NORME INTERNATIONALE

ISO/IEC 29100

Première édition
2011-12-15

Technologies de l'information — Techniques de sécurité — Cadre privé

Information technology — Security techniques — Privacy framework

Numéro de référence
ISO/IEC 29100:2011(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

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. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/IEC, Partie 2.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/IEC 29100 a été élaborée par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Introduction

La présente Norme internationale propose un cadre de haut niveau pour la protection des données à caractère personnel (DCP) au sein des systèmes de technologies de l'information et de la communication (TIC). Elle est d'une portée générale par nature, et place les aspects organisationnels, techniques et procéduraux dans un cadre global pour la protection de la vie privée.

Le cadre pour la protection de la vie privée a pour but d'aider les organismes à définir leurs exigences de protection de la vie privée associées aux DCP dans un environnement TIC:

— en établissant une terminologie commune relative à la protection de la vie privée;

— en définissant les acteurs et leurs rôles dans le traitement de DCP;

— en décrivant les exigences de protection de la vie privée; et

— en faisant référence à des principes connus de protection de la vie privée.

Dans certaines juridictions, les références de la présente Norme internationale aux exigences de protection de la vie privée peuvent être considérées comme complémentaires aux exigences légales de protection des DCP. Au vu du nombre croissant des technologies de l'information et de la communication traitant des DCP, il est important de disposer de Normes internationales sur la sécurité de l'information qui garantissent une compréhension commune pour la protection des DCP. La présente Norme internationale a pour but d'améliorer les normes de sécurité existantes en attirant l'attention sur le traitement de DCP.

L'utilisation et la valeur commerciales croissantes des DCP, le partage des DCP entre plusieurs juridictions légales, et la complexité grandissante des systèmes TIC, peuvent rendre difficile, pour un organisme, la tâche d'assurer la protection de la vie privée et la conformité avec les différentes lois applicables. Les parties prenantes en matière de protection de la vie privée peuvent éviter toute incertitude et méfiance en gérant correctement les questions de vie privée et en évitant les cas d'utilisation abusive des DCP.

L'utilisation de la présente Norme internationale permet:

— d'aider à la conception, la mise en œuvre, l'exploitation et la maintenance de systèmes TIC qui traitent des DCP et les protègent;

— de favoriser des solutions innovantes pour mettre en place la protection des DCP au sein des systèmes TIC; et

— d'améliorer les programmes de protection de la vie privée des organismes via l'utilisation des meilleures pratiques.

Le cadre pour la protection de la vie privée défini dans la présente Norme internationale peut servir de base à des initiatives complémentaires de normalisation dans le domaine de la protection de la vie privée, comme:

— une architecture de référence technique;

— la mise en œuvre et l'utilisation de technologies spécifiques pour la protection de la vie privée, ainsi que le management global de la protection de la vie privée;

— des mesures de protection de la vie privée pour les processus de traitement de données qui sont sous-traités;

— l'étude des risques sur la vie privée; ou

— des spécifications d'ingénierie spécifiques.

Certaines juridictions peuvent exiger la conformité avec un ou plusieurs des documents référencés dans l'ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD2) — *Official Privacy Documents References*

[3] ou avec d'autres lois et règlements applicables, mais la présente Norme internationale ne vise pas à constituer un modèle mondial de politique, ni un cadre législatif.

Technologies de l'information — Techniques de sécurité — Cadre privé

1 Domaine d'application

La présente Norme internationale fournit un cadre pour la protection de la vie privée qui:

— spécifie une terminologie commune relative à la protection de la vie privée;

— définit les acteurs et leurs rôles dans le traitement de données à caractère personnel (DCP);

— décrit les éléments à prendre en considération pour la protection de la vie privée; et

— fournit des références à des principes connus de protection de la vie privée pour les technologies de l'information.

La présente Norme internationale s'applique aux personnes physiques et aux organismes participant à la spécification, à la fourniture, à l'architecture, à la conception, au développement, aux essais, à la maintenance, à l'administration et à l'exploitation des systèmes ou services de technologies de l'information et de la communication dans lesquels des mesures de protection de la vie privée sont requises pour le traitement de DCP.

2 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

NOTE Pour faciliter l'utilisation de la famille de Normes internationales ISO/IEC 27000 dans le contexte spécifique de la protection de la vie privée, et pour intégrer les concepts de protection de la vie privée dans le contexte de l'ISO/IEC 27000, les concepts de l'ISO/IEC 27000, qui correspondent aux concepts de l'ISO/IEC 29100 utilisés dans la présente Norme internationale, sont indiqués dans le tableau à l'Annexe A.

2.1
anonymat
caractéristique d'une donnée qui ne permet pas d'identifier directement ou indirectement la personne concernée par des données à caractère personnel

2.2
anonymisation
processus par lequel des données à caractère personnel (DCP) sont altérées irréversiblement, de telle façon que la personne concernée ne puisse plus être identifiée, directement ou indirectement, par le responsable du traitement des DCP, seul ou en collaboration avec une autre partie

2.3
données anonymisées
données générées en sortie d'un processus d'anonymisation de données à caractère personnel

2.4
consentement
accord spécifique et éclairé accordé librement par la personne concernée pour le traitement de ses données à caractère personnel (DCP)

2.5
identifiabilité
condition ayant pour conséquence l'identification, directe ou indirecte, d'une personne concernée par des données à caractère personnel (DCP), sur la base d'un ensemble donné de données à caractère personnel

2.6
identifier
établir un lien entre une personne concernée par des données à caractère personnel (DCP) et des données à caractère personnel (DCP) ou un ensemble de DCP

2.7
identité
ensemble d'attributs qui permettent d'identifier la personne concernée par des données à caractère personnel

2.8
accord préalable
processus ou type de politique par lequel la personne concernée par des données à caractère personnel (DCP) doit activement exprimer son consentement explicite et préalable au traitement de ses données à caractère personnel (DCP), pour une finalité donnée

Note 1 à l'article: Un terme différent, «acceptation par défaut», est souvent utilisé dans le contexte du principe «consentement et choix» de protection de la vie privée. Il décrit un processus ou un type de politique par lequel la personne concernée doit effectuer une démarche séparée afin de refuser d'accorder son consentement, ou de le retirer, ou de s'opposer à un type de traitement spécifique. L'adoption d'une politique d'acceptation par défaut implique que le responsable de traitement de DCP a le droit de traiter les DCP de la manière prévue. Ce droit peut être signifié par une certaine action de la personne concernée différente du consentement (par exemple, le fait de passer commande dans une boutique en ligne).

2.9
données à caractère personnel
DCP
toute donnée qui (a) peut être utilisée pour identifier la personne à laquelle cette donnée se rapporte, ou qui (b) est ou peut être directement ou indirectement associée à une personne concernée

Note 1 à l'article: Pour déterminer si une personne concernée est identifiable, il convient de tenir compte de tous les moyens pouvant être raisonnablement utilisés par la partie prenante en matière de protection de la vie privée qui détient les données, ou par toute autre partie, pour identifier cette personne physique.

2.10
responsable de traitement de DCP
partie(s) prenante(s) en matière de protection de la vie privée qui détermine(-nt) les finalités et les moyens pour le traitement de données à caractère personnel (DCP), autre(s) que les personnes physiques qui utilisent des données à des fins personnelles

Note 1 à l'article: Un responsable de traitement de DCP demande parfois à des tiers (par exemple, des sous-traitants de DCP) de traiter des DCP en son nom, bien qu'un tel traitement relève toujours de la responsabilité du responsable de traitement de DCP.

2.11
personne concernée
personne physique à qui se rapportent les données à caractère personnel (DCP)

Note 1 à l'article: Selon la juridiction et la loi applicable en matière de protection des données et de la vie privée, en anglais, le terme «data subject» peut également être employé en lieu et place de «PII principal».

2.12
sous-traitant de DCP
partie prenante en matière de protection de la vie privée qui traite des données à caractère personnel (DCP) pour le compte d'un responsable de traitement de DCP et conformément à ses instructions

2.13
violation de données à caractère personnel
situation dans laquelle des données à caractère personnel sont traitées en violation d'une ou de plusieurs exigences applicables en matière de protection de la vie privée

2.14
mesures de protection de la vie privée
mesures de traitement des risques sur la vie privée destinées à réduire leur probabilité ou leurs conséquences

Note 1 à l'article: Les mesures de protection de la vie privée comprennent des mesures organisationnelles, physiques et techniques, telles que, par exemple, les politiques, les procédures, les lignes directrices, les contrats juridiques, les pratiques de management ou les structures organisationnelles.

Note 2 à l'article: Le terme «mesure de protection» est également utilisé comme synonyme de «mesure de sauvegarde» ou «contre-mesure».

2.15
technologie contribuant à la protection de la vie privée
(*Privacy Enhancing Technologies – PET*)
mesure de protection de la vie privée constituée de mesures, produits ou services des technologies de l'information et de la communication (TIC) qui protègent la vie privée en éliminant ou en réduisant les données à caractère personnel (DCP) ou en empêchant tout traitement inutile et/ou indésirable des DCP, tout cela sans perte de la fonctionnalité du système TIC

Note 1 à l'article: Les exemples de technologies contribuant à la protection de la vie privée comprennent, sans s'y limiter, les outils d'anonymisation et de pseudonymisation qui éliminent, réduisent, masquent ou désidentifient les DCP, ou qui empêchent tout traitement inutile, non autorisé et/ou indésirable des DCP.

Note 2 à l'article: Le masquage est le processus qui consiste à obscurcir des éléments de DCP.

2.16
politique de protection de la vie privée
intention et orientation générales, règles et engagement, tels qu'ils sont formellement exprimés par un responsable de traitement de données à caractère personnel (DCP), en relation avec le traitement de données à caractère personnel DCP dans un contexte particulier

2.17
préférences relatives à protection de la vie privée
choix spécifiques faits par une personne concernée par des données à caractère personnel (DCP) et relatifs à la manière dont il convient de traiter ses données à caractère personnel DCP pour une finalité donnée

2.18
principes de protection de la vie privée
ensemble de valeurs partagées qui régissent la protection des données à caractère personnel (DCP) quand elles sont traitées par des systèmes de technologies de l'information et de la communication

2.19
risque sur la vie privée
effet de l'incertitude sur la protection de la vie privée

Note 1 à l'article: Le risque est défini comme «l'effet de l'incertitude sur l'atteinte des objectifs» dans le Guide ISO 73 et l'ISO 31000.

Note 2 à l'article: L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.

2.20
étude des risques sur la vie privée
processus général d'identification des risques, d'analyse du risque et d'évaluation du risque par rapport au traitement de données à caractère personnel (DCP)

Note 1 à l'article: Ce processus est également appelé études d'impacts sur la vie privée.

2.21
exigences de protection de la vie privée
ensemble d'exigences qu'un organisme doit prendre en compte lorsqu'il traite des données à caractère personnel (DCP), eu égard à la protection des DCP

2.22
partie prenante en matière de protection de la vie privée
personne physique ou morale, autorité publique, service ou tout autre organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité associée au traitement de données à caractère personnel (DCP)

2.23
traitement de DCP
opération ou ensemble d'opérations exécutées sur des données à caractère personnel (DCP)

Note 1 à l'article: Les opérations de traitement des DCP incluent par exemple, sans toutefois s'y limiter, la collecte, le stockage, l'altération, la récupération, la consultation, la divulgation, l'anonymisation, la pseudonymisation, la distribution ou toute autre mise à disposition, la suppression ou la destruction de DCP.

2.24
pseudonymisation
processus appliqué aux données à caractère personnel (DCP) qui remplace les données d'identification par un alias

Note 1 à l'article: La pseudonymisation peut être effectuée soit par les personnes concernées elles-mêmes, soit par les responsables de traitement de DCP. La pseudonymisation peut permettre aux personnes concernées d'utiliser régulièrement une ressource ou un service sans divulguer leur identité à cette ressource ou ce service (ou entre services), tout en restant responsable de cette utilisation.

Note 2 à l'article: La pseudonymisation n'exclut pas la possibilité qu'il puisse y avoir (un nombre restreint de) parties prenantes en matière de protection de la vie privée, autres que le responsable de traitement de DCP des données pseudonymisées, capable de déterminer l'identité de la personne concernée d'après l'alias et les données qui y sont rattachées.

2.25
utilisation secondaire
traitement de données à caractère personnel (DCP) dans des conditions qui diffèrent des conditions initiales

Note 1 à l'article: Les conditions qui diffèrent des conditions initiales pourraient mettre en jeu, par exemple, une nouvelle finalité de traitement des DCP, un nouveau destinataire des DCP, etc.

2.26
DCP sensibles
catégorie de données à caractère personnel (DCP), soit qui sont sensibles par nature, comme celles qui concernent la sphère la plus privée de la personne concernée, soit qui pourraient avoir un impact significatif sur la personne concernée

Note 1 à l'article: Dans certaines juridictions ou dans des contextes spécifiques, les DCP sensibles sont définies suivant leur nature et peuvent être des DCP qui révèlent l'origine raciale, les opinions politiques ou les convictions religieuses ou autres, les données personnelles sur la santé, la vie sexuelle ou les antécédents judiciaires, ainsi que d'autres DCP qui pourraient être considérées comme sensibles.

2.27
tiers
partie prenante en matière de protection de la vie privée, autre que la personne concernée par les données à caractère personnel, le responsable de traitement de DCP et le sous-traitant de DCP, et les personnes physiques autorisées à traiter les données sous l'autorité directe du responsable de traitement de DCP ou du sous-traitant de DCP

3 Symboles et abréviations

Les abréviations suivantes sont communes à l'ISO/IEC 29100.

TIC Technologies de l'information et de la communication

PET Technologie contribuant à la protection de la vie privée

DCP Données à caractère personnel

4 Éléments de base du cadre pour la protection de la vie privée

4.1 Vue d'ensemble du cadre pour la protection de la vie privée

Les éléments suivants concernent la protection de la vie privée et le traitement de DCP dans les systèmes TIC, et constituent le cadre de protection de la vie privée décrit dans la présente Norme internationale:

— acteurs et rôles;

— interactions;

— reconnaissance des DCP;

— exigences de protection de la vie privée;

— politique de protection de la vie privée; et

— mesures de protection de la vie privée.

Des concepts, des définitions et des recommandations d'autres sources officielles ont été prises en compte pour le développement de ce cadre pour la protection de la vie privée. Ces sources sont répertoriées dans l'ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD2) — *Official Privacy Documents References [3]*.

4.2 Acteurs et rôles

Pour les besoins de la présente norme, il est important d'identifier les acteurs qui interviennent dans le traitement de DCP. Quatre types d'acteurs peuvent intervenir dans le traitement de DCP: les personnes concernées, les responsables de traitement de DCP, les sous-traitants de DCP et les tiers.

4.2.1 Personnes concernées

Les personnes concernées fournissent leurs DCP pour traitement par les responsables de traitement de DCP et les sous-traitants de DCP et, en l'absence de toutes dispositions contraires dans les lois applicables, elles donnent leur consentement et déterminent leurs préférences relatives à la protection de la vie privée sur la manière dont il convient que leurs DCP soient traitées. Les personnes concernées peuvent inclure, par exemple, un employé mentionné dans le système de ressources humaines d'une société, un consommateur mentionné dans un rapport d'antécédents de crédit, et un patient mentionné dans un dossier médical informatisé. Il n'est pas toujours nécessaire que la personne physique respective soit identifiée directement sous son nom pour être considérée comme une personne concernée. Si la personne concernée à laquelle se rapportent les DCP peut être identifiée indirectement (par exemple au moyen d'un identifiant de compte, un numéro de sécurité sociale, ou éventuellement par le biais d'une combinaison d'attributs accessibles), elle est considérée comme personne concernée pour l'ensemble de ces DCP.

4.2.2 Responsables de traitement de DCP

Un responsable de traitement de DCP détermine pourquoi (finalité) et comment (moyens) le traitement de DCP a lieu. Il convient que le responsable de traitement de DCP garantisse le respect des principes de