامل أصحاب المعلومات PII بطريقة مناسبة. وفي بعض الولايات القضائية، قد يكون تقييم المخاطر ذات الصلة بالخصوصية ضرورياً لتلبية المتطلبات القانونية والتنظيمية. ويمكن استخدام المعيار ISO/IEC 29134 للاسترشاد به في تقييم المخاطر ذات الصلة بالخصوصية.

وينبغي للمنظمات أن تأخذ الأصول والتهديدات ومواطن الضعف والضمانات في الاعتبار عند إجراء تقييم المخاطر ذات الصلة بالخصوصية. وينبغي للمنظمات أن توثّق:

أ ) نتائج تقييم المخاطر ذات الصلة بالخصوصية بما في ذلك، على سبيل الذكر وليس الحصر، المعلومات PII التي تمت معالجتها؛

ب) والمخاطر ذات الصلة بالخصوصية التي تم تحديدها؛

ج) وتدابير التخفيف المقترحة.

### 3.11.A المتطلبات الخاصة بالمتعاقدين ومعالجي المعلومات PII بشأن الخصوصية

الهدف: التأكد، من خلال وسائل تعاقدية أو وسائل أخرى مثل السياسات الداخلية الإلزامية، من أن الأطراف الثالثة المتلقية توفر على الأقل مستويات مكافئة من حماية المعلومات PII.

**المراقبة**

ينبغي للمنظمات أن تنفذ تدابير ملائمة للتأكد من أن المتعاقدين ومعالجي المعلومات PII قد نفذوا مستويات وافية من حماية المعلومات PII.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) توثّق في اتفاق مستوى الخدمة المتطلبات الخاصة بحماية المعلومات PII والتي يتعين على معالجي المعلومات PII تلبيتها؛

ب) وتراقب تنفيذ المتعاقدين لتلك المتطلبات وتدقّق فيه؛

ج) وتحدّد أدوار ومسؤوليات المتعاقدين ومعالجي المعلومات PII في حماية المعلومات PII؛

د ) وتحدّد في العقد موضوع الخدمة الواجب تقديمها وإطارها الزمني، ونطاق معالجة المعلومات PII من قبل المعالج والطريقة التي تتم بها والغرض منها وكذلك أنواع المعلومات PII التي تمت معالجتها؛

ه ) وتحدّد الشروط التي ينبغي بموجبها لمعالج المعلومات PII أن يعيد المعلومات PII أو يتخلص منها بأمان عند انتهاء الخدمة أو انتهاء أي اتفاق حاكم أو غير ذلك بناء على طلب مراقب المعلومات PII؛

و ) وتدرج بنداً بشأن السرية يكون ملزماً لمقدّم الخدمة وأيّ من موظفيه الذين تتوفر لديهم إمكانية النفاذ إلى المعلومات PII؛

ز ) وتتأكد من أن مقدم الخدمة لا يبلّغ المعلومات PII إلى أطراف ثالثة حتى لأغراض الحفظ ما لم يكن ذلك مسموحاً بالعقد بشكل محدد؛

ح) وتوضح مسؤوليات مقدم الخدمة فيما يتعلق بإبلاغ مراقب المعلومات PII في حالة حدوث انتهاك للبيانات يؤثر على المعلومات PII؛

ط) وتحدّد بواسطة عقد أنه يتعين على مقدم الخدمة إبلاغ مراقب المعلومات PII بالتغييرات ذات الصلة المتعلقة بالخدمة من قبيل تنفيذ وظائف إضافية؛

ي) وتوثّق السياسات والإجراءات والممارسات المتصلة بحماية المعلومات PII وترسلها إلى الآخرين بشأنها عند الاقتضاء.

وينبغي للمنظمات أن تتشاور مع المستشار القانوني وكبير موظفي الخصوصية والمسؤولين المتعاقدين بشأن القوانين أو التوجيهات أو السياسات أو اللوائح التي قد تؤثر على تنفيذ هذا العقد.

**ملاحظة** – ينبغي أيضاً تطبيق التوجيهات الإضافية بشأن التنفيذ الواردة في الفقرة 2.1.15.

**معلومات أخرى بشأن حماية المعلومات PII**

يمكن أن يشمل المتعاقدون ومعالجو المعلومات PII، على سبيل الذكر وليس الحصر، مكاتب الخدمات ومقدّمي المعلومات ومعالجي المعلومات والمنظمات الأخرى التي توفر وضع أنظمة المعلومات وخدمات تكنولوجيا المعلومات وغيرها من التطبيقات الخارجية المصدر.

### 4.11.A مراقبة الخصوصية والتدقيق فيها

الهدف: مراقبة وتدقيق ضوابط حماية المعلومات PII وفعالية السياسة الداخلية بشأن حماية المعلومات PII.

**المراقبة**

ينبغي للمنظمات أن تنفذ، بصورة دورية، تدابير ملائمة لمراقبة وتدقيق ضوابط الخصوصية وفعالية السياسة الداخلية بشأن الخصوصية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تراقب وتدقق، بصورة دورية، عمليات معالجة المعلومات PII، لا سيّما تلك التي تنطوي على معلومات PII حساسة، لضمان امتثالها للقوانين واللوائح النافذة والشروط التعاقدية؛

ب) وتراقب وتدقق، بصورة دورية، ضوابط وسياسات حماية المعلومات PII لضمان امتثالها للقوانين واللوائح النافذة والشروط التعاقدية؛

ج) وتتأكد من أن عمليات التدقيق تقوم بها أطراف مؤهلة ومستقلة (داخلية أو خارجية عن المنظمة)؛

د ) وأن يكون لديها، في الحالة التي تستخدم فيها الأطراف المدقّقة موارد داخلية، بصورة دورية طرف خارجي لإجراء التدقيق من أجل تقييم مستقل.

### 5.11.A الوعي والتدريب لحماية المعلومات PII

الهدف: توفير التدريب والوعي المناسبين لموظفي مراقب المعلومات PII الذين سينفذون إلى المعلومات PII فيما يتعلق بحماية المعلومات PII.

**المراقبة**

ينبغي للمنظمات أن تنفذ تدابير ملائمة لتوفير تدريب ملائم لموظفي مراقب المعلومات PII.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تنفذ استراتيجية شاملة للتدريب والوعي ترمي إلى التأكد من فهم الموظفين لمسؤولياتها وإجراءاتها المتعلقة بحماية المعلومات PII؛

ب) وتستحدث آليات لإبقاء الموظفين المسؤولين عن حماية المعلومات PII مطّلعين على أحدث التطورات في البيئة التنظيمية والتعاقدية والتكنولوجية التي قد تؤثر على تعهّد المنظمة بشأن الخصوصية؛

ج) وتقدّم بانتظام (سنوياً مثلاً) أو حسب الطلب تدريباً موجهاً وعلى أساس الأدوار على حماية المعلومات PII – ويكتسي ذلك أهمية خاصة في الأنشطة التي لا تعالج إلا المعلومات PII بوتيرة منخفضة؛

د ) وتضمن أن يشهد الموظفون بصورة دورية (يدوياً أو إلكترونياً) على تحملهم المسؤوليات المتعلقة بمتطلبات حماية المعلومات PII.

### 6.11.A الإبلاغ عن حماية المعلومات PII

| |
|---|
| الهدف: وضع تقارير بشأن حماية المعلومات PII ونشرها وتحديثها. |

**المراقبة**

ينبغي للمنظمات أن ترفع إلى الإدارة العليا والموظفين الآخرين الذين تقع على عاتقهم مسؤولية مراقبة حماية المعلومات PII تقارير (مثلاً الإبلاغ عن الانتهاكات والتحقيقات وعمليات التدقيق) وأن تنشرها عند الاقتضاء وتقوم بتحديثها لإثبات المساءلة تجاه ولايات محددة قانونية وتنظيمية لبرامج حماية المعلومات PII.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات، عبر الإبلاغ الداخلي والخارجي عن حماية المعلومات PII، أن تعزز المساءلة والشفافية في عمليات المنظمة لحماية المعلومات PII. كذلك فإن لإبلاغ يساعد المنظمات في تحديد التقدم الحاصل في تلبية متطلبات الامتثال لحماية المعلومات PII وضوابط حماية المعلومات PII، ومقارنة الأداء في المنظمة، وتحديد نقاط الضعف والثغرات في السياسة والتنفيذ، وتحديد نماذج النجاح.

### 12.A أمن المعلومات

| |
|---|
| الهدف: التأكد من أن المعلومات PII محمية بشكلٍ ملائم وفقاً لنتائج تقييم المخاطر. |

**المراقبة**

ينبغي حماية المعلومات PII التي تكون تحت رعاية المنظمة وبحوزتها بواسطة ضوابط ملائمة، وفقاً لنتائج تقييم مخاطر التهديدات أو أثر الخصوصية.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تحمي المعلومات PII بواسطة ضوابط أمنية على المستويات التشغيلية والوظيفية والاستراتيجية لضمان سلامة وسرية وتوافر المعلومات PII، وحمايتها من مخاطر معينة من قبيل النفاذ غير المرخّص أو الإتلاف أو الاستعمال أو التعديل أو الكشف أو الضياع خلال كامل دورة حياتها؛

ب) وتختار معالجي المعلومات PII والعقود المناسبة التي تقدم ضمانات كافية فيما يتعلق بالضوابط التنظيمية والمادية والتقنية لمعالجة المعلومات PII وضمان الامتثال لهذه الضوابط؛

ج) وتضع الضوابط الأمنية على أساس المتطلبات القانونية المعمول بها والمعايير الأمنية ونتائج العمليات المنهجية لتقييم المخاطر الأمنية كما هو محدد في المعيار ISO 31000 ونتائج تحليل التكاليف/المنافع؛

د ) وتقصر النفاذ على الأشخاص الذين يطلبون هذا النفاذ للقيام بواجباتهم وقصر نفاذ هؤلاء الأشخاص فقط على المعلومات PII التي يطلبون النفاذ إليها من أجل القيام بواجباتهم؛

هـ ) وتعمل على إيجاد حلول للمخاطر ونقاط الضعف التي اكتشفت خلال عمليات تقييم مخاطر الخصوصية وعمليات التدقيق؛

و ) وتُخضِع الضوابط إلى استعراض وإعادة تقييم دوريين في عملية مستمرة لإدارة المخاطر الأمنية.

في بعض الأحيان تنص بعض القوانين المتعلقة بخصوصية البيانات على المتطلبات الأمنية، وينبغي في هذه الحالة إبلاغها إلى وظيفة أمن البيانات لتنفيذها.

وينبغي إيلاء العناية الواجبة عند تصميم وتنفيذ الضوابط الأمنية.

## 13.A الامتثال للخصوصية

### 1.13.A الامتثال

| |
|---|
| الهدف: تجنب انتهاكات الالتزامات القانونية أو التنظيمية أو المتعلقة بسياسة الخصوصية أو الالتزامات التعاقدية المتصلة بالخصوصية وبمتطلبات الخصوصية. |

**المراقبة**

ينبغي للمنظمات أن تنفذ تدابير ملائمة للتأكد من أن معالجة المعلومات PII تلبي متطلبات الامتثال.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

ينبغي للمنظمات أن:

أ ) تصدر تقريراً سنوياً ترد فيه تفاصيل المخاطر القائمة ويحدد وضع الامتثال ويتضمن ملخصاً عن الإجراءات البارزة؛

ب) وتتبع عمليات محددة جيداً للاستجابة للانتهاكات قد تتضمن في بعض الولايات القضائية شرط إبلا غ أصحاب المعلومات PII والسلطات الأخرى (مثلاً سلطات حماية البيانات).

### 2.13.A القيود على نقل البيانات عبر الحدود في بعض الولايات القضائية

| |
|---|
| الهدف: حماية المعلومات PII عند نقلها عبر الحدود. |

**المراقبة**

ينبغي للمنظمات أن تنفذ تدابير ملائمة للتأكد من أن عمليات نقل المعلومات PII عبر الحدود تلبي متطلبات الامتثال ذات الصلة.

**توجيهات التنفيذ بشأن حماية المعلومات PII**

في الحالة التي يتعين فيها نقل المعلومات PII إلى بلد غير الأراضي التي تقع فيها المعلومات PII حالياً، قد تفرض اللوائح المتعلقة بخصوصية البيانات في بعض الولايات القضائية قيوداً يمكن أن تكون عادة واحداً أو أكثر من القيود التالية:

أ ) إبلا غ السلطة المعنية بحماية البيانات؛

ب) موافقة السلطة المعنية بحماية البيانات، لا سيما إذا كانت البيانات حساسة؛

ج) إيلاء العناية الواجبة المناسبة للتأكد من أن الحماية المتوفرة للمعلومات PII المنقولة عبر أحد الحدود مكافئة للحماية المطلوبة في البلد الأصلي؛

د ) تنفيذ صكوك محددة لنقل المعلومات من قبيل الاشتراطات التعاقدية المعيارية أو القواعد العامة الملزمة (BCR).

وينبغي للمنظمات أن تنفذ تدابير للتحقق مما إذا كانت القيود المحددة تنطبق على أي نقل مقرر وأن تمتثل لها قبل تنفيذ النقل.

# بيبليوغرافيا


- BSI 10012, *Specification for a personal information management system.*
- European Commission, *Evaluation report on the data retention directive (Directive 2006/24/EC)*, 2011.
- ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
- ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*.
- ISO/IEC 27005, *Information technology – Security techniques – Information security risk management*.
- ISO/IEC 27009, *Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements*.
- ISO/IEC 27018, *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*.
- ISO/IEC 29134, *Information technology – Security techniques – Guidelines for privacy impact assessment*.
- IEC *Electropedia*. Available (viewed 2017-07-06) at: http://www.electropedia.org/.
- ISO *Online* browsing *platform*. Available (viewed 2017-07-06) at: http://www.iso.org/obp.
- ITU *Terms and definitions*. Available (viewed 2017-07-07) at: http://www.itu.int/ITU-R/go/terminology-database.
- KCS, *Personal information management system*, December, 2011.
- NIST Special Publication 800-53 Appendix J, *Security and privacy controls for federal information systems and organizations*, July, 2011.
- NIST Special Publication 800-122, *Guide to protecting the confidentiality of personally identifiable information (PII)*, April 2010.

## سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

| | |
|---|---|
| السلسلة A | تنظيم العمل في قطاع تقييس الاتصالات |
| السلسلة D | مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي |
| السلسلة E | التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية |
| السلسلة F | خدمات الاتصالات غير الهاتفية |
| السلسلة G | أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية |
| السلسلة H | الأنظمة السمعية المرئية والأنظمة متعددة الوسائط |
| السلسلة I | الشبكة الرقمية متكاملة الخدمات |
| السلسلة J | الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط |
| السلسلة K | الحماية من التداخلات |
| السلسلة L | البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها |
| السلسلة M | إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات |
| السلسلة N | الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية |
| السلسلة O | مواصفات تجهيزات القياس |
| السلسلة P | نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية |
| السلسلة Q | التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما |
| السلسلة R | الإرسال البرقي |
| السلسلة S | التجهيزات المطرافية للخدمات البرقية |
| السلسلة T | المطاريف الخاصة بالخدمات التليماتية |
| السلسلة U | التبديل البرقي |
| السلسلة V | اتصالات البيانات على الشبكة الهاتفية |
| **السلسلة X** | **شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن** |
| السلسلة Y | البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية |
| السلسلة Z | اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات |

طُبعت في سويسرا
جنيف، 2018