NORME INTERNATIONALE

ISO/IEC 29151

Première édition
2017-08

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la protection des données à caractère personnel

Information technology — Security techniques — Code of practice for personally identifiable information protection

Numéro de référence
ISO/IEC 29151:2017(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) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

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 ISO. 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 ne saurait être tenue pour responsable 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).

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 ISO/JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée* en collaboration avec l'ITU-T. Ce même texte est publié en tant que Recommandation ITU-T X.1058.

Introduction

Le nombre d'organisations traitant des données à caractère personnel (DCP) est en augmentation, tout comme la quantité de DCP que ces organisations traitent. Dans le même temps, les attentes de la société en matière de protection des DCP et de sécurité des données relatives aux personnes augmentent également. Un certain nombre de pays renforcent leur législation afin de faire face au nombre croissant de violations de données à grand retentissement.

Avec l'augmentation du nombre de violations des DCP, les organisations qui collectent ou traitent des DCP auront de plus en plus besoin de recommandations sur la manière dont il convient qu'elles protègent les DCP afin de réduire le risque de violations de données à caractère personnel ainsi que l'impact des violations sur l'organisation et les personnes concernées. La présente Spécification fournit ces recommandations.

La présente Spécification fournit aux responsables de traitement de DCP des recommandations sur un large éventail de mesures de sécurité de l'information et de protection des DCP qui sont couramment appliquées dans de nombreuses organisations différentes qui traitent de la protection des DCP. Les autres parties de la famille de normes ISO/IEC, répertoriées ici, fournissent des recommandations ou des exigences sur d'autres aspects du processus global de protection des DCP :

- L'ISO/IEC 27001 spécifie un processus de management de la sécurité de l'information et les exigences associées, qui pourraient être utilisés comme base pour la protection des DCP.
- L'ISO/IEC 27002 fournit des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information, incluant la sélection, la mise en œuvre et la gestion de mesures de sécurité, en tenant compte du ou des environnement(s) de risques de sécurité de l'information de l'organisation.
- L'ISO/IEC 27009 définit les exigences relatives à l'utilisation de l'ISO/IEC 27001 dans n'importe quel secteur spécifique (domaine, domaine d'application ou secteur de marché). Elle explique comment ajouter des exigences supplémentaires à celles de l'ISO/IEC 27001, comment affiner les exigences de l'ISO/IEC 27001, et comment ajouter des mesures de sécurité ou des ensembles de mesures de sécurité à l'Annexe A de l'ISO/IEC 27001.
- L'ISO/IEC 27018 fournit des recommandations aux organisations agissant comme sous-traitants de DCP lorsqu'elles offrent des capacités de traitement en tant que services en nuage.
- L'ISO/IEC 29134 fournit des lignes directrices pour l'identification, l'analyse et l'évaluation des risques sur la vie privée, tandis que l'ISO/IEC 27001 et l'ISO/IEC 27005 fournissent une méthodologie pour l'identification, l'analyse et l'évaluation des risques de sécurité.

Il convient que les mesures de sécurité soient choisies sur la base des risques identifiés à la suite d'une analyse du risque afin de développer un système de mesures de sécurité complet et cohérent. Il convient que les mesures de sécurité soient adaptées au contexte du traitement de DCP spécifique.

La présente Spécification contient deux parties : 1) le corps principal, composé des Articles 1 à 18, et 2, une annexe normative. Cette structure reflète la pratique normale pour l'élaboration d'extensions sectorielles de l'ISO/IEC 27002.

La structure du corps principal de la présente Spécification, y compris l'intitulé des articles et paragraphes, reflète le corps principal de l'ISO/IEC 27002. L'introduction et les Articles 1 à 4 fournissent le contexte de l'utilisation de la présente Spécification. Les intitulés des Articles 5 à 18 reflètent ceux de l'ISO/IEC 27002, ce qui illustre le fait que la présente Spécification s'appuie sur les recommandations de l'ISO/IEC 27002, et ajoute de nouvelles mesures de sécurité spécifiques à la protection des DCP. Un grand nombre de mesures de sécurité de l'ISO/IEC 27002 n'ont pas besoin d'être renforcées dans le contexte des responsables de traitement des DCP. Toutefois, dans certains cas, des recommandations de mise en œuvre supplémentaires sont nécessaires et sont fournies sous l'intitulé (et le numéro de paragraphe ou d'article) approprié de l'ISO/IEC 27002.

L'annexe normative contient un ensemble étendu de mesures de sécurité spécifiques à la protection des DCP qui complètent celles fournies dans l'ISO/IEC 27002. Ces nouvelles mesures de protection des DCP, et les recommandations qui leur sont associées, sont réparties en 12 catégories, qui correspondent à la politique de protection de la vie privée et aux 11 principes de protection de la vie privée de l'ISO/IEC 29100 :

- consentement et choix ;
- licéité et spécification de la finalité ;
- limitation de la collecte ;
- minimisation des données ;

- limitation de l'utilisation, de la conservation et de la divulgation ;
- exactitude et qualité ;
- ouverture, transparence et information ;
- participation et accès individuels ;
- responsabilité ;
- sécurité de l'information ; et
- conformité aux règles de protection de la vie privée.

La Figure 1 décrit la relation entre la présente Spécification et la famille de normes ISO/IEC.

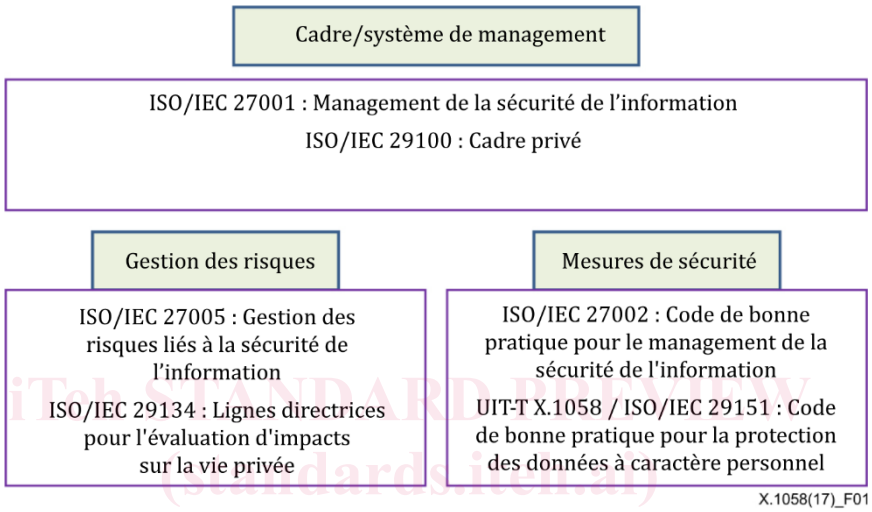

Figure 1 – Relation entre la présente Spécification et la famille de normes ISO/IEC

La présente Spécification comprend des lignes directrices basées sur l'ISO/IEC 27002, et les adapte si nécessaire pour répondre aux exigences de protection de la vie privée qui découlent du traitement des DCP :

a) dans différents domaines de traitement tels que :
   - services en nuage public ;
   - application de réseaux sociaux ;
   - dispositifs domestiques connectés à Internet ;
   - recherche, analyse ;
   - ciblage des DCP à des fins publicitaires ou similaires ;
   - programmes d'analyse des mégadonnées ;
   - traitement de l'emploi ;
   - gestion d'entreprise dans le domaine de la vente et du service (planification des ressources d'entreprise, gestion de la relation client) ;

b) dans différents emplacements, tels que :
   - sur une plateforme de traitement personnelle fournie à un individu (par exemple : cartes à puce, les smartphones et leurs applications, les compteurs intelligents, les dispositifs portables) ;
   - au sein de réseaux de transport et de collecte de données (par exemple : lorsque des données de localisation des téléphones mobiles sont créées de manière opérationnelle par le traitement du réseau, et qui peuvent être considérées comme des DCP dans certaines juridictions) ;
   - au sein de la propre infrastructure de traitement d'une organisation ;

- sur une plateforme de traitement tierce ;

c) pour la caractéristique de collecte, telle que :

- collecte de données unique (par exemple : lors de l'enregistrement à un service) ;
- collecte de données continue (par exemple : surveillance fréquente de paramètres de santé par des capteurs sur ou dans le corps d'une personne, collecte de données multiples à l'aide de cartes de paiement sans contact pour le paiement, systèmes de collecte de données de compteurs intelligents, etc.).

NOTE – La collecte de données continue peut contenir ou produire des DCP relatives au comportement, à la localisation et d'autres types de DCP. Dans ces cas, il est nécessaire d'envisager l'utilisation de mesures de protection des DCP qui permettent de gérer l'accès et la collecte sur la base du consentement et qui permettent à la personne concernée d'exercer un contrôle approprié sur cet accès et cette collecte.

NORME INTERNATIONALE
RECOMMANDATION UIT-T

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des données à caractère personnel

1 Domaine d'application

La présente Recommandation | Norme internationale établit des objectifs de mesure de sécurité, des mesures de sécurité et des lignes directrices pour la mise en œuvre des mesures de sécurité, afin de satisfaire aux exigences identifiées par une appréciation du risque et de l'impact liée à la protection des données à caractère personnel.

En particulier, la présente Recommandation | Norme internationale spécifie des lignes directrices basées sur l'ISO/IEC 27002, en tenant compte des exigences relatives au traitement des DCP qui peuvent être applicables dans le contexte du ou des environnements de risques de sécurité de l'information d'une organisation.

La présente Recommandation | Norme internationale s'applique à tous les types et toutes les tailles d'organisations agissant en tant que responsable de traitement de DCP (tel que défini dans l'ISO/IEC 29100), y compris les entreprises publiques et privées, les entités gouvernementales et les organisations à but non lucratif qui traitent des DCP.

2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui en est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations et Normes internationales sont sujettes à révision et les parties prenantes des accords fondés sur la présente Recommandation | Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de l'IEC et de l'ISO tiennent à jour les registres des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l´UIT tient à jour une liste des Recommandations de l´UIT-T en vigueur.

– ISO/IEC 27002:2013, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*.

– ISO/IEC 29100:2011, *Technologies de l'information — Techniques de sécurité — Cadre privé*.

3 Définitions et abréviations

3.1 Définitions

Pour les besoins de la présente Recommandation | Norme internationale, les termes et définitions donnés dans l'ISO/IEC 27000:2016, l'ISO/IEC 29100 et les suivants s'appliquent.

L'ISO *Online browsing platform*, l'IEC *Electropedia* et les *Termes et définitions* de l'UIT sont des bases de données terminologiques destinées à être utilisées en normalisation.

3.1.1 responsable de la confidentialité (**CPO)** membre de la direction qui est responsable de la protection des données à caractère personnel (DCP) dans une organisation

3.1.2 processus de désidentification processus consistant à supprimer l'association entre un ensemble de données d'identification et la personne concernée, à l'aide de techniques de désidentification

3.2 Abréviations

Pour les besoins de la présente Spécification, les abréviations suivantes s'appliquent.

BCR règle d'entreprise contraignante (Binding Corporate Rule)

CCTV télévision en circuit fermé (Closed-Circuit Television)

CPO	responsable de la confidentialité (Chief Privacy Officer)
PBD	protection de la vie privée dès la conception (Privacy By Design)
PDA	assistant numérique personnel (Personal Digital Assistant)
PET	technologie contribuant à la protection de la vie privée (Privacy Enhancing Technology)
PIA	évaluation de l'impact sur la vie privée (Privacy Impact Assessment)
DCP	données à caractère personnel
RFID	identification par radiofréquence (Radio Frequency Identification)
USB	bus série universel (Universal Serial Bus)

4 Vue d'ensemble

4.1 Objectif de protection des DCP

La présente Spécification fournit un ensemble de mesures de protection des DCP. L'objectif de la protection des DCP est de permettre aux organisations de mettre en place un ensemble de mesures de sécurité dans le cadre de leur programme global de protection des DCP. Elles peuvent être utilisées dans un cadre permettant de maintenir et d'améliorer la conformité aux lois et réglementations relatives à la vie privée, de gérer les risques sur la vie privée et de répondre aux attentes des personnes concernées, des régulateurs ou des clients, conformément aux principes de protection de la vie privée décrits dans l'ISO/IEC 29100.

4.2 Exigences liées à la protection des DCP

Il convient qu'une organisation identifie ses exigences en matière de protection des DCP. Les principes de protection de la vie privée de l'ISO/IEC 29100 s'appliquent à l'identification des exigences. Il existe trois sources principales d'exigences liées à la protection des DCP :

- exigences légales, statutaires, réglementaires et contractuelles liées à la protection des DCP, y compris, par exemple, les exigences en matière de DCP auxquelles une organisation, ses partenaires commerciaux, ses entrepreneurs et ses prestataires de services sont tenus de se conformer ;
- appréciation du risque (c'est-à-dire les risques de sécurité et les risques sur la vie privée) pour l'organisation et la personne concernée, en tenant compte de la stratégie et des objectifs métier globaux de l'organisation, par le biais d'une appréciation du risque ;
- politiques d'entreprise : une organisation peut également choisir volontairement d'aller au-delà des critères qui découlent des exigences précédentes.

Il convient que les organisations tiennent également compte des principes (c'est-à-dire les principes de protection de la vie privée définis dans l'ISO/IEC 29100), des objectifs et des exigences métier pour le traitement des DCP qui ont été élaborés pour soutenir leurs opérations.

Il convient que les mesures de protection des DCP (y compris les mesures de sécurité) soient choisies sur la base d'une appréciation du risque. Les résultats d'une évaluation de l'impact sur la vie privée (PIA), par exemple tel que spécifié dans l'ISO/IEC 29134, aideront à définir les actions de traitement appropriées et les priorités en matière de gestion des risques liés à la protection des DCP, et de mise en œuvre des mesures de sécurité identifiées destinées à contrer ces risques.

Une spécification de PIA telle que celle de l'ISO/IEC 29134 peut fournir des recommandations en matière de PIA, y compris des conseils relatifs à l'appréciation du risque, au plan de traitement du risque, à l'acceptation du risque et la revue des risques.

4.3 Mesures de sécurité

Une étude des risques sur la vie privée peut aider les organisations à identifier les risques spécifiques de violation des données à caractère personnel découlant d'un traitement illégal ou d'une atteinte aux droits de la personne concernée impliquée dans une opération envisagée. Il convient que les organisations identifient et mettent en œuvre des mesures de sécurité afin de traiter les risques identifiés par le processus d'impact des risques. Il convient que les mesures de sécurité et les traitements soient ensuite documentés, idéalement séparément dans un registre des risques séparé. Certains types de traitement de DCP peuvent requérir des mesures de sécurité spécifiques dont la nécessité n'apparaît qu'après une analyse attentive des opérations envisagées.

4.4 Sélection des mesures de sécurité

Les mesures de sécurité peuvent être sélectionnées à partir de la présente Spécification (ce qui inclut, par voie de référence, les mesures de sécurité de l'ISO/IEC 27002, créant ainsi un ensemble de mesures de sécurité de référence combinées). Si besoin, des mesures de sécurité peuvent être sélectionnées à partir d'autres ensembles de mesures de sécurité, ou de nouvelles mesures de sécurité peuvent être spécifiées en vue de satisfaire à des besoins spécifiques.

La sélection des mesures de sécurité dépend des décisions prises par l'organisation en fonction de ses critères pour les options de traitement du risque et de son approche de la gestion générale des risques, appliqués à l'organisation et, par le biais d'accords contractuels, à ses clients et fournisseurs. Il convient également de prendre en considération les lois et règlements nationaux et internationaux applicables.

La sélection et la mise en œuvre des mesures de sécurité dépendent également du rôle de l'organisation dans la fourniture d'infrastructures ou de services. De nombreuses organisations différentes peuvent être impliquées dans la fourniture d'infrastructures ou de services. Dans certains cas, les mesures de sécurité sélectionnées peuvent être propres à une organisation particulière. Dans d'autres cas, il peut y avoir des rôles partagés dans la mise en œuvre des mesures de sécurité. Il convient que les accords contractuels spécifient clairement les responsabilités en matière de protection des DCP de toutes les organisations impliquées dans la fourniture ou l'utilisation des services.

Les mesures de sécurité de la présente Spécification peuvent être utilisées comme référence par les organisations qui traitent des DCP et sont destinées à être applicables à toutes les organisations qui agissent comme responsable de traitement de DCP. Il convient que les organisations qui agissent comme sous-traitant de DCP le fassent conformément aux instructions du responsable de traitement de DCP. Il convient que les responsables de traitement de DCP s'assurent que leurs sous-traitants de DCP sont capables de mettre en œuvre toutes les mesures de sécurité nécessaires incluses dans leur accord de traitement des DCP, conformément à la finalité du traitement des DCP. Les responsables de traitement de DCP qui utilisent les services en nuage en tant que sous-traitants de DCP peuvent passer en revue l'ISO/IEC 27018 afin d'identifier les mesures de sécurité pertinentes à mettre en œuvre.

Les mesures de sécurité de la présente Spécification sont expliquées plus en détail aux Articles 5 à 18, et accompagnées de recommandations de mise en œuvre. La mise en œuvre peut être simplifiée si les exigences applicables à la protection des DCP ont été prises en compte dans la conception du système d'information, des services et des opérations de l'organisation. Cette prise en compte est un élément du concept souvent appelé « protection de la vie privée dès la conception » (PBD). De plus amples informations sur la sélection des mesures de sécurité et d'autres options de traitement du risque sont disponibles dans l'ISO/IEC 29134. Les autres références pertinentes sont indiquées dans la bibliographie.

4.5 Élaboration de lignes directrices propres à une organisation

La présente Spécification peut servir de base pour l'élaboration de lignes directrices propres à une organisation. Les mesures de sécurité et recommandations de la présente Spécification ne sont pas toutes applicables à toutes les organisations.

Par ailleurs, des mesures de sécurité et des lignes directrices supplémentaires ne figurant pas dans la présente Spécification peuvent être nécessaires. Lors de la rédaction de documents contenant des lignes directrices ou des mesures de sécurité supplémentaires, il peut être utile d'intégrer des références croisées aux articles de la présente Spécification, le cas échéant, afin de faciliter la vérification de la conformité par les auditeurs et les partenaires commerciaux.

4.6 Considérations relatives au cycle de vie

Les DCP ont un cycle de vie naturel, depuis leur création ou leur origine jusqu'à leur mise au rebut éventuelle (par exemple : destruction sécurisée), en passant par leur collecte, leur stockage, leur utilisation et leur transfert. La valeur des DCP et les risques auxquels elles sont exposées peuvent varier au cours de leur cycle de vie, mais la protection des DCP reste importante, dans une certaine mesure, à toutes les étapes et dans tous les contextes de leur cycle de vie.

Les systèmes d'information ont également des cycles de vie durant lesquels ils sont pensés, caractérisés, conçus, élaborés, testés, mis en œuvre, utilisés, entretenus et finalement retirés du service et mis au rebut. Il convient que la protection des DCP soit aussi prise en compte à chacune de ces étapes. La mise au point de nouveaux systèmes et les changements apportés aux systèmes existants donnent l'occasion aux organisations de mettre à jour et d'améliorer les mesures de sécurité et les mesures de protection des DCP en tenant compte des incidents réels survenus et des risques sur la vie privée et des risques pour la sécurité de l'information actuels et anticipés.

4.7 Structure de la présente Spécification

Le reste de la présente Spécification contient deux parties normatives principales.

La première partie de la présente Spécification, constituée des Articles 5 à 18, contient des recommandations de mise en œuvre supplémentaires et autres informations pour certaines mesures de sécurité existantes pertinentes décrites dans l'ISO/IEC 27002. Le format de cette partie utilise les intitulés et la numérotation des articles et paragraphes pertinents de l'ISO/IEC 27002 afin de permettre les références croisées avec cette Norme internationale.

La seconde partie contient un ensemble de mesures de sécurité spécifiques pour la protection des DCP spécifiées à l'Annexe A. Elle utilise le même format que l'ISO/IEC 27002, qui définit les objectifs des mesures de sécurité (texte dans un encadré) suivis d'une ou plusieurs mesures de sécurité qui peuvent être appliquées. La description des mesures de sécurité est structurée comme suit.

Mesure de sécurité

Le texte figurant sous cet intitulé définit la déclaration de mesure de sécurité spécifique pour atteindre l'objectif de la mesure de sécurité.

Recommandations de mise en œuvre pour la protection des DCP

Le texte figurant sous cet intitulé fournit des informations plus détaillées destinées à soutenir la mise en œuvre de la mesure de sécurité et atteindre les objectifs de la mesure de sécurité. Les recommandations fournies dans la présente Spécification peuvent ne pas être tout à fait adaptées ou suffisantes dans toutes les situations et peuvent ne pas répondre aux exigences spécifiques de l'organisation en matière de mesures de sécurité. Des mesures alternatives ou supplémentaires, ou d'autres formes de traitement du risque (évitement ou transfert des risques) peuvent donc être appropriées.

Autres informations pour la protection des DCP

Le texte figurant sous cet intitulé fournit des informations complémentaires qu'il peut être nécessaire de prendre en compte, tels que des éléments juridiques et des références à d'autres normes.

5 Politiques de sécurité de l'information

5.1 Orientations de la direction en matière de sécurité de l'information

5.1.1 Introduction

L'objectif spécifié en 5.1 de l'ISO/IEC 27002:2013 s'applique.

5.1.2 Politiques de sécurité de l'information

La mesure de sécurité 5.1.1 et les recommandations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent. Les recommandations supplémentaires suivantes s'appliquent également.

Recommandations de mise en œuvre pour la protection des DCP

Il convient que les politiques en matière de sécurité de l'information incluent des déclarations de mesures de sécurité appropriées pour la protection des DCP. Les détails relatifs à la protection des DCP sont disponibles au paragraphe 18.1.4 de l'ISO/IEC 27002:2013.

Lors de la conception, de la mise en œuvre et de la revue de la politique de sécurité de l'information, il convient que les organisations tiennent compte des exigences de protection de la vie privée décrites dans l'ISO/IEC 29100.

Il convient que les organisations spécifient les éléments de protection des DCP qui ne sont pas liés à la sécurité en tant que politique de protection de la vie privée séparée. Voir les recommandations au paragraphe A.2.

5.1.3 Revue des politiques de sécurité de l'information

La mesure de sécurité 5.1.2 et les recommandations de mise en œuvre associées spécifiées dans l'ISO/IEC 27002 s'appliquent.

6 Organisation de la sécurité de l'information

6.1 Organisation interne

6.1.1 Introduction

L'objectif spécifié en 6.1 de l'ISO/IEC 27002 s'applique.

6.1.2 Rôles et responsabilités liés à la sécurité de l'information

La mesure de sécurité 6.1.1 et les recommandations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent. Les recommandations supplémentaires suivantes s'appliquent également.

Recommandations de mise en œuvre pour la protection des DCP

Il est nécessaire que les rôles et les responsabilités en matière de protection des DCP soient clairement définis, correctement documentés et communiqués de façon appropriée. Notamment :

a) il convient qu'une personne de haut niveau clairement identifiée [parfois appelée responsable de la confidentialité (CPO)] au sein de l'organisation se voie attribuer la responsabilité de la protection des DCP ;

b) il convient qu'une ou plusieurs personnes clairement identifiées (c'est-à-dire la fonction de protection des DCP) se voient attribuer la responsabilité de coordination avec les fonctions de sécurité de l'information au sein de l'organisation ; et

c) il convient que des exigences de protection des DCP appropriées soient incluses dans la description de poste de toutes les personnes impliquées dans le traitement des DCP (y compris les utilisateurs et le personnel d'assistance).

Il convient que la fonction de protection des DCP établie travaille en étroite collaboration avec les autres fonctions traitant des DCP, la fonction de sécurité de l'information, qui met en œuvre les exigences de sécurité, ce qui inclut celles découlant des lois relatives à la protection des DCP, ainsi que la fonction juridique, qui aide à interpréter les lois, les règlements et les conditions contractuelles et à gérer les violations de données.

Il convient que l'organisation étudie la nécessité de créer (et si nécessaire qu'elle mette en place) un conseil ou un comité interfonctionnel composé de membres de haut niveau issus des fonctions qui traitent des DCP. La protection des DCP étant une fonction pluridisciplinaire, un tel groupe peut aider à identifier de manière proactive les opportunités d'amélioration, à identifier les nouveaux risques et les domaines dans lesquels mener des PIA, à planifier des mesures préventives, des mesures de détection et de réaction face à toute violation, etc. Il est recommandé qu'un tel groupe se réunisse périodiquement et soit présidé par la personne responsable de la protection des DCP telle qu'identifiée au point a).

Il convient que le responsable de traitement de DCP exige de son ou ses sous-traitants de DCP qu'ils désignent un interlocuteur chargé de répondre aux questions concernant le traitement des DCP dans le cadre du contrat de traitement des DCP.

Il convient que les personnes chargées des fonctions de protection des DCP rendent compte à un CPO afin de garantir qu'elles disposent de l'autorité suffisante pour assumer leurs responsabilités.

6.1.3 Séparation des tâches

La mesure de sécurité 6.1.2 et les recommandations de mise en œuvre associées spécifiées dans l'ISO/IEC 27002 s'appliquent. Les recommandations supplémentaires suivantes s'appliquent également.

Recommandations de mise en œuvre pour la protection des DCP

Il convient que les tâches et domaines de responsabilité en matière de protection des DCP soient indépendants de ceux relatifs à la sécurité de l'information. Tout en reconnaissant l'importance de la sécurité de l'information pour la protection des DCP, il est important que les tâches et les domaines de responsabilité en matière de sécurité et de protection des DCP soient aussi indépendants les uns des autres que possible. Si cela est nécessaire ou utile, dans l'intérêt de la protection des DCP, il convient de faciliter la coordination et la coopération entre les personnes responsables de la sécurité de l'information et de la protection des DCP.

Il convient que les organisations adoptent le principe de séparation des tâches lors de l'attribution des droits d'accès pour le traitement des DCP, particulièrement pour tout traitement identifié comme présentant un risque élevé.

Il convient que l'accès aux DCP en cours de traitement et l'accès aux fichiers journaux concernant ce traitement soient des tâches séparées.

Il convient que l'accès aux informations relatives à la collecte des DCP destiné à répondre aux demandes des personnes concernées soit séparé de toutes les autres formes d'accès aux DCP. Il convient que l'accès soit limité aux personnes dont les tâches incluent le fait de répondre aux demandes des personnes concernées.

6.1.4 Relations avec les autorités

La mesure de sécurité 6.1.3 et les recommandations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent. Les recommandations supplémentaires suivantes s'appliquent également.

Recommandations de mise en œuvre pour la protection des DCP

Le cas échéant, il convient que les organisations mettent en place des procédures précisant quand et par qui il convient que les autorités (y compris les autorités chargées de la protection des données) soient contactées, par exemple pour signaler des violations de données à caractère personnel ou communiquer des détails relatifs au traitement.

6.1.5 Relations avec des groupes de travail spécialisés

La mesure de sécurité 6.1.4 et les recommandations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent.

6.1.6 La sécurité de l'information dans la gestion de projet

La mesure de sécurité 6.1.5 et les recommandations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent. Les recommandations supplémentaires suivantes s'appliquent également.

Recommandations de mise en œuvre pour la protection des DCP

Il convient que tout lancement de nouveau projet déclenche au minimum une analyse du seuil afin de déterminer s'il est nécessaire de réaliser une PIA. Il est à noter que le terme projet couvre tous les incidents où une organisation met en œuvre ou modifie une technologie, un produit, un service, un programme, un système d'information, un processus ou un projet nouveau ou existant.

Des recommandations supplémentaires sont disponibles dans la PIA spécifiée dans l'ISO/IEC 29134.

6.2 Appareils mobiles et télétravail

6.2.1 Introduction

L'objectif spécifié en 6.2 de l'ISO/IEC 27002:2013 s'applique.

6.2.2 Politique en matière d'appareils mobiles

La mesure de sécurité 6.2.1 et les recommandations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent. Les recommandations supplémentaires suivantes s'appliquent également.

Recommandations de mise en œuvre pour la protection des DCP

Il convient que les organisations limitent strictement l'accès aux DCP à partir de dispositifs portables et mobiles, tels que les ordinateurs portables, les téléphones portables, les dispositifs à bus série universel (USB) et les assistants numériques personnels (PDA), qui peuvent généralement être exposés à un risque plus élevé que les dispositifs non portables (par exemple : ordinateurs de bureau dans les locaux de l'organisation), en fonction de l'appréciation du risque.

Il convient que les organisations limitent strictement l'accès distant aux DCP et, dans les cas où l'accès distant serait inévitable, s'assurent que les communications pour l'accès distant sont chiffrées, que les messages sont authentifiés et que leur intégrité est protégée.

6.2.3 Télétravail

La mesure de sécurité 6.2.2 et les recommandations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent.

7 Sécurité des ressources humaines

7.1 Avant l'embauche

7.1.1 Introduction

L'objectif spécifié en 7.1 de l'ISO/IEC 27002:2013 s'applique.

7.1.2 Sélection des candidats

La mesure de sécurité 7.1.1 et les recommandations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent.

7.1.3 Termes et conditions d'embauche

La mesure de sécurité 7.1.2 et les recommandations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent.

7.2 Pendant la durée du contrat

7.2.1 Introduction

L'objectif spécifié en 7.2 de l'ISO/IEC 27002:2013 s'applique.

7.2.2 Responsabilités de la direction

La mesure de sécurité 7.2.1 et les recommandations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent.

7.2.3 Sensibilisation, apprentissage et formation à la sécurité de l'information

La mesure de sécurité 7.2.2 et les recommandations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent. Les recommandations supplémentaires suivantes s'appliquent également.

Recommandations de mise en œuvre pour la protection des DCP

Il convient de mettre en place des mesures pour sensibiliser le personnel concerné aux conséquences possibles pour le responsable de traitement de DCP (par exemple : conséquences juridiques, perte d'activités ou détérioration de l'image de marque et de la réputation), pour le membre du personnel (par exemple : conséquences disciplinaires) et pour la personne concernée (par exemple : conséquences physiques, matérielles et émotionnelles) d'une violation des règles et procédures de protection de la vie privée ou de sécurité, en particulier celles relatives au traitement des DCP.