Norme internationale

ISO/IEC 27701

Deuxième édition
2025-10

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la protection de la vie privée — Exigences et recommandations

Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

Numéro de référence
ISO/IEC 27701:2025(fr)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos ..... **v**

Introduction ..... **vi**

1 Domaine d'application **1**

2 Références normatives **1**

3 Termes, définitions et abréviations **1**

4 Contexte de l'organisme **5**
4.1 Comprendre l'organisme et son contexte 5
4.2 Comprendre les besoins et attentes des parties intéressées 5
4.3 Déterminer le champ d'application du système de management de la protection de la vie privée 6
4.4 Système de management de la protection de la vie privée 6

5 Leadership **6**
5.1 Leadership et engagement 6
5.2 Politique de protection de la vie privée 7
5.3 Rôles, responsabilités et autorités au sein de l'organisme 7

6 Planification **8**
6.1 Actions pour traiter les risques et les opportunités 8
6.1.1 Généralités 8
6.1.2 Appréciation des risques sur la vie privée 8
6.1.3 Traitement des risques sur la vie privée 9
6.2 Objectifs de protection de la vie privée et planification pour les atteindre 10
6.3 Planification des changements 11

7 Support **11**
7.1 Ressources 11
7.2 Compétences 11
7.3 Sensibilisation 11
7.4 Communication 11
7.5 Informations documentées 12
7.5.1 Généralités 12
7.5.2 Création et mise à jour des informations documentées 12
7.5.3 Maîtrise des informations documentées 12

8 Réalisation **13**
8.1 Planification et maîtrise 13
8.2 Appréciation des risques sur la vie privée 13
8.3 Traitement des risques sur la vie privée 13

9 Évaluation des performances **13**
9.1 Surveillance, mesure, analyse et évaluation 13
9.2 Audit interne 14
9.2.1 Généralités 14
9.2.2 Programme d'audit interne 14
9.3 Revue de direction 14
9.3.1 Généralités 14
9.3.2 Éléments d'entrée de la revue de direction 14
9.3.3 Résultats des revues de direction 15

10 Amélioration **15**
10.1 Amélioration continue 15
10.2 Non-conformité et action corrective 15

11 Informations supplémentaires sur les annexes **15**

Annexe A (normative) **Objectifs et mesures de référence du PIMS pour les responsables de traitement de DCP et les sous-traitants de DCP** **17**

Annexe B (normative) **Recommandations de mise en œuvre pour les responsables de traitement de DCP et les sous-traitants de DCP** **23**
Annexe C (informative) **Correspondance avec l'ISO/IEC 29100** **56**
Annexe D (informative) **Correspondance avec le Règlement général sur la protection des données** **59**
Annexe E (informative) **Correspondance avec l'ISO/IEC 27018 et l'ISO/IEC 29151** **62**
Annexe F (informative) **Correspondance avec l'ISO/IEC 27701:2019** **64**
Bibliographie **71**

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, participent également aux travaux.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives ou www.iec.ch/members_experts/refdocs).

L'ISO et l'IEC attirent l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO et l'IEC ne prennent pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, L'ISO et l'IEC n'avaient pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets et https://patents.iec.ch. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié tout ou partie de tels droits de propriété.

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/iso/avant-propos. Pour l'IEC, voir www.iec.ch/understanding-standards.

Le présent document a été élaboré par le comité technique ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée,* en collaboration avec le comité technique CEN/CLC/JTC 13, *Cybersécurité et protection des données*, du Comité européen de normalisation (CEN), conformément à l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Cette deuxième édition annule et remplace la première édition (ISO/IEC 27701:2019), qui a fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— le document a été reformulé en tant que norme de système de management autonome.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/members.html et www.iec.ch/national-committees.

Introduction

0.1 Généralités

Tous les organismes ou presque traitent des données à caractère personnel (DCP). En outre, la quantité et les types de DCP traitées sont en augmentation, de même que le nombre de situations où un organisme a besoin de collaborer avec d'autres organismes en ce qui concerne le traitement des DCP. La protection de la vie privée dans le contexte du traitement des DCP est une nécessité sociétale, et elle fait l'objet d'exigences légales dédiées dans le monde entier.

Le présent document inclut une mise en correspondance avec:

— les principes et le cadre de la protection de la vie privée définis dans l'ISO/IEC 29100;

— l'ISO/IEC 27018;

— ISO/IEC 29151;

— le Règlement général sur la protection des données.

NOTE Il est possible d'interpréter ces correspondances de façon à tenir compte des exigences légales locales.

Le présent document peut être utilisé par les responsables de traitement de DCP (y compris ceux qui sont des responsables conjoints de traitement) et les sous-traitants de DCP (y compris ceux qui utilisent des sous-traitants de DCP sous-traitants et ceux qui traitent des DCP en tant que sous-traitants à des sous-traitants de DCP).

En se conformant aux exigences du présent document, un organisme peut produire des preuves de la façon dont il gère le traitement des DCP. Ces preuves peuvent être utilisées pour faciliter les accords avec les partenaires d'affaires là où les deux parties sont concernées par le traitement des DCP. Cela peut également faciliter les relations avec d'autres parties intéressées. L'utilisation du présent document peut fournir une vérification indépendante de ces preuves.

0.2 Compatibilité avec les autres normes de systèmes de management

Le présent document applique le cadre élaboré par l'ISO afin d'améliorer l'harmonisation entre ses normes de systèmes de management.

Le présent document permet à un organisme d'aligner ou d'intégrer son système de management de la protection de la vie privée (PIMS) aux exigences d'autres normes de systèmes de management, et notamment au système de management de la sécurité de l'information spécifié dans l'ISO/IEC 27001.

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la protection de la vie privée — Exigences et recommandations

1 Domaine d'application

Le présent document spécifie les exigences relatives à la création, la mise en œuvre, le maintien et l'amélioration continue d'un système de management de la protection de la vie privée (PIMS).

Des recommandations sont également fournies pour faciliter la mise en œuvre des exigences du présent document.

Le présent document s'adresse aux responsables de traitement de données à caractère personnel (DCP) et aux sous-traitants de DCP chargés et responsables du traitement des DCP.

Le présent document s'applique aux organismes de tous types et de toutes tailles, y compris les entreprises publiques et privées, les entités gouvernementales et les organismes à but non lucratif.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 29100, *Technologies de l'information — Techniques de sécurité — Cadre privé*

3 Termes, définitions et abréviations

Pour les besoins du présent document, les termes et les définitions de l'ISO/IEC 29100 ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/

3.1
organisme
personne ou groupe de personnes ayant ses propres fonctions, avec des responsabilités, des autorités et des relations lui permettant d'atteindre ses *objectifs* (3.6)

Note 1 à l'article: Le concept d'organisme englobe, sans s'y limiter, les travailleurs indépendants, les compagnies, les sociétés, les firmes, les entreprises, les administrations, les partenariats, les organisations caritatives ou les institutions, ou bien une partie ou une combinaison des entités précédemment mentionnées, qu'il s'agisse d'une personne morale ou non, de droit public ou privé.

Note 2 à l'article: Si l'organisme fait partie d'une plus grande entité, le terme «organisme» fait uniquement référence à la partie de cette entité qui est comprise dans le champ d'application du *système de management* (3.23) de la protection de la vie privée.