NORME INTERNATIONALE

ISO/IEC 29184

Première édition
2020-06

Technologies de l'information — Mentions sur la protection de la vie privée et consentement en ligne

Information technology — Online privacy notices and consent

Numéro de référence
ISO/IEC 29184:2020(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.

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 document. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

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. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets) ou dans la liste des déclarations de brevets reçues par l'IEC (voir http://patents.iec.ch).

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 le lien suivant: www.iso.org/iso/fr/avant-propos.

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

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/fr/members.html.

Introduction

La plus grande disponibilité des infrastructures de communication telles que les connexions domestiques haut débit et l'internet mondial, l'utilisation croissante des smartphones et d'autres appareils (par exemple, appareils portables) qui collectent des informations sur les activités des individus, et les améliorations des capacités de traitement de l'information ont permis une collecte et une analyse beaucoup plus larges des informations personnelles. Ces améliorations technologiques offrent de meilleures perspectives en matière de confort de vie des consommateurs, de nouvelles opportunités commerciales, de services plus attrayants et de valeur ajoutée. D'autre part, les consommateurs sont de plus en plus soucieux de la protection de leur vie privée et remettent en question l'impact sur celle-ci de la collecte et de l'utilisation des données à caractère personnel (DCP) par les services en ligne. Cette critique est souvent due à l'absence d'explication claire sur la manière dont leurs DCP sont traitées, stockées, conservées et gérées.

Le présent document spécifie les mesures et les informations complémentaires associées destinées aux organismes pour:

— fournir une base pour présenter des informations claires et faciles à comprendre aux personnes dont les DCP sont collectées, sur la manière dont l'organisme traite leurs DCP (par exemple, lors de la fourniture de services à des consommateurs ou dans le cadre d'une relation de travail); et

— obtenir le consentement de la part des personnes concernées de manière loyale, démontrable, transparente, univoque et révocable (rétractable).

Le présent document fournit les détails de la mise en œuvre de deux principes de protection de la vie privée de l'ISO/IEC 29100 (c'est-à-dire, principe 1: consentement et choix; principe 7: ouverture, transparence et information).

Technologies de l'information — Mentions sur la protection de la vie privée et consentement en ligne

1 Domaine d'application

Le présent document spécifie les mesures qui forment le contenu et la structure des mentions sur la protection de la vie privée en ligne ainsi que le processus de demande du consentement en vue de collecter et de traiter les données à caractère personnel (DCP) des personnes concernées.

Le présent document s'applique à tous les contextes en ligne dans lesquels un responsable de traitement de DCP ou toute autre entité traitant des DCP informe les personnes concernées du traitement.

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 et définitions

Pour les besoins du présent document, les termes et 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
consentement explicite
accord univoque spécifique et éclairé accordé librement par la personne concernée pour le traitement de ses données à caractère personnel (DCP), exprimé à travers un acte positif indiquant un tel consentement de la part de la personne concernée

Note 1 à l'article: Le consentement explicite est le résultat d'un accord préalable.

Note 2 à l'article: Le consentement explicite peut également être désigné par «consentement exprès».

EXEMPLE Le consentement est obtenu en demandant à la personne concernée de réaliser une action spécifique dans le contexte d'une mention.

[SOURCE: ISO/IEC 29100:2011, 2.4, modifié – Les mots «exprimé à travers un acte positif indiquant un tel consentement de la part de la personne concernée» ont été ajoutés.]

3.2
mention
informations concernant le traitement des DCP

Note 1 à l'article: Communiquées aux personnes concernées à travers différents canaux, sous une forme concise, transparente, compréhensible et facile d'accès, à l'aide d'un langage clair et simple.

3.3
élément de DCP
catégorie de DCP
information de DCP
descripteur d'un type d'information ou d'un ensemble de types d'information

4 Symboles et abréviations

DCP données à caractère personnel

JSON notation d'objet JavaScript [*JavaScript object notation*]

PC ordinateur individuel [*personal computer*]

XML langage XML [*extensible markup language*]

5 Exigences générales et recommandations

5.1 Objectif général

L'objectif général du présent document est de permettre aux personnes concernées de comprendre et d'agir en fonction des implications du traitement des DCP, telles que la probabilité et la gravité de tout impact potentiel du traitement, ainsi que des conséquences directes et/ou indirectes du traitement.

Les organismes souhaitant démontrer leur conformité au présent document doivent documenter pour chaque mesure de l'Article 5:

a) si la mesure s'applique;

b) lorsque des raisons peuvent justifier la non-application de la mesure, que la justification est documentée et validée;

c) la manière dont la mise en œuvre de la mesure est vérifiée et validée.

5.2 Mention

5.2.1 Généralités

Objectif: fournir une mention lorsqu'elle est exigée, dans un langage adapté aux personnes concernées, à un moment qui permet aux personnes concernées d'exercer leur consentement à bon escient, à des endroits où il est facile pour les personnes concernées de reconnaître les informations, et avec des références qui fournissent aux personnes concernées un accès à du contenu complémentaire, notamment des mentions préalables et leurs réponses.

5.2.2 Obligation de fournir une mention

Mesure

L'organisme doit identifier les situations où il est nécessaire de fournir une mention et doit fournir une mention conforme au paragraphe 5.3 aux personnes concernées lorsqu'elle est exigée.

Informations complémentaires

Il convient que la mention fournisse à toutes les parties intéressées, y compris extérieures à l'organisme, les pratiques de l'organisme en matière de protection de la vie privée ainsi que d'autres informations pertinentes telles que les coordonnées, notamment l'identité et la domiciliation, du responsable de traitement de DCP, et les points de contact à partir desquels les personnes concernées peuvent obtenir des informations supplémentaires (voir Annexe A).

L'affichage d'une mention visuelle est une manière de fournir une mention. En matière d'accessibilité, des lecteurs d'écran pour les mentions visuelles ou des mentions directement audibles peuvent être appropriés pour aider les personnes malvoyantes. D'autres formes de mention peuvent également être appropriées (voir 5.2.9).

Il convient que l'organisme fournisse une mention aux personnes concernées. Une mention peut être requise, entre autres, lorsque l'organisme prévoit de collecter de nouvelles DCP (auprès de la personne concernée ou à partir d'une autre source) ou lorsqu'il prévoit d'utiliser des DCP déjà collectées pour de nouvelles finalités.

5.2.3 Expression appropriée

Mesure

L'organisme doit fournir la mention de manière claire et facile à comprendre pour les personnes concernées visées. La mention doit être facilement lisible et formulée dans un langage concis qu'une personne sans aucune formation juridique ou technique puisse comprendre de manière raisonnable.

Informations complémentaires

Il convient que la mention soit rédigée en tenant compte des catégories ou types particuliers de personnes concernées (par exemple, sous-groupes sociétaux défavorisés).

5.2.4 Mention multilingue

Mesure

L'organisme doit fournir la mention dans la ou les langue(s) convenant aux attentes linguistiques des personnes concernées visées.

Informations complémentaires

Par exemple, l'organisme peut présenter à la personne concernée une liste des langues prises en charge affichées dans leur langue respective et permettre à la personne concernée de choisir la langue. Il est important d'afficher le nom de chaque langue dans sa propre langue, car la personne concernée peut ne pas être capable de reconnaître une langue si elle est affichée dans une autre langue.

Un navigateur web possède un paramètre de préférence pour une langue préférée, ce qui peut être utilisé à cette fin. Toutefois, dépendre uniquement de la préférence de langue du navigateur peut ne pas être une bonne idée, car la personne concernée peut utiliser un ordinateur partagé.

5.2.5 Moment approprié

Mesure

L'organisme doit déterminer et documenter le moment approprié (par exemple, immédiatement avant la collecte de DCP) pour fournir une mention aux personnes concernées lorsque l'activité considérée concerne leurs intérêts en matière de protection de la vie privée.

Informations complémentaires

Lorsqu'un organisme fournit une mention à une personne concernée puis collecte les DCP ultérieurement, y compris dans les cas où les données sont collectées à partir d'une autre source, le moment de la mention peut différer de celui de la collecte des DCP de manière significative.

Il convient que l'organisme fournisse une mention lorsque l'utilisation des DCP peut avoir des effets inattendus ou importants sur les personnes concernées. Si un organisme prévoit de collecter des DCP supplémentaires, il convient qu'il fournisse une mention supplémentaire.

5.2.6 Emplacements appropriés

Mesure

L'organisme doit fournir des mentions d'une manière qui soit appropriée au produit ou service concerné de sorte que les personnes concernées puissent trouver et accéder aux mentions par voie électronique et facilement, notamment sur des emplacements en ligne.

Informations complémentaires

Les emplacements en ligne appropriés peuvent inclure, sans toutefois s'y limiter, des liens sur les pages principales des sites web de l'organisme ou sur la page d'accueil, la page de démarrage des applications mobiles, des formulaires en ligne ou dans des portails captifs.

Dans certains cas, les DCP peuvent être traitées sans interaction préalable avec la personne concernée. Du point de vue des personnes concernées, il serait très difficile de savoir qui traite leurs données et, par conséquent, il n'est pas utile de publier la mention sur la protection de la vie privée uniquement sur le site web de l'organisme. Il est utile d'avoir un endroit où une personne concernée peut se rendre et obtenir les mentions sur la protection de la vie privée de ces organismes. Ainsi, il convient, lorsque cela s'applique et dans la mesure du possible, que l'organisme envisage d'utiliser un référentiel commun accessible au public où les parties prenantes peuvent trouver et accéder facilement aux mentions pertinentes.

5.2.7 Forme appropriée

Mesure

L'organisme doit déterminer la manière dont la mention est fournie et rendue accessible par rapport au moment du traitement.

Informations complémentaires

L'organisme peut mettre en œuvre la mesure à l'aide de différentes techniques: mentions sur différents niveaux, tableaux de bord, mentions et icônes «juste à temps», et peut fournir des mentions dans un format lisible par machine de sorte que le logiciel qui le présente à la personne concernée peut l'analyser afin d'optimiser l'interface utilisateur et d'aider les personnes concernées dans leur prise de décision.

Si l'organisme met en œuvre la mesure à l'aide d'une mention sur différents niveaux, il convient que le premier niveau détaille tout élément inattendu ou pouvant avoir un impact significatif, tel que déterminé par l'évaluation décrite en 5.3.3, sur une personne concernée. Il convient que les autres niveaux fassent mention de toutes les activités de collecte et/ou de traitement afin de donner à la personne concernée des informations détaillées concernant ces activités.

Il convient que les organismes affichent le premier niveau de chaque mention de sorte que les personnes concernées soient capables de la lire le plus rapidement possible. Il convient qu'elle ne dépasse pas quelques écrans. Compte tenu des contraintes de volume, il peut ne pas être possible d'afficher tout le contenu sur un écran. Auquel cas, il convient que les organismes affichent le résumé en premier. Dans le contexte des appareils mobiles et des smartphones, il est utile, pour une meilleure lisibilité, d'introduire une «approche multi-niveaux» pour les mentions et le consentement, en montrant un texte court contenant les informations essentielles et un lien vers le texte intégral de la mention/déclaration de consentement.

Lorsque les organismes affichent les éléments de DCP à collecter, il convient de les afficher par groupes en énumérant en premier ceux ayant l'impact potentiel le plus élevé en matière de vie privée de sorte que les personnes concernées puissent reconnaître clairement les différences.

Il convient que les organismes mettent le contenu, notamment les informations pertinentes omises dans le premier écran ou les écrans suivants, à la disposition des personnes concernées si elles le souhaitent.

NOTE Dans le cas des notifications en ligne, des fenêtres contextuelles et des zooms avant peuvent être utilisés pour afficher le contenu. Les personnes concernées peuvent avoir des difficultés à lire un grand nombre de conditions générales dans un contrat, notamment lorsqu'elles sont sur le point de réaliser une action.

Les mentions lisibles par machine peuvent être fournies dans un format XML ou JSON standard. Ainsi, il devient possible pour les appareils de sélectionner les éléments de manière appropriée et d'afficher des graphismes et des icônes le cas échéant. Toutefois, les organismes doivent noter que l'interprétation de la représentation graphique par la personne concernée peut varier considérablement en fonction des milieux culturels. Des recommandations pour la région ou la culture concernée peuvent être créées afin d'éviter la confusion des personnes concernées.

5.2.8 Consultation continue

Mesure

L'organisme doit conserver et mettre à disposition la version de la mention présentée lorsque la personne concernée a donné son consentement, ainsi que la version pertinente la plus récente pour que la personne concernée puisse la consulter facilement.

Informations complémentaires

Il convient de conserver les versions des mentions aussi longtemps qu'elles sont associées à des DCP conservées.

5.2.9 Accessibilité

Mesure

L'organisme doit fournir une mention d'une manière accessible et adaptée aux technologies qui sous-tendent le service en ligne.

Informations complémentaires

En particulier dans les cas où il est attendu que des personnes ayant des problèmes d'accessibilité accèdent aux mentions, il convient que celles-ci leur permettent de comprendre le contenu des mentions. Cela peut impliquer la nécessité de s'assurer que le texte de la mention peut être converti en son pour les personnes ayant des problèmes de vue.

Les lignes directrices telles que l'ISO/IEC 40500 aident à la conception de l'accessibilité.

5.3 Contenu de la mention

5.3.1 Généralités

Objectif: S'assurer que la personne concernée a suffisamment d'informations dans la mention pour comprendre la manière dont les DCP sont traitées et quels sont ses droits.

5.3.2 Description des finalités

Mesure

L'organisme doit s'assurer que la mention inclut les informations concernant la finalité ou les finalités pour lesquels les DCP sont traitées.

Informations complémentaires

Il est important que les personnes concernées comprennent les finalités du traitement des DCP collectées de sorte qu'elles puissent fournir un consentement averti. À des fins de concision de la mention, un nom ou une formule courte peuvent être utilisés, mais il convient qu'il soit possible (par exemple, au moyen d'un lien hypertexte) d'associer ce nom ou cette formule à un aperçu de la finalité qui soit suffisant pour que les personnes concernées fournissent un consentement averti.

Les mentions doivent être rédigées avec soin, car l'inclusion de trop de détails peut entraîner la nécessité de les rééditer fréquemment.

5.3.3 Présentation de la description des finalités

Mesure

L'organisme doit spécifier les finalités liés à la collecte de chaque élément de DCP ainsi que les informations appropriées concernant le risque plausible lié au traitement, dans un ordre correspondant à l'évaluation générale du risque.

NOTE L'impact et le risque sont nécessairement évidents.

Informations complémentaires

L'organisme explique la manière dont les DCP sont utilisées de façon à ce que la personne concernée en comprenne la finalité clairement et facilement. Si la finalité de l'utilisation varie parmi les éléments de DCP collectés, il convient que l'organisme indique clairement à quel élément de DCP s'applique chaque finalité.

5.3.4 Identification du responsable de traitement de DCP

Mesure

L'organisme doit fournir à la personne concernée les informations pertinentes (par exemple, l'identité et les coordonnées) relatives au responsable de traitement de DCP.

Informations complémentaires

Le responsable de traitement de DCP est généralement identifié par le nom de l'entreprise, mais peut également l'être en mentionnant le numéro de société, l'adresse du siège/du site d'exploitation et (le cas échéant) les informations du service concerné.

5.3.5 Collecte des DCP

Mesure

L'organisme doit fournir les informations permettant aux personnes concernées de comprendre quels éléments de DCP sont collectés, même lorsque la collecte des éléments particuliers de DCP est évidente.

Informations complémentaires

Outre l'utilisation d'un langage générique tel que «Nous collectons vos informations personnelles.», le cas échéant, en fonction de l'impact déterminé par l'évaluation décrite en 5.3.3, il convient que l'organisme fournisse la liste des éléments spécifiques de DCP collectés (par exemple, «Nous collectons votre nom, votre adresse et votre numéro de téléphone.»), même si les informations collectées sont évidentes.

Pour identifier quelles DCP méritent d'être énumérées dans la mention, il convient que l'organisme consulte l'ISO/IEC 29100:2011, 4.4.

Il convient que l'organisme présente la valeur réelle d'un élément de DCP collecté au moment de la collecte lorsque cela est pertinent, réalisable et concret. Lorsque ce n'est pas réalisable, l'organisme

