Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1058

(03/2017)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité de l'information et des réseaux – Gestion de la sécurité

Technologie de l'information – Techniques de sécurité – Code de bonne pratique pour la protection des informations d'identification personnelle

Recommandation UIT-T X.1058

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	**X.1050–X.1069**
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
Recommandations relatives aux infrastructures de clé publique	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents (ITS)	X.1370–X.1379
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

NORME INTERNATIONALE ISO/CEI 29151
RECOMMANDATION UIT-T X.1058

Technologie de l'information – Techniques de sécurité – Code de bonne pratique pour la protection des informations d'identification personnelle

Résumé

Le nombre d'organisations chargées de traiter des Informations d'identification personnelle (IIP) ne cesse de croître, tout comme le volume de données que ces organisations doivent gérer. Parallèlement, la société exige toujours plus de protection de ces informations et de sécurité des données personnelles. Face au nombre croissant d'atteintes sophistiquées à des données personnelles, un certain nombre de pays ont entrepris de renforcer leur législation.

La présente spécification définit un certain nombre de buts et de mesures de contrôle, et contient des directives permettant de mettre ces mesures en œuvre. Elle vise à répondre aux besoins recensés dans le cadre des évaluations de risque et d'impact effectuées dans le domaine de la protection des IIP. En particulier, la présente spécification définit des directives qui sont fondées sur la norme ISO/CEI 27002, compte tenu des besoins de traitement des IIP et pouvant être pertinents au regard des risques de sécurité pesant sur les informations d'une organisation particulière.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T X.1058	2017-03-30	17	11.1002/1000/13182

Mots clés

Code de bonne pratique, contrôle, conseil de mise en oeuvre, IIP

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas des renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Introduction

Le nombre d'organisations chargées de traiter des informations d'identification personnelle (IIP) ne cesse de croître, tout comme le volume de données que ces organisations doivent gérer. Parallèlement, la société exige toujours plus de protection de ces informations et de sécurité des données personnelles. Face au nombre croissant d'atteintes sophistiquées à des données personnelles, un certain nombre de pays ont entrepris de renforcer leur législation.

Alors que ces atteintes se multiplient, les organisations qui recueillent ou traitent les IIP vont avoir de plus en plus besoin de conseils sur la manière de protéger ces informations pour réduire les risques d'atteinte et d'atténuer l'incidence de ces atteintes sur l'organisation ou la personne qui en est victime. La présente spécification fournit précisément ce type de conseils.

La présente spécification contient des conseils destinés aux contrôleurs des IIP et couvre un large éventail de mesures sur la sécurité de l'information et la protection des IIP. Ces mesures sont fréquemment employées par des organisations très diverses chargées de protéger des informations. Les autres éléments des normes ISO/CEI, qui sont énumérés ci-après, contiennent des conseils ou des prescriptions sur d'autres aspects du processus général de protection des IIP:

- La norme ISO/CEI 27001 définit un système de gestion de la sécurité de l'information ainsi que ses besoins connexes. Elle pourrait servir de fondement à la protection des IIP.
- La norme ISO/CEI 27002 établit des directives en matière de normes organisationnelles relatives à la sécurité de l'information, ainsi que des bonnes pratiques de gestion de la sécurité de l'information. Elle porte notamment sur le choix, la mise en œuvre et la gestion de mesures de sécurité, compte tenu des risques pesant sur la sécurité de l'information d'une organisation.
- La norme ISO/CEI 27009 définit les besoins découlant de l'application de la norme ISO/CEI 27001 dans un secteur donné (sujet, domaine d'application ou secteur du marché). Elle indique comment compléter la liste de besoins établie dans la norme ISO/CEI 27001, comment affiner ces besoins et comment ajouter une ou plusieurs mesures de contrôle à celles qui sont déjà prévues dans l'Annexe A de la norme ISO/CEI 27001.
- La norme ISO/CEI 27018 contient des conseils pour les prestataires de services chargés de traiter des IIP qui proposent des services en nuage.
- La norme ISO/CEI 29134 établit des directives permettant de recenser, d'analyser et d'évaluer les risques menaçant des données personnelles, tandis que les normes ISO/CEI 27001 et ISO/CEI 27005 constituent ensemble une méthode de recensement, d'analyse et d'évaluation des risques de sécurité.

Il convient de choisir les mesures de contrôle en fonction des risques recensés au terme d'une analyse de risque afin de mettre en place un système de contrôle global et cohérent. Ces mesures devraient être adaptées au contexte du traitement particulier des IIP.

La présente spécification comporte deux parties: 1) le corps principal du texte qui va des paragraphes 1 à 18, et 2) une annexe normative. Cette structure est conforme à la pratique courante d'extension de la norme ISO/CEI 27002 à un secteur particulier.

La structure du texte principal de la présente spécification, y compris le titre des paragraphes, reprend celle du texte principal de la recommandation ISO/CEI 27002. L'introduction et les paragraphes 1 à 4 définissent le contexte d'emploi de la présente spécification. Les paragraphes 5 à 18 ont le même titre que ceux de la norme ISO/CEI 27002, compte tenu du fait que la présente spécification s'inspire des conseils fournis dans cette norme en y ajoutant des mesures de contrôle propres à la protection des IIP. Beaucoup de mesures prévues dans la norme ISO/CEI 27002 n'ont pas eu besoin d'être étendues pour pouvoir être appliquées aux contrôleurs des IIP. Toutefois, dans certains cas, il a été nécessaire d'ajouter des conseils supplémentaires sur la mise en œuvre de ces mesures; ces conseils apparaissent alors sous le titre (et le numéro de paragraphe) correspondants de la norme ISO/CEI 27002.

On trouvera dans l'annexe normative de nombreuses mesures de contrôle qui visent spécifiquement à protéger les IIP et sont complémentaires aux mesures prévues dans la norme ISO/CEI 27002. Ces nouvelles mesures de protection, ainsi que les conseils qui les accompagnent, sont répartis en 12 catégories correspondant à la politique de sécurité et aux onze principes relatifs à la vie privée qui sont énoncés dans la norme ISO/CEI 29100:

- Consentement et choix;
- Légitimité et définition du but;
- Limites du recueil d'informations;
- Réduction des informations au minimum;
- Limites d'utilisation, de conservation et de divulgation;
- Exactitude et qualité;
- Ouverture, transparence et note d'information;
- Participation et accès de l'entité principale;

– Responsabilité;
– Sécurité des informations; et
– Respect de la vie privée.

On trouvera dans la Figure 1 ci-après une description de la relation entre la présente spécification et les normes ISO/CEI.

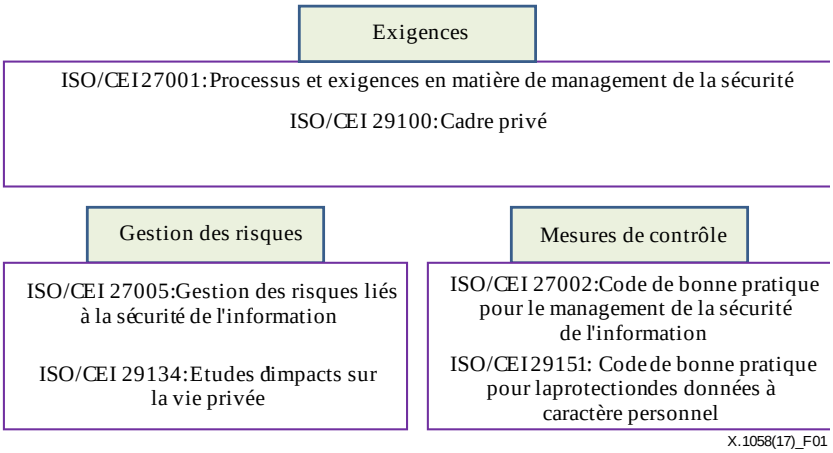

Figure 1 – Relation entre la présente spécification et les normes ISO/CEI

La présente spécification contient des directives fondées sur la norme ISO/CEI 27002 qui visent à adapter les dispositions de celle-ci afin de répondre aux besoins de protection de la confidentialité des IIP:

a) Dans différents domaines de traitement, notamment:
   – les services publics en nuage;
   – les applications de réseaux sociaux;
   – les appareils domestiques connectés à l'Internet;
   – la recherche et l'analyse;
   – le ciblage d'IIP à des fins de publicité et d'autres fins analogues;
   – les programmes d'analyse des grands volumes de données;
   – le traitement des données relatives à l'emploi;
   – la gestion des ventes et des services (planification des ressources de l'entreprise, gestion de la relation client).

b) Sur différentes plates-formes de traitement, notamment:
   – sur une plate-forme de traitement personnelle fournie à une personne (comme une carte à puce, un téléphone intelligent équipé d'applications, un compteur électrique intelligent, des dispositifs à porter sur soi);
   – dans des réseaux de transmission et de recueil de données (par exemple lorsque l'administration d'un réseau permet de localiser un téléphone mobile, cette information pouvant être considérée comme une IIP sous certaines juridictions);
   – dans l'infrastructure de traitement propre à une organisation;
   – sur la plate-forme de traitement d'un tiers.

c) Pour certains types de recueil de données, notamment:
   – un recueil de données n'intervenant qu'une seule fois (par exemple lors de la création d'un compte d'accès à un service);
   – le recueil permanent de données (par exemple dans le cadre de la surveillance de la santé, où des capteurs situés sur ou dans le corps recueillent fréquemment des informations, ou encore les nombreuses opérations de recueil de données intervenant lorsqu'on emploie une carte de paiement sans contact, ou des systèmes de recueil de données par des compteurs électriques intelligents, etc.).

NOTE – Les opérations permanentes de recueil de données peuvent contenir ou produire des IIP concernant le comportement ou l'emplacement des personnes, ainsi que d'autres types de données à caractère personnel. Dans ces cas, il convient d'envisager des mesures de contrôle de ces IIP, qui permettraient de gérer l'accès et le recueil de ces informations sur la base du consentement, et permettraient en outre à l'entité principale des IIP de surveiller comme il convient cet accès et ce recueil.

NORME INTERNATIONALE
RECOMMANDATION UIT-T

Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la protection des informations d'identification personnelle

1 Domaine d'application

La présente Recommandation | Norme internationale définit un certain nombre de buts et de mesures de contrôle, et contient des directives permettant de mettre ces mesures en œuvre. Elle vise à répondre aux besoins recensés dans le cadre des évaluations de risque et d'impact effectuées dans le domaine de la protection des informations d'identification personnelle (IIP).

Certaines de ces directives, qui sont fondées sur la norme ISO/CEI 27002, tiennent notamment compte des besoins de traitement des IIP et peuvent être pertinentes au regard des risques de sécurité pesant sur les informations d'une organisation particulière.

La présente Recommandation | Norme internationale s'applique aux organisations de tout type et de toute taille ayant pour mission de contrôler les IIP (au sens de la norme ISO/CEI 29100), qu'il s'agisse d'entreprises publiques ou privées, d'organismes publics ou d'ONG, dès lors qu'elles effectuent un traitement des IIP.

2 Références normatives

Les Recommandations et les Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes Recommandations et Normes sont sujettes à révision, et les parties prenantes aux 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 la CEI et de l'ISO possèdent le registre 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 actuellement en vigueur.

- ISO/CEI 27002:2013, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information*.
- ISO/CEI 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 figurant dans les normes ISO/CEI 27000:2016, ISO/CEI 29100 et les définitions suivantes s'appliquent.

La plate-forme de navigation en ligne de l'ISO, Electropedia de la CEI et la base de données des termes et définitions de l'UIT sont les bases de données terminologiques à utiliser dans le cadre des travaux de normalisation.

3.1.1 directeur des données personnelles (DDP): cadre supérieur responsable de la protection des données d'identification personnelle (IIP) dans une organisation.

3.1.2 désidentification: opération consistant à supprimer l'association entre un ensemble de données permettant l'identification et l'entité à qui appartiennent ces données en utilisant des techniques de désindentification.

3.2 Abréviations

Aux fins de la présente spécification, les abréviations suivantes sont employées:

ANP Assistant numérique personnel
CCTV Télévision en circuit fermé
DDP Directeur des données personnelles
EIVP Evaluation des incidences sur la vie privée

IIP	Informations d'identification personnelle
PVPC	Protection de la vie privée dès la conception
REC	Règles d'entreprise contraignantes
RFID	Identification par radiofréquences
TPVP	Technologie de protection de la vie privée
USB	Bus série universel

4 Aperçu général

4.1 But de la protection des IIP

La présente spécification contient un ensemble de mesures de contrôle destinées à protéger les informations d'identification personnelle (IIP). Elle a pour but d'aider les organisations à mettre en place un ensemble de mesures de contrôle nécessaires dans le cadre de leur programme général de protection des IIP. Ces mesures peuvent être appliquées pour assurer et améliorer la conformité de l'organisation à la législation et aux réglementations en matière de données personnelles, ainsi que pour gérer les risques concernant les données personnelles et pour répondre aux attentes des entités principales des IIP, des législateurs ou des clients, conformément aux principes en matière de données personnelles énoncés dans la norme ISO/CEI 29100.

4.2 Besoins en matière de protection des IIP

Toute organisation devrait recenser ses besoins en matière de protection des IIP. Les principes relatifs à la vie privée énoncés dans la norme ISO/CEI 29100 peuvent être appliqués pour ce faire. Il existe trois grandes sources de besoins dans ce domaine:

- Les besoins juridiques, statutaires, réglementaires et contractuels liés à la protection des IIP, notamment, par exemple, les exigences auxquelles les organisations, leurs partenaires commerciaux, leurs sous-traitants et leurs fournisseurs de services doivent se conformer.
- L'évaluation des risques (c'est-à-dire des risques de sécurité et des risques liés aux données personnelles) du point de vue de l'organisation et de l'entité principale des IIP, compte tenu de la stratégie commerciale et des buts généraux de l'organisation.
- Les politiques d'entreprise: une organisation peut volontairement choisir d'aller au-delà des critères découlant des besoins déjà recensés.

Les organisations devraient aussi tenir compte des principes (c'est-à-dire des principes de protection de la vie privée établis par la norme ISO/CEI 29100), des buts et des besoins commerciaux qui ont été définis à l'appui de ses activités dans le domaine du traitement des IIP.

Les mesures de protection des IIP (et en particulier les mesures de sécurité) devraient être choisies au regard des résultats de l'évaluation des risques. Les résultats d'une évaluation des incidences sur la vie privée (EIVP) comme celle qui est décrite dans la norme ISO/CEI 29134 peuvent contribuer à orienter et à définir le traitement adéquat et les priorités concernant la gestion des risques liés à la protection des IIP, et la mise en place des mesures de contrôle choisies pour se prémunir contre ces risques.

Le cahier des charges d'une EIVP tel que défini dans la norme ISO/CEI 29134 peut faciliter ces travaux; il contient notamment des conseils en matière d'évaluation des risques, un plan de traitement des risques et des indications sur l'acceptation et la révision des risques.

4.3 Mesures de contrôle

L'évaluation des risques concernant les données personnelles peut aider une organisation à recenser les risques particuliers liés à des violations de confidentialité découlant du traitement illicite ou de la restriction des droits de l'entité principale des IIP dans un projet particulier. Les organisations devraient choisir et mettre en œuvre les mesures de contrôle visant à remédier aux risques ainsi recensés. Les mesures de contrôle et les solutions devraient ensuite être documentées; dans l'idéal, cette documentation devrait être effectuée de manière séparée et dans un dossier distinct. Certains types de solutions peuvent nécessiter des mesures particulières, dont le besoin peut n'apparaître qu'au terme d'une analyse minutieuse du projet envisagé.

4.4 Choix des mesures de contrôle

Les mesures de contrôle peuvent être choisies parmi celles qui sont proposées dans la présente spécification (qui comprend aussi, par référence, les mesures de la norme ISO/CEI 27002 et offre par conséquent un ensemble de mesures mixtes). Au besoin, on peut également choisir des mesures parmi d'autres ensembles, ou en concevoir de nouvelles pour répondre à des besoins particuliers.

Le choix des mesures dépend des décisions que l'organisation va prendre en fonction des options dont elle dispose pour lutter contre les risques, et de sa stratégie générale de gestion des risques. Ces mesures seront appliquées à l'organisation et, par le biais d'accord contractuels, à ses clients et ses fournisseurs. Elles doivent par ailleurs être conformes à toute la législation et la réglementation applicables aux échelles nationale et internationale.

Le choix et la mise en œuvre des mesures de contrôle dépendent aussi du rôle que l'organisation joue dans la mise à disposition d'infrastructures ou la prestation de services. De nombreuses organisations peuvent intervenir dans ces deux types d'activités. Dans certains cas, les mesures peuvent être propres à une organisation particulière, tandis que dans d'autres, plusieurs organisations peuvent partager les mêmes rôles dans la mise en œuvre des mesures. Les accords contractuels devraient définir clairement les responsabilités de protection des IIP de toutes les organisations concernées dans la prestation ou l'utilisation de ces services.

Les mesures de contrôle proposées dans la présente spécification peuvent servir de point de référence aux organisations qui sont amenées à traiter des IIP, et elles sont applicables par toute organisation ayant pour mission de contrôler des IIP. Les prestataires de services chargés de traiter des IIP devraient s'acquitter de leurs tâches conformément aux instructions du contrôleur des IIP. Ce dernier devrait s'assurer que les prestataires sont en mesure de mettre en œuvre toutes les mesures de contrôle prévues dans leur accord de traitement des IIP, conformément à l'objectif de traitement de ces informations. Si les contrôleurs des IIP utilisent des services en nuage pour le traitement des IIP, ils devraient aussi examiner la norme ISO/CEI 27018 pour déterminer quelles mesures de contrôle doivent être appliquées.

Les mesures figurant dans la présente spécification sont exposées plus en détail dans les paragraphes 5 à 18, avec un certain nombre de conseils sur leur mise en œuvre. Celle-ci peut être simplifiée si les besoins de protection des IIP ont été pris en compte dès la conception du système d'information, des services et du fonctionnement de l'organisation. Cette démarche fait partie d'une notion souvent appelée "protection de la vie privée dès la conception" (PVPC). On trouvera de plus amples informations sur le choix des mesures de contrôle et d'autres méthodes de gestion des risques dans la norme ISO/CEI 29134. La bibliographie comporte en outre d'autres documents de référence pertinents.

4.5 Elaboration de directives propres à l'organisation

La présente spécification peut servir de point de départ pour élaborer des directives propres à une organisation donnée. Néanmoins, toutes les mesures et les conseils qu'elle présente ne sont pas applicables à toutes les organisations.

Au demeurant, certaines mesures de contrôle ou directives supplémentaires qui ne figurent pas dans la présente spécification peuvent aussi se révéler nécessaires. Lorsque des documents contenant des directives ou des mesures de contrôle supplémentaires sont élaborés, il peut être utile de les citer en référence dans la présente spécification, le cas échéant, afin que les auditeurs et les partenaires commerciaux puissent plus facilement effectuer leurs vérifications de conformité.

4.6 Eléments concernant le cycle de vie

Les IIP ont un cycle de vie naturel, qui commence à leur création ou leur origine, passe par le recueil, le stockage, l'utilisation et la transmission et s'achève par leur suppression (par exemple au moyen d'un système de destruction sécurisé). La valeur des IIP et les risques qui lui correspondent varient au cours de ce cycle de vie, mais la protection de ces informations reste importante, à un degré variable, à toutes les étapes et dans tous les contextes du cycle de vie.

Les systèmes d'information ont également un cycle de vie au cours duquel ils sont conçus, spécifiés, élaborés, développés, testés, mis en œuvre, exploités, maintenus et finalement mis hors service et éliminés. La protection des IIP doit également être prise en compte à chacune de ces étapes. A l'occasion de la création d'un nouveau système d'information ou de la modification d'un système existant, les organisations peuvent mettre à jour et améliorer leurs mesures de sécurité ainsi que leurs mesures de protection des IIP en tenant compte des incidents réellement survenus et des risques actuels et futurs pesant sur la sécurité des données personnelles.

4.7 Structure de la présente spécification

Le reste de la présente spécification contient deux grandes parties normatives.

La première, qui va des paragraphes 5 à 18, contient des conseils supplémentaires sur la mise en œuvre de certaines mesures de contrôle figurant dans la norme ISO/CEI 27002, ainsi que d'autres informations relatives à ces mesures. Le

format de cette partie reprend les titres et la numérotation des paragraphes de la norme ISO/CEI 27002 pour que le lecteur puisse facilement se reporter à celle-ci.

La seconde partie du document contient un ensemble de mesures propres à la protection des IIP définies dans l'Annexe A. Elle suit également le format de la norme ISO/CEI 27002, c'est-à-dire qu'elle contient une définition des objectifs de chaque mesure (dans un encadré) suivie de l'indication d'une ou plusieurs mesures pouvant être appliquées. La description d'une mesure de contrôle est structurée de la manière suivante:

Mesures de contrôle

Cette partie contient une définition des mesures de contrôle qui permettront d'atteindre l'objectif spécifié.

Conseils de mise en œuvre de la protection des IIP

Cette partie contient des informations plus détaillées sur la mise en œuvre des mesures de contrôle et la manière d'atteindre les objectifs de protection. Les conseils fournis dans la présente spécification ne seront peut-être pas entièrement pertinents ou suffisants dans toutes les situations, et peuvent ne pas répondre aux besoins de contrôle propres à l'organisation. Il conviendra donc peut-être de prendre des mesures différentes ou supplémentaires, ou de gérer les risques de toute autre manière (par exemple pour les éviter ou les déplacer).

Autres informations concernant la protection des IIP

Cette partie contient des informations supplémentaires qui peuvent être utiles, notamment dans le domaine juridique, ainsi que 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

Le but défini au § 5.1 de la norme ISO/CEI 27002:2013 s'applique.

5.1.2 Politiques de sécurité de l'information

Les mesures prévues au § 5.1.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Les politiques de sécurité de l'information devraient comprendre des instructions pertinentes sur les mesures de sécurité à prendre pour la protection des IIP. Des informations détaillées sur la protection des IIP sont disponibles au § 18.1.4 de la norme ISO/CEI 27002:2013.

Les organisations qui entreprennent de concevoir, mettre en œuvre et réviser leur politique de sécurité de l'information devraient examiner les prescriptions sur la protection des données personnelles figurant dans la norme ISO/CEI 29100.

Les organisations devraient spécifier les éléments de la protection des IIP ne se rapportant pas à la sécurité sous la forme d'une politique de sécurité séparée. Voir les conseils donnés au § A.2.

5.1.3 Revue des politiques de sécurité de l'information

Les mesures prévues au § 5.1.2 et les conseils de mise en œuvre connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

6 Organisation de la sécurité de l'information

6.1 Organisation interne

6.1.1 Introduction

Le but défini au § 6.1 de la norme ISO/CEI 27002 s'applique.

6.1.2 Fonctions et responsabilités liées à la sécurité de l'information

Les mesures prévues au § 6.1.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Les fonctions et responsabilités en matière de protection des IIP doivent être clairement définies, correctement documentées et communiquées de manière adéquate. Plus précisément:

a) la responsabilité de la protection des IIP devrait être attribuée à un cadre supérieur clairement désigné [parfois appelé Directeur des données personnelles (DDP)] au sein de l'organisation;

b) la responsabilité de la coordination des fonctions de sécurisation de l'information (c'est-à-dire la fonction de protection des IIP) devrait être attribuée à une ou plusieurs personnes clairement désignées au sein de l'organisation; et

c) des exigences en matière de protection des IIP devraient figurer dans la description de poste de toutes les personnes intervenant dans le processus des IIP (y compris les utilisateurs et le personnel d'appui).

La personne responsable de la protection des IIP devrait travailler en étroite collaboration avec les autres responsables du traitement des IIP et de la sécurité de l'information, ainsi qu'avec les personnes chargées de mettre en œuvre les prescriptions de sécurité (notamment celles qui découlent de la législation en matière de protection des IIP) et les personnes qui contribuent à interpréter la législation, la réglementation et les conditions contractuelles, ou qui sont chargées de gérer les cas d'atteinte à des données personnelles.

L'organisation devrait déterminer l'opportunité d'établir un conseil ou un comité transversal composé de hauts responsables de services chargés de traiter des IIP. La protection de ces données étant une fonction pluridisciplinaire, un tel groupe peut contribuer activement à recenser les pistes d'amélioration, les nouveaux risques et les domaines dans lesquels il convient d'effectuer des EIVP, ainsi qu'à mettre en place des mesures préventives, des mesures de détection et des mesures de réaction en cas d'atteinte à des données personnelles, etc. Ce groupe devrait se réunir régulièrement et être dirigé par la personne chargée de la protection des IIP, comme indiqué au point a).

Le contrôleur des IIP devrait prier les prestataires chargés de traiter les IIP de désigner un interlocuteur auquel il pourrait poser toute question concernant le traitement des IIP effectué au titre du contrat de traitement de ces données.

Les personnes chargées de protéger les IIP devraient rendre compte au DDP, ce qui leur conférerait l'autorité requise pour s'acquitter de leurs tâches.

6.1.3 Séparation des tâches

Les mesures prévues au § 6.1.2 et les conseils de mise en œuvre connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

En matière de protection des IIP, les tâches et les domaines de responsabilité devraient être indépendants de ceux qui concernent la sécurité de l'information. Si l'importance de celle-ci est incontestable au regard de la protection des IIP, il est essentiel de distinguer les tâches et les domaines de responsabilité de ces deux secteurs. Il est néanmoins recommandé de faciliter la coordination et la coopération entre les personnes chargées de la sécurité de l'information et de la protection des IIP, pour autant que cela soit nécessaire ou utile.

Les organisations devraient adopter le principe du cloisonnement des tâches pour attribuer des droits d'accès au personnes chargées de traiter les IIP, et notamment à celles qui effectuent des traitements jugés à haut risque.

L'accès aux IIP en cours de traitement comme l'accès aux journaux consignant ce traitement devraient être des tâches séparées.

L'accès aux informations concernant un recueil d'IIP effectué pour répondre à des demandes des entités principales de ces IIP devrait être traité différemment de toutes les autres formes d'accès aux IIP. Il devrait être limité aux seules personnes officiellement chargées de répondre à ces demandes.

6.1.4 Relations avec les autorités

Les mesures prévues au § 6.1.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Le cas échéant, les organisations devraient disposer de procédures permettant de préciser quand et par qui les autorités (notamment celles qui sont chargées de protéger les données) devraient être contactées, par exemple pour signaler une atteinte à des données personnelles ou pour communiquer le détail d'un traitement.

6.1.5 Relations avec des groupes de travail spécialisés

Les mesures prévues au § 6.1.4 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

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

Les mesures prévues au § 6.1.5 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Lors du lancement de tout nouveau projet, il convient de déterminer s'il est nécessaire de mener une EIVP. (A noter que le terme "projet" s'entend de toute activité dans le cadre de laquelle une organisation met en place ou modifie une technologie, un produit, un service, un programme, un système d'information, un processus ou un projet nouveau ou existant.)

On trouvera des conseils supplémentaires dans l'EIVP spécifiée dans la norme ISO/CEI 29134.

6.2 Appareils mobiles et télétravail

6.2.1 Introduction

Le but défini au § 6.2 de la norme ISO/CEI 27002 s'applique.

6.2.2 Politique en matière d'appareil mobile

Les mesures prévues au § 6.2.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient imposer des limites strictes à l'accès aux IIP depuis des appareils portables et mobiles tels que des ordinateurs portables, des téléphones mobiles, des clés USB ou des assistants numériques personnels, qui risquent généralement d'être exposés à des risques plus élevés que des appareils non portables (comme un ordinateur de bureau situé dans les locaux de l'organisation), en fonction de l'évaluation des risques.

Les organisations devaient également limiter de manière stricte l'accès à distance aux IIP, et si cet accès est indispensable, elles devraient s'assurer que les communications avec le dispositif d'accès à distance sont chiffrées, que les messages sont authentifiés et que l'intégrité des données est protégée.

6.2.3 Télétravail

Les mesures prévues au § 6.2.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

7 La sécurité des ressources humaines

7.1 Avant l'embauche

7.1.1 Introduction

Le but défini au § 7.1 de la norme ISO/CEI 27002:2013 s'applique.

7.1.2 Sélection des candidats

Les mesures prévues au § 7.1.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

7.1.3 Termes et conditions de l'embauche

Les mesures prévues au § 7.1.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

7.2 Pendant la durée du contrat

7.2.1 Introduction

Le but indiqué au § 7.2 de la norme ISO/CEI 27002:2013 s'applique.

7.2.2 Responsabilités de la direction

Les mesures prévues au § 7.2.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

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

Les mesures prévues au § 7.2.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Il convient de prendre des mesures pour sensibiliser le personnel concerné aux conséquences que la mise en œuvre d'une protection des IIP peut avoir pour le contrôleur des IIP (par exemple des conséquences judiciaires, la perte de marchés ou une atteinte à sa marque ou sa réputation), pour les membres du personnel (par exemple des conséquences disciplinaires) et pour l'entité principale des IIP (par exemple des conséquences physiques, matérielles ou émotionnelles) en cas d'atteinte à des données personnelles ou de violation des règles et procédures de sécurité, notamment celles qui concernent le traitement des IIP.

Comme dans le domaine de la sécurité de l'information, les organisations devraient mettre en place des séances de formation et de sensibilisation à la protection et au traitement des IIP.

7.2.4 Processus disciplinaire

Les mesures prévues au § 7.2.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

En cas d'atteinte à des données personnelles, les organisations devraient mettre en place des mesures disciplinaires officielles, les communiquer clairement aux personnes concernées et les appliquer systématiquement.

7.3 Rupture, terme et modification du contrat de travail

7.3.1 Introduction

Le but indiqué au § 7.3 de la norme ISO/CEI 27002:2013 s'applique.

7.3.2 Achèvement ou modification des responsabilités associées au contrat de travail

Les mesures prévues au § 7.3.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

8 Gestion des actifs

8.1 Responsabilités relatives aux actifs

8.1.1 Introduction

Le but indiqué au § 8.1 de la norme ISO/CEI 27002:2013 s'applique.

8.1.2 Inventaire des actifs

Les mesures prévues au § 8.1.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient établir, alimenter et tenir à jour un inventaire des actifs en se servant par exemple des informations fournies dans les rapports d'évaluation de l'impact sur la vie privée (rapports EIVP), s'ils existent,

conformément à la norme ISO/CEI 29134. Cet inventaire devrait couvrir tous les actifs d'IIP et l'ensemble des systèmes employés pour traiter ces données.

Pour créer et alimenter l'inventaire, les organisations devraient extraire des rapports EIVP les informations suivantes concernant les systèmes d'information employés pour traiter les IIP. La liste ci-après est fournie à titre d'exemple; certains éléments pourront lui être ajoutés ou retirés dans la liste finale de l'organisation:

a) nom et acronyme de chaque système recensé;

b) types d'IIP traités par ces systèmes;

c) classification (voir le § 8.2.2) de tous les types d'IIP, tant à titre d'éléments d'information individuels qu'en tant qu'éléments combinés dans ces systèmes d'information;

d) niveau de l'impact potentiel, pour l'entité principale des IIP et l'organisation, de toute atteinte à des IIP;

e) but du recueil des IIP;

f) sous-traitance éventuelle des IIP à un prestataire spécialisé dans leur traitement;

g) transmission éventuelle des IIP à d'autres contrôleurs des IIP (dans ce cas, préciser lesquels) ou à un groupe de destinataires;

h) durée de la conservation des IIP;

i) zone géographique dans laquelle les IIP ont été recueillies ou traitées; et

j) transfert éventuel des données vers un autre pays.

Les organisations devraient régulièrement envoyer des mises à jour de l'inventaire des IIP à la personne chargée de protéger ces données afin de faciliter la mise en place de mesures de sécurité adéquates dans tous les systèmes d'information, nouveaux ou existants, employés pour traiter des IIP.

8.1.3 Propriété des actifs

Les mesures prévues au § 8.1.2 et les conseils de mise en œuvre connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

8.1.4 Utilisation correcte des actifs

Les mesures prévues au § 8.1.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient protéger les actifs employés pour traiter les IIP contre tout accès, modification ou suppression non autorisés, et contre toute perte ou destruction, tout traitement erroné ou illicite, etc.

8.1.5 Restitution des actifs

Les mesures prévues au § 8.1.4 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

8.2 Classification de l'information

8.2.1 Introduction

Les buts définis au § 8.2 de la norme ISO/CEI 27002:2013 s'appliquent.

8.2.2 Classification des informations

Les mesures prévues au § 8.2.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient classer toutes les informations contenant des IIP en utilisant une catégorie de classification existante (appelée groupe d'informations dans la norme ISO/CEI 27002) ou de nouvelles catégories de classification. Les nouvelles catégories devraient comprendre notamment les catégories générales, comme les IIP sensibles et non sensibles. Une classification pourra aussi comprendre des catégories plus spécifiques, comme des informations sur la santé des personnes (ISP) et des informations financières personnelles (IFP). Si les organisations créent de nouvelles catégories, leur niveau de protection devrait également être défini. Les catégories réellement employées devraient également dépendre par exemple des prescriptions de la législation et de la réglementation sur la protection des données, d'autres

obligations juridiques (par exemple contractuelles), de la nature et la sensibilité des informations et du risque de préjudice que l'organisation pourrait subir en cas d'atteinte à des données.

A noter que certaines IIP peuvent être considérées comme non sensibles dans un pays et sensibles dans un autre, selon la législation applicable en matière de protection des données.

Il pourrait être nécessaire de revoir et modifier la classification d'un élément d'IIP si celui-ci est associé à un ou plusieurs attributs supplémentaires. Il convient d'établir des directives et des procédures appropriées dans ce domaine.

8.2.3 Marquage des informations

Les mesures prévues au § 8.2.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Lorsqu'une organisation ne classe pas les IIP dans une catégorie, elle devrait veiller à ce que les personnes sous sa responsabilité connaissent la définition des IIP et sachent les reconnaître.

8.2.4 Manipulation des actifs

Les mesures prévues au § 8.2.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Si une organisation permet aux personnes sous sa responsabilité de pouvoir omettre le marquage des informations pour les catégories liées aux IIP, elle devrait faire en sorte que les personnes sous sa responsabilité traitent toutes les informations contenant des IIP comme les informations de la catégorie assignée.

8.3 Manipulation des supports

8.3.1 Introduction

Les buts définis au § 8.3 de la norme ISO/CEI 27002:2013 s'appliquent.

8.3.2 Gestion des supports amovibles

Les mesures prévues au § 8.3.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Certaines juridictions peuvent rendre obligatoire le chiffrement des supports amovibles. Que cette pratique soit ou non obligatoire, elle est recommandée pour réduire le risque d'atteinte à des IIP.

Si la confidentialité ou l'intégrité des données ont une importance particulière, il convient d'employer des techniques de cryptographie pour protéger les IIP stockées sur des supports amovibles. Il faut aussi effectuer une étude de risque pour déterminer le niveau de protection requis, ce qui permettra ensuite de définir le type, la robustesse et la qualité de l'algorithme cryptographique à employer.

On trouvera des conseils supplémentaires sur l'emploi de mesures de cryptographie au § 10.1.

8.3.3 Mise au rebut des supports

Les mesures prévues au § 8.3.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Les procédures permettant de mettre au rebut de manière sécurisée les supports contenant des IIP devraient être proportionnelles à la sensibilité des informations et à l'impact que provoquerait un traitement inadéquat de ces informations. Certaines juridictions peuvent imposer des critères particuliers pour le choix des procédures de mise au rebut de supports contenant des IIP, ou des types d'IIP particuliers (par exemple des données sur la santé, des données financières)

8.3.4 Transfert physique des supports

Les mesures prévues au § 8.3.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Lorsque des supports physiques sont employés pour transférer des IIP, il convient de prendre des mesures pour consigner leurs entrées et sorties, en précisant le type de support physique, tout numéro d'identification (par exemple le numéro de série ou le numéro d'inventaire), l'expéditeur et le destinataire autorisés, la date et l'heure, le nombre de supports et les types d'IIP contenus. Il faut aussi être en mesure de détecter toute perte de support physique. Il convient par ailleurs de préciser le but et la portée du transfert, la personne l'ayant autorisé et le fondement juridique ou contractuel du transfert. Enfin, il est recommandé de faire en outre explicitement référence au principe de minimisation des données.

9 Contrôle d'accès

9.1 Exigences métier en matière de contrôle d'accès

9.1.1 Introduction

Le but défini au § 9.1 de la norme ISO/CEI 27002:2013 s'applique.

9.1.2 Politique de contrôle d'accès

Les mesures prévues au § 9.1.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

9.1.3 Accès aux réseaux et aux services en réseau

Les mesures prévues au § 9.1.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

9.2 Gestion de l'accès utilisateur

9.2.1 Introduction

Le but défini au § 9.2 de la norme ISO/CEI 27002:2013 s'applique.

9.2.2 Enregistrement et désinscription des utilisateurs

Les mesures prévues au § 9.2.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Les procédures d'enregistrement et de désinscription des utilisateurs, ainsi que la gestion du cycle de vie des utilisateurs devraient permettre de trouver un compromis entre les mesures de contrôle d'accès, qui portent par exemple sur la corruption ou la compromission de mots de passe, et les mesures visant les autres données d'enregistrement des utilisateurs (par exemple des données divulguées par inadvertance).

9.2.3 Maîtrise de la gestion des accès utilisateur

Les mesures prévues au § 9.2.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient accorder aux utilisateurs un droit d'accès adéquat aux systèmes d'information employés pour traiter des IIP, en tenant compte du principe de minimisation des données énoncé dans la norme ISO/CEI 29100.

Elles ne devraient accorder l'accès à ces systèmes d'information qu'au plus petit nombre possible de personnes nécessaires pour traiter les IIP, conformément au principe de minimisation des données énoncé dans la norme ISO/CEI 29100.

Elles devraient mettre en place des méthodes d'authentification robustes pour le stockage et le traitement de certaines IIP particulières (par exemple pour des données concernant la santé).

9.2.4 Gestion des privilèges d'accès

Les mesures prévues au § 9.2.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Le traitement des IIP à grande échelle (par exemple dans le cadre de requêtes, de modifications, d'exportation ou de suppression par lots) accroît le risque d'infraction à grande échelle. Les organisations devraient prendre des précautions particulières lorsqu'elles accordent des droits d'accès offrant ce type de privilèges. Pour éviter tout abus, les droits d'accès privilégiés pour traiter des IIP (notamment des IIP à haut risque) ne devraient être accordés que de manière strictement limitée. Ils devraient en outre être attribués d'une manière qui contribue à réduire les risques de collusion entre deux personnes ou plus. L'octroi et l'utilisation de ces droits devraient être consignés dans le journal pertinent. Ces accès ne devraient être accordés que pour une période précise. Les organisations devraient régulièrement revoir toutes ces autorisations avant de les renouveler, de les révoquer ou de les laisser parvenir à expiration selon les besoins.

9.2.5 Gestion des informations secrètes d'authentification des utilisateurs

Les mesures prévues au § 9.2.4 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

9.2.6 Revue des droits d'accès utilisateur

Les mesures prévues au § 9.2.5 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

9.2.7 Suppression ou adaptation des droits d'accès

Les mesures prévues au § 9.2.6 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

9.3 Responsabilités des utilisateurs

9.3.1 Introduction

Le but défini au § 9.3 de la norme ISO/CEI 27002:2013 s'applique.

9.3.2 Utilisation d'informations secrètes d'authentification

Les mesures prévues au § 9.3.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

9.4 Contrôle de l'accès au système et aux applications

9.4.1 Introduction

Le but défini au § 9.4 de la norme ISO/CEI 27002:2013 s'applique.

9.4.2 Restriction d'accès à l'information

Les mesures prévues au § 9.4.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Avant d'autoriser certaines personnes, notamment des opérateurs et des administrateurs, à utiliser des langages de requête permettant d'extraire d'importants volumes d'IIP de façon automatique à partir de bases de données, les organisations devraient déterminer s'il est nécessaire d'employer ces langages dans le traitement des IIP.

Si l'utilisation de ces langages n'est pas contraire aux exigences de protection, les organisations devraient prendre les mesures techniques requises pour limiter l'emploi de ces langages au minimum nécessaire pour remplir la ou les fonctions prévues.

En conséquence, les requêtes effectuées au moyen de ces langages peuvent par exemple être limitées à un petit nombre de champs sensibles définis au préalable.

Si certaines personnes demandent un accès à des zones qui sont en principe protégées (par exemple des zones d'exploitation), il convient d'appliquer un mécanisme d'approbation robuste. Les organisations devraient conserver la trace de toutes ces approbations.

9.4.3 Sécuriser les procédures de connexion

Les mesures prévues au § 9.4.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Si les entités principales des IIP peuvent demander des comptes d'accès à un contrôleur des IIP, celui-ci devrait mettre en place des procédures de connexion sécurisées à ces comptes, sous réserve des résultats de son analyse de risque.

9.4.4 Système de gestion des mots de passe

Les mesures prévues au § 9.4.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

9.4.5 Utilisation de programmes utilitaires à privilèges

Les mesures prévues au § 9.4.4 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

9.4.6 Contrôle d'accès au code source des programmes

Les mesures prévues au § 9.4.5 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

10 Cryptographie

10.1 Mesures cryptographiques

10.1.1 Introduction

Le but défini au § 10.1 de la norme ISO/CEI 27002:2013 s'applique.

10.1.2 Politique d'utilisation des mesures cryptographiques

Les mesures prévues au § 10.1.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

10.1.3 Gestion des clés

Les mesures prévues au § 10.1.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

11 Sécurité physique et environnementale

11.1 Zones sécurisées

11.1.1 Introduction

Le but défini au § 11.1 de la norme ISO/CEI 27002:2013 s'applique.

11.1.2 Périmètre de sécurité physique

Les mesures prévues au § 11.1.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

11.1.3 Contrôles physiques des accès

Les mesures prévues au § 11.1.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

11.1.4 Sécurisation des bureaux, des salles et des équipements

Les mesures prévues au § 11.1.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

11.1.5 Protection contre les menaces extérieures et environnementales

Les mesures prévues au § 11.1.4 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

11.1.6 Travail dans les zones sécurisées

Les mesures prévues au § 11.1.5 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

11.1.7 Zones de livraison et de chargement

Les mesures prévues au § 11.1.6 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

11.2 Matériels

11.2.1 Introduction

Le but défini au § 11.2 de la norme ISO/CEI 27002:2013 s'applique.

11.2.2 Emplacement et protection du matériel

Les mesures prévues au § 11.2.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

11.2.3 Services généraux

Les mesures prévues au § 11.2.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

11.2.4 Sécurité du câblage

Les mesures prévues au § 11.2.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

11.2.5 Maintenance du matériel

Les mesures prévues au § 11.2.4 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

11.2.6 Sortie des actifs

Les mesures prévues au § 11.2.5 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

11.2.7 Sécurité du matériel et des actifs hors des locaux

Les mesures prévues au § 11.2.6 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

11.2.8 Mise au rebut ou recyclage sécurisé(e) du matériel

Les mesures prévues au § 11.2.7 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Pour mettre au rebut ou recycler de manière sécurisée le matériel comportant des supports de stockage susceptibles de contenir des IIP, celui-ci devrait être physiquement détruit ou les IIP devraient être détruites, supprimées ou recouvertes en surécriture selon des techniques agréées, conformément à des procédures bien définies et documentées. Le but est de faire en sorte qu'il soit impossible de récupérer les IIP originales; il ne suffit donc pas d'employer les fonctions courantes de suppression ou de formatage. Si le matériel comporte des supports susceptibles de contenir des IIP chiffrées, il peut suffire de détruire les clés de déchiffrement ou leur support (comme une carte à puce) de manière supervisée.

11.2.9 Matériel utilisateur laissé sans surveillance

Les mesures prévues au § 11.2.8 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

11.2.10 Politique du bureau propre et de l'écran vide

Les mesures prévues au § 11.2.9 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

12 Sécurité liée à l'exploitation

12.1 Procédures et responsabilités liées à l'exploitation

12.1.1 Introduction

Le but défini au § 12.1 de la norme ISO/CEI 27002:2013 s'applique.

12.1.2 Procédures d'exploitation documentées

Les mesures prévues au § 12.1.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

12.1.3 Gestion des changements

Les mesures prévues au § 12.1.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

12.1.4 Dimensionnement

Les mesures prévues au § 12.1.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

12.1.5 Séparation des environnements de développement, de test et d'exploitation

Les mesures prévues au § 12.1.4 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Les environnements de développement, de test et d'exploitation devraient être séparés sur le plan numérique, et si possible sur le plan physique. Il convient de mettre en place des mesures adéquates de contrôle de l'accès pour s'assurer que l'accès est réservé aux personnes dûment autorisées. Si les réseaux ou les appareils servant au développement ou au test ont besoin d'accéder au réseau d'exploitation, il convient de contrôler cet accès par des mesures robustes.

L'organisation devrait évaluer le risque lié à l'emploi de supports amovibles et d'appareils contenant des IIP dotés de capacités hertziennes, quel que soit l'environnement dans lequel ils vont être utilisés.

Les IIP ne devraient pas être employées à des fins de développement et de test sans avoir été anonymisées au préalable si la législation l'interdit ou que l'entité principale des IIP n'a pas donné son consentement de manière explicite.

12.2 Protection contre les logiciels malveillants

12.2.1 Introduction

Le but défini au § 12.2 de la norme ISO/CEI 27002:2013 s'applique.

12.2.2 Mesures contre les logiciels malveillants

Les mesures prévues au § 12.2.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

12.3 Sauvegarde

12.3.1 Introduction

Le but défini au § 12.3 de la norme ISO/CEI 27002:2013 s'applique.

12.3.2 Sauvegarde des informations

Les mesures prévues au § 12.3.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Des mécanismes supplémentaires ou différents devraient être mis en place pour les systèmes d'information qui traitent des IIP, par exemple des mécanismes de sauvegardes sur des sites éloignés, de sorte que les IIP ne puissent être perdues, que la pérennité de leur traitement soit garantie et qu'il soit possible de reprendre leur traitement après un événement perturbateur. Toutefois, cette mesure ne devrait être prise que si elle est strictement nécessaire.

NOTE – Un certain temps s'écoule entre le moment où une sauvegarde est effectuée et celui où les données vont être récupérées. Les IIP sauvegardées peuvent ne plus être à jour au moment où elles sont récupérées. Toute opération effectuée sur des IIP obsolètes peut fausser les résultats et créer un risque d'atteinte à la vie privée.

12.4 Journalisation et surveillance

12.4.1 Introduction

Le but défini au § 12.4 de la norme ISO/CEI 27002:2013 s'applique.

12.4.2 Journalisation des événements

Les mesures prévues au § 12.4.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Dans la mesure du possible, le journal devrait indiquer à quelles IIP l'utilisateur a accédé, le traitement dont elles ont fait l'objet (par exemple des actions de lecture, d'impression, d'ajout, de modification ou de suppression), la date de l'accès et l'identité de l'utilisateur. Ces inscriptions au journal sont tout particulièrement importantes pour certains types d'IIP (notamment les informations sur la santé). Si plusieurs prestataires de services sont concernés, il peut être nécessaire de créer différentes fonctions ou de partager des fonctions pour mettre en œuvre ce conseil.

Il convient de mettre en place un processus d'examen du journal à une fréquence définie et documentée afin de détecter toute irrégularité et de proposer des mesures correctives.

Le contrôleur des IIP devrait instaurer des procédures définissant s'il est possible de mettre l'information journalisée à la disposition de l'administrateur pour qu'il contrôle la sécurité et analyse l'exploitation des données, et dans l'affirmative, quand et comment cette information peut lui être communiquée.

12.4.3 Protection de l'information journalisée

Les mesures prévues au § 12.4.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

L'information journalisée à des fins de contrôle de la sécurité et d'analyse de l'exploitation des données peut contenir des IIP. Il convient donc de mettre en place des mesures de contrôle de l'accès à ces informations (voir le § 9.2.3) pour s'assurer que celles-ci sont exploitées uniquement dans le but prévu. Il faut aussi prendre des mesures pour garantir l'intégrité des journaux.

12.4.4 Journaux administrateur et opérateur

Les mesures prévues au § 12.4.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient contrôler les accès privilégiés (par exemple ceux des administrateurs et des opérateurs) aux IIP et tout traitement effectué par ces personnes. Ce contrôle devrait s'inscrire dans le cadre de la surveillance générale des systèmes d'information employés pour traiter des IIP.

Chaque organisation devrait définir ce qu'elle considère être une activité anormale et mettre en place des procédures automatiques pour signaler une telle activité à son personnel compétent.

12.4.5 Synchronisation des horloges

Les mesures prévues au § 12.4.4 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

12.5 Maîtrise des logiciels en exploitation

12.5.1 Introduction

Le but défini au § 12.5 de la norme ISO/CEI 27002:2013 s'applique.

12.5.2 Installation de logiciels sur des systèmes en exploitation

Les mesures prévues au § 12.5.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

12.6 Gestion des vulnérabilités techniques

12.6.1 Introduction

Le but défini au § 12.6 de la norme ISO/CEI 27002:2013 s'applique.

12.6.2 Gestion des vulnérabilités techniques

Les mesures prévues au § 12.6.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

12.6.3 Restrictions liées à l'installation de logiciels

Les mesures prévues au § 12.6.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

12.7 Considérations sur l'audit du système d'information

12.7.1 Introduction

Le but défini au § 12.7 de la norme ISO/CEI 27002:2013 s'applique.

12.7.2 Mesures relatives à l'audit des systèmes d'information

Les mesures prévues au § 12.7.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

13 Sécurité des communications

13.1 Management de la sécurité des réseaux

13.1.1 Introduction

Le but défini au § 13.1 de la norme ISO/CEI 27002:2013 s'applique.

13.1.2 Contrôle des réseaux

Les mesures prévues au § 13.1.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

13.1.3 Sécurité des services de réseau

Les mesures prévues au § 13.1.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

13.1.4 Cloisonnement des réseaux

Les mesures prévues au § 13.1.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

13.2 Transfert de l'information

13.2.1 Introduction

Le but défini au § 13.2 de la norme ISO/CEI 27002:2013 s'applique.

13.2.2 Politiques et procédures de transfert de l'information

Les mesures prévues au § 13.2.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Il convient de prendre les mesures nécessaires pour réduire le risque de fuite d'IIP au cours d'un transfert de ces informations. Ce problème peut généralement être réglé par des techniques de chiffrement et d'autres mesures préliminaires, notamment la désidentification, le masquage et l'obfuscation.

13.2.3 Accords en matière de transfert d'information

Les mesures prévues au § 13.2.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

13.2.4 Messagerie électronique

Les mesures prévues au § 13.2.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

13.2.5 Engagements de confidentialité ou de non-divulgation

Les mesures prévues au § 13.2.4 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

L'organisation devrait définir les conditions dans lesquelles les IIP peuvent être traitées à l'extérieur. Ces conditions devraient être énoncées dans un accord adéquat (par exemple un contrat ou un engagement de confidentialité ou de non-divulgation).

14 Acquisition, développement et maintenance des systèmes d'information

14.1 Exigences de sécurité applicables aux systèmes d'information

14.1.1 Introduction

Le but défini au § 14.1 de la norme ISO/CEI 27002:2013 s'applique.

14.1.2 Analyse et spécification des exigences de sécurité de l'information

Les mesures prévues au § 14.1.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Dans le cadre de la mise en place ou de modifications majeures de systèmes d'information destinés à traiter des IIP, il convient de mener une EIVP. La norme ISO/CEI 29134 contient un certain nombre de conseils à cet égard. Les résultats de cette étude devraient orienter le choix des mesures à prendre pour gérer les risques recensés.

14.1.3 Sécurisation des services d'application sur les réseaux publics

Les mesures prévues au § 14.1.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

14.1.4 Protection des transactions liées aux services d'application

Les mesures prévues au § 14.1.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

14.2 Sécurité des processus de développement et d'assistance technique

14.2.1 Introduction

Le but défini au § 14.2 de la norme ISO/CEI 27002:2013 s'applique.

14.2.2 Politique de développement sécurisé

Les mesures prévues au § 14.2.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

14.2.3 Procédures de contrôle des changements apportés au système

Les mesures prévues au § 14.2.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

14.2.4 Revue technique des applications après changement apporté à la plate-forme d'exploitation

Les mesures prévues au § 14.2.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

14.2.5 Restrictions relatives aux changements apportés aux progiciels

Les mesures prévues au § 14.2.4 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

14.2.6 Principes d'ingénierie de la sécurité des systèmes

Les mesures prévues au § 14.2.5 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

14.2.7 Environnement de développement sécurisé

Les mesures prévues au § 14.2.6 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

14.2.8 Développement externalisé

Les mesures prévues au § 14.2.7 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

14.2.9 Phase de test de la sécurité du système

Les mesures prévues au § 14.2.8 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

14.2.10 Test de conformité du système

Les mesures prévues au § 14.2.9 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Le test de conformité du système devrait notamment comprendre un test de conformité aux exigences en matière de protection des données personnelles.

14.3 Données de test

14.3.1 Introduction

Le but défini au § 14.3 de la norme ISO/CEI 27002:2013 s'applique.

14.3.2 Protection des données de test

Les mesures prévues au § 14.3.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

En principe, les données opérationnelles contenant des IIP ne devraient pas être utilisées pour effectuer des développements ou des tests. L'emploi de ce type de données dans ces environnements accroît le risque de compromettre des informations. Les organisations devraient plutôt employer des données créées artificiellement ou prendre des mesures pour "cacher" (c'est-à-dire masquer, obfusquer, désidentifier) les véritables IIP éventuellement employées.

15 Relations avec les fournisseurs

15.1 Sécurité de l'information dans les relations avec les fournisseurs

15.1.1 Introduction

Le but défini au § 15.1 de la norme ISO/CEI 27002:2013 s'applique.

15.1.2 Politique de sécurité de l'information dans les relations avec les fournisseurs

Les mesures prévues au § 15.1.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Si une organisation doit faire appel aux services d'un prestataire pour traiter des IIP, elle doit évaluer l'expérience de celui-ci, déterminer dans quelle mesure elle peut lui faire confiance et apprécier sa capacité à répondre aux exigences en matière de protection de ces informations, conformément à la législation, à la réglementation et aux contrats ou autres accords juridiques en vigueur.

L'organisation chargée de contrôler les IIP devrait établir par écrit un contrat avec tout prestataire chargé de traiter des IIP. Ce contrat devrait clairement répartir les rôles et les responsabilités entre les deux entités, et il devrait contenir toutes les dispositions requises concernant la protection des IIP afin que le prestataire assume la responsabilité du traitement qu'il effectue.

Le contrat établi par le contrôleur des IIP devrait au moins contenir les dispositions suivantes:

- une déclaration adéquate de l'échelle, de la nature et du but du traitement faisant l'objet du contrat;
- une définition des services d'appui que le prestataire doit offrir aux entités principales des IIP en leur permettant d'accéder à leurs IIP pour les vérifier et en assurant la gestion de toute plainte déposée par une entité principale des IIP (voir le § A.10);
- toute autre mesure d'organisation permettant au prestataire de s'acquitter de ses obligations découlant de la législation ou de la réglementation;
- l'autorisation du contrôleur des IIP de mener des audits dans les locaux du prestataire;
- les obligations de déclaration en cas d'atteinte à des données personnelles, de traitement non autorisé de ces données ou de tout manquement aux conditions générales du contrat. Il convient à cet égard d'indiquer la personne à contacter au sein des deux parties;
- la procédure permettant au contrôleur des IIP d'adresser des injonctions au prestataire;
- les mesures à prendre à l'expiration du contrat, notamment pour supprimer de manière sécurisée les IIP dans les locaux du prestataire ou restituer les IIP et les supports physiques.

Le contrôleur des IIP devrait s'assurer que ses prestataires ne sous-traitent pas à leur tour le traitement des informations (c'est-à-dire qu'ils ne font pas appel à d'autres prestataires) sans avoir au préalable obtenu son approbation. Il devrait se conformer à l'ensemble de la législation et de la réglementation à cet égard.

Il devrait en outre s'assurer que ses prestataires ne traitent pas les IIP dans un but différent de ceux qui sont définis dans le contrat ou dans tout autre accord ayant une valeur juridique.

Il devrait enfin veiller à ce que ses prestataires suppriment les IIP de manière sécurisée et conformément aux politiques et autres directives qu'il a établies (par exemple dans le respect des exigences particulières énoncées par l'organisation).

15.1.3 La sécurité dans les accords conclus avec les fournisseurs

Les mesures prévues au § 15.1.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

15.1.4 Chaîne d'approvisionnement informatique

Les mesures prévues au § 15.1.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

15.2 Gestion de la prestation du service

15.2.1 Introduction

Le but défini au § 15.2 de la norme ISO/CEI 27002:2013 s'applique.

15.2.2 Surveillance et revue des services des fournisseurs

Les mesures prévues au § 15.2.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

15.2.3 Gestion des changements apportés dans les services avec les fournisseurs

Les mesures prévues au § 15.2.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

16 Gestion des incidents liés à la sécurité de l'information

16.1 Gestion des incidents liés à la sécurité de l'information et améliorations

16.1.1 Introduction

Le but défini au § 16.1 de la norme ISO/CEI 27002:2013 s'applique.

16.1.2 Responsabilités et procédures

Les mesures prévues au § 16.1.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient être en mesure de réagir de manière structurée et efficace à un incident concernant des données personnelles, et elles devraient être toujours prêtes pour cette éventualité. Elles devraient donc élaborer et mettre en place un plan de réaction à ce type d'incidents.

Tout plan de réaction d'une organisation aux incidents concernant des données personnelles devrait notamment comporter les étapes suivantes:

a) La définition d'un incident concernant des données personnelles et le domaine d'application d'un plan de réaction à ce type d'incidents.

b) La mise en place d'une équipe transversale chargée de réagir à l'incident, qui va élaborer, mettre en place, tester, exécuter et analyser le plan de réaction (l'approbation du plan relevant de la compétence de la haute direction de l'organisation).

c) L'établissement d'une définition claire des rôles, des responsabilités et de l'autorité de chaque membre de l'équipe de réaction.

d) L'élaboration de procédures établissant le fondement juridique d'une coopération avec des organisations extérieures (nationales et internationales) en cas d'incident transnational.

e) L'élaboration de procédures garantissant que toute personne soumise à la politique interne de protection des données personnelles signale rapidement tout incident concernant ce type de données aux responsables de la sécurité de l'information et à la personne chargée de la protection des IIP (parfois appelée DDP), conformément à la politique de l'organisation en matière de gestion des incidents.

f) L'évaluation de l'impact de l'incident (effectuée selon des tâches précises) pour déterminer la nature et la portée de tout préjudice potentiel ou réel causé aux personnes concernées (embarras, désagrément ou injustice) ou à l'organisation.

g) La mise en place d'un processus visant à recenser les mesures nécessaires pour limiter les préjudices déterminés dans l'étude d'impact précitée, et à réduire la probabilité que ces préjudices surviennent à nouveau.

h) La mise en place de procédures permettant de déterminer s'il est obligatoire d'informer les personnes concernées ou toute autre entité désignée (par exemple les responsables de la réglementation), de définir à quel moment et sous quelle forme ces informations doivent être communiquées, et le cas échéant, de transmettre ces informations.

Les organisations peuvent choisir d'intégrer leurs plans de réaction aux incidents concernant des données personnelles dans leurs plans de réaction aux incidents de sécurité, ou de les conserver à part. Tout incident de sécurité concernant des informations devrait déclencher une analyse de la part du contrôleur des IIP, dans le cadre du processus normal de gestion de ce type d'incidents, afin de déterminer s'il y a eu atteinte à des données contenant des IIP.

En revanche, un simple événement de sécurité concernant des informations ne doit pas nécessairement déclencher ce type d'analyse. Il peut s'agir par exemple, mais pas seulement, d'un sondage par écho (ping) ou d'une attaque radiodiffusée sur

les pare-feu ou les serveurs périphériques, d'une analyse de ports, de tentatives de connexion infructueuses, d'attaques par déni de service ou de reniflage de paquets. Un événement de sécurité concernant des informations n'entraîne pas forcément une remise en cause probable ou réelle des IIP ou du matériel et installations employés pour traiter les IIP.

16.1.3 Signalement des événements liés à la sécurité de l'information

Les mesures prévues au § 16.1.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Lorsque des IIP sont compromises, il est impératif de prendre immédiatement des mesures pour protéger les droits et les intérêts de l'entité principale des IIP.

Certaines juridictions peuvent imposer (par exemple dans leur législation ou leur réglementation) des mesures précises pour signaler et/ou notifier les incidents de sécurité concernant des IIP (par exemple un traitement non autorisé, une atteinte à des données). En cas d'incident de ce type, tous les détails le concernant, y compris la réaction envisagée par l'organisation (dont la divulgation peut faire l'objet d'un certain nombre de restrictions) doivent être communiqués aussi rapidement que possible aux autorités compétentes. Il peut s'agir notamment des autorités responsables de la protection de données, des forces de l'ordre et des personnes concernées par l'incident.

Les organisations devraient accorder aux entités principales des IIP un accès leur permettant de prendre des mesures correctives adéquates et efficaces, par exemple en rectifiant ou en supprimant des informations inexactes après une intrusion.

16.1.4 Signalement des failles liées à la sécurité de l'information

Les mesures prévues au § 16.1.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

16.1.5 Appréciation des événements liés à la sécurité de l'information et prise de décision

Les mesures prévues au § 16.1.4 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

16.1.6 Réponse aux incidents liés à la sécurité de l'information

Les mesures prévues au § 16.1.5 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

16.1.7 Tirer des enseignements des incidents liés à la sécurité de l'information

Les mesures prévues au § 16.1.6 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

16.1.8 Recueil de preuves

Les mesures prévues au § 16.1.7 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

17.1 Continuité de la sécurité de l'information

17.1.1 Introduction

Le but défini au § 17.1 de la norme ISO/CEI 27002:2013 s'applique.

17.1.2 Organisation de la continuité de la sécurité de l'information

Les mesures prévues au § 17.1.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

17.1.3 Mise en œuvre de la continuité de la sécurité de l'information

Les mesures prévues au § 17.1.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

17.1.4 Vérifier, revoir et évaluer la continuité de la sécurité de l'information

Les mesures prévues au § 17.1.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

17.2 Redondances

17.2.1 Introduction

Le but défini au § 17.2 de la norme ISO/CEI 27002:2013 s'applique.

17.2.2 Disponibilité des moyens de traitement de l'information

Les mesures prévues au § 17.2.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

18 Conformité

18.1 Conformité aux obligations légales et réglementaires

18.1.1 Introduction

Le but défini au § 18.1 de la norme ISO/CEI 27002:2013 s'applique.

18.1.2 Identification de la législation et des exigences contractuelles applicables

Les mesures prévues au § 18.1.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient recenser la législation et la réglementation en matière de protection des IIP auxquelles elles sont soumises. Les organisations devraient ensuite prendre les mesures nécessaires pour se conformer aux exigences recensées, qui peuvent par exemple être les suivantes:

a) Lorsqu'une protection supplémentaire (par exemple un numéro d'identification national, de passeport ou de carte de crédit) est requise pour certaines catégories d'IIP, des techniques cryptographiques, comme le chiffrement, devraient être utilisées. Le type, la solidité et la qualité requis pour l'algorithme cryptographique devraient être pris en compte. Les algorithmes cryptographiques devraient être choisis exclusivement parmi une liste d'algorithmes agréés.

   Le protocole de sécurité lié à cette exigence est spécifié au § 10.1.2.

b) Les juridictions peuvent imposer une fréquence minimum de sauvegarde des données pour les informations comprenant des IIP, ainsi qu'une fréquence minimum d'examen des procédures de sauvegarde et de récupération.

   Le protocole de sécurité lié à cette exigence est spécifié au 12.3.2.

Les organisations devraient mener des EIVP et mettre en place des plans de protection de la vie privée en conséquence, afin de s'assurer que les programmes et services liés au traitement des IIP soient conformes aux exigences en la matière. On trouvera de plus amples conseils à cet égard dans la norme ISO/CEI 29134 ".

Les organisations devraient établir un programme d'audit pour faire en sorte que le traitement des IIP soit conforme aux exigences pertinentes en matière de protection des données personnelles. Ce programme devrait préciser la fréquence à laquelle ces audits doivent être menés.

Les audits peuvent être effectués par l'organisation elle-même (qui peut les confier par exemple à un service d'audit interne), ou par un tiers indépendant et qualifié.

Autres informations concernant la protection des IIP

Si de nombreuses juridictions tiennent le contrôleur des IIP pour responsable, en dernier ressort, de la conformité de l'organisation aux obligations de protection de ces données, tous les acteurs intervenant dans le traitement des IIP devraient s'efforcer de recenser l'ensemble des exigences prévues dans la législation ou d'autres textes concernant la protection des données personnelles.

Le contrat conclu entre le contrôleur des IIP et le prestataire chargé de traiter ces informations prévoit que ce dernier doit s'assurer de la conformité de ses travaux. Le contrat prévoit en outre que cette conformité sera vérifiée dans le cadre d'un

audit indépendant acceptable par le prestataire. Il peut par exemple s'agir de mesures de contrôle prises au titre de la présente spécification ou des normes ISO/CEI 27002 ou ISO/CEI 27018.

18.1.3 Droits de propriété intellectuelle

Les mesures prévues au § 18.1.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

18.1.4 Protection des enregistrements

Les mesures prévues au § 18.1.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

18.1.5 Protection de la vie privée et protection des données à caractère personnel

Les mesures prévues au § 18.1.4 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

18.1.6 Réglementation relative aux mesures cryptographiques

Les mesures prévues au § 18.1.5 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

18.2 Revue de la sécurité de l'information

18.2.1 Introduction

Le but défini au § 18.2 de la norme ISO/CEI 27002:2013 s'applique.

18.2.2 Revue indépendante de la sécurité de l'information

Les mesures prévues au § 18.2.1 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent. Les conseils supplémentaires proposés ci-après s'appliquent également.

Conseils de mise en œuvre de la protection des IIP

Si les parties concernées ont des difficultés à effectuer l'audit ou que celui-ci risque d'accroître les risques de sécurité, les organisations devraient communiquer aux parties potentiellement intéressée, avant de conclure tout contrat, des éléments de preuves indépendants attestant que des mesures ont été prises pour sécuriser l'information et qu'elles sont appliquées conformément aux politiques et procédures du contrôleur des IIP. Un audit indépendant et spécialisé, choisi par le contrôleur des IIP et portant sur les procédures de fonctionnement de celui-ci, devrait en principe constituer une méthode acceptable pour protéger les intérêts des parties concernées, pour autant qu'il se déroule de manière suffisamment transparente.

18.2.3 Conformité avec les politiques et les normes de sécurité

Les mesures prévues au § 18.2.2 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

18.2.4 Examen de la conformité technique

Les mesures prévues au § 18.2.3 et les conseils de mise en œuvre et autres informations connexes figurant dans la norme ISO/CEI 27002 s'appliquent.

Annexe A

Extension des mesures de contrôle à la protection des IIP

(La présente Annexe fait partie intégrante de la Recommandation | Norme internationale.)

A.1 Considérations générales

La présente Annexe propose de nouveaux objectifs, de nouvelles mesures de contrôle et de nouveaux conseils de mise en œuvre. Elle étend ainsi les mesures de contrôle existantes pour répondre aux exigences particulières de la protection des IIP.

Les conseils énoncés dans la présente spécification sont fondés sur ceux qui apparaissent dans la norme ISO 29100:201 et reposent sur l'hypothèse que ces derniers ont déjà été suivis.

Le paragraphe A.1 contient une description des politiques générales concernant la protection des IIP. Les paragraphes ci-après reprennent les principes de protection des données personnelles figurant dans la norme ISO/CEI 29100.

A.2 Politiques générales concernant l'utilisation et la protection des IIP

Objectif: Offrir à la direction générale des orientations et un appui pour protéger les IIP conformément aux exigences de la profession et aux législations et réglementations pertinentes.

Mesure de contrôle

Les organisations intervenant dans le traitement des IIP devraient mettre en place une politique régissant l'utilisation et la protection de ces informations.

Conseils de mise en œuvre de la protection des IIP

Les politiques de confidentialité devraient comprendre des instructions pertinentes (présentées dans des politiques concernant spécifiquement les données personnelles, ou en complément de politiques existantes) concernant l'appui à apporter et les engagements à prendre pour parvenir à se conformer à la législation sur la protection des IIP applicable, aux obligations contractuelles et aux politiques internes.

Les politiques de protection des données personnelles et de sécurité ne traitent pas nécessairement des mêmes sujets mais elles sont étroitement liées: en effet, les deux devraient traiter de la confidentialité, de l'intégrité et de la disponibilité de l'information. Les politiques sur les données personnelles devraient en outre porter sur des sujets tels que le consentement et l'accès individuel.

La norme ISO/CEI 29100 contient un certain nombre de conseils visant à instaurer un cadre de protection des données à caractère personnel. La politique de protection des IIP devrait:

- être adaptée au(x) besoin(s) de l'organisation;
- décrire de manière transparente les processus de recueil et de traitement des IIP au sein de l'organisation;
- fournir le cadre nécessaire à la définition des buts de la protection des IIP;
- définir les règles de prise de décision en matière de protection des IIP;
- définir les critères d'acceptation des risques concernant les données personnelles (voir également le sous-paragraphe 6.3.1 de la norme ISO/CEI 29134);
- affirmer l'engagement de se conformer aux exigences en vigueur en matière de protection des données personnelles;
- affirmer l'engagement d'améliorer la situation en permanence;
- être diffusée au sein de l'organisation; et
- être mise à la disposition des parties intéressées, le cas échéant.

A.3 Consentement et choix

A.3.1 Consentement

Objectif: Faire en sorte que les entités principales des IIP participent activement au processus de prise de décision concernant le traitement de leurs IIP, sauf disposition contraire dans la législation ou la réglementation, en exprimant un consentement sérieux, éclairé et accordé librement.

Mesure de contrôle

Les organisations devraient offrir aux entités principales des IIP les moyens d'exprimer un consentement sérieux, éclairé, sans ambiguïté et accordé librement, sauf dans les situations où les entités principales ne peuvent refuser librement leur consentement ou lorsque la législation pertinente prévoit expressément que les IIP peuvent faire l'objet d'un traitement sans le consentement de l'entité principale.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) trouver des moyens pratiques d'obtenir le consentement des entités principales des IIP, analyser les cas dans lesquels les moyens choisis ne peuvent plus être employés et trouver alors d'autres solutions, si nécessaire, pour obtenir leur consentement avant le début de tout traitement;

b) donner aux entités principales des IIP, lorsque c'est faisable et pertinent ou que la législation le prévoit, le moyen d'exprimer leur consentement avant le début de tout traitement. Le terme "traitement" s'entend du recueil, du stockage, de la modification, de l'extraction, de la consultation, de la divulgation, de la désidentification, de l'anonymisation, de la dissémination ou toute autre méthode de diffusion, de la suppression ou de la destruction des IIP;

c) lorsque le consentement est accordé par un responsable légal (par exemple au nom d'un mineur ou d'un personne frappée d'incapacité juridique), conserver l'enregistrement du consentement;

d) au besoin, informer les entités principales des IIP de tous les cas de transfert d'IIP à des tiers et leur offrir un moyen adéquat d'exprimer leur consentement à ces transferts;

e) obtenir, lorsque c'est faisable et pertinent ou que la législation le prévoit, le consentement des entités principales des IIP avant toute nouvelle utilisation ou divulgation d'IIP préalablement recueillies, et s'assurer qu'un consentement a été obtenu avant tout nouveau traitement;

f) s'assurer que le consentement a été obtenu de manière transparente après que les entités principales des IIP ont été dûment informées des buts du traitement, et veiller à ce que le consentement soit accordé dans un but précis;

g) sensibiliser les personnes avant d'obtenir un consentement, par exemple via des notes d'information publiques;

h) permettre aux entités principales des IIP de modifier la portée de leur consentement. Toute modification de consentement devrait être prise en compte en temps utile, et le traitement devrait être modifié ou arrêté conformément à la version modifiée du consentement;

i) s'assurer que le consentement est conforme à toutes les prescriptions juridiques, notamment si le consentement doit être explicite en cas d'IIP sensibles;

j) le cas échéant, prévoir la possibilité d'un consentement implicite lorsque les entités principales des IIP ont été clairement informées du traitement et qu'elles n'ont pas exprimé d'objection, car leur comportement peut alors indiquer un accord;

k) notifier toute opération de traitement préalablement à sa mise en œuvre; et

l) confirmer, au besoin, l'identité de l'entité principale des IIP ou de son représentant agréé qui consent au traitement. Il convient de ne demander que le minimum d'informations nécessaires à cette vérification, de ne conserver ces informations que le temps requis pour vérifier l'identité et de supprimer ces informations de manière sécurisée une fois qu'elles ne sont plus utiles.

Autres informations concernant la protection des IIP

Sous réserve de la législation applicable, les organisations devraient obtenir un consentement exprès ou implicite. Il est préférable que le consentement soit exprès, mais ce n'est pas toujours possible. Le consentement exprès exige que les entités principales des IIP prennent une mesure positive autorisant les organisations à recueillir ou utiliser des IIP. Lorsque ce consentement est accordé par voie électronique, l'organisation doit déterminer si une simple mesure positive suffit ou si elle doit être doublée.

Dans un consentement implicite, les organisations peuvent former l'hypothèse que les entités principales des IIP ont consenti au traitement de leurs IIP du fait qu'elles n'ont pas pris de mesure positive dans le sens contraire.

Le consentement implicite est généralement déduit des mesures prises ou non par une personne, ou de circonstances particulières. Ainsi, un client peut fournir son adresse de livraison à un détaillant en ligne, et celui-ci va strictement utiliser l'information pour livrer les marchandises achetées.

Les organisations devraient fournir des moyens pratiques d'obtenir un consentement distinct pour chaque entité principale lorsque des numéros d'identification nationaux (par exemple un numéro de sécurité sociale, de résident ou de passeport) sont demandés.

Elles peuvent ainsi permettre aux entités principales de choisir si elles veulent être contactées dans certains buts particuliers. Elles mettent alors en place des mécanismes pour s'assurer que leur fonctionnement interne est cohérent, dans toute la mesure du possible, avec les choix exprimés par les entités principales.

Le consentement peut être exprimé par voie électronique ou sur papier, selon les prescriptions réglementaires en vigueur et certaines considérations pratiques.

Lorsque les IIP ont été transférées d'une organisation à une autre, les organisations devraient mettre en place une procédure de mise à jour de leurs enregistrements afin de prendre en compte les mises à jour et les modifications de consentement (par exemple un changement ou une révocation du consentement) des entités principales des IIP. Cette procédure devrait aussi permettre de transmettre les mises à jour ou les modifications aux organisations avec lesquelles les IIP ont été partagées. Il convient de ne demander et de ne partager avec d'autres organisations que le minimum d'informations nécessaires pour s'assurer que les bonnes données ont été mises à jour. Les organisations devraient revoir régulièrement leurs procédures pour éliminer tout traitement inutile d'une IIP.

A.3.2 Choix

Objectif: Accorder aux entités principales des IIP, lorsque c'est pertinent et faisable, le choix de ne pas autoriser le traitement de leurs IIP, de refuser ou de retirer leur consentement, ou de s'opposer à un type de traitement particulier, et expliquer aux entités principales les conséquences de leur consentement ou de leur refus.

Mesure de contrôle

Les organisations devraient mettre à la disposition des entités principales des IIP des mécanismes clairs, visibles, faciles à comprendre, accessibles et peu coûteux pour exprimer leur choix concernant le traitement de leurs IIP, sauf dans les cas où les entités principales ne peuvent refuser leur consentement ou lorsque la législation prévoit de manière spécifique que les IIP peuvent être traitées sans le consentement de leur entité principale.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) s'assurer que les entités principales des IIP censées exprimer un choix concernant le traitement de leurs informations peuvent le faire avant que ce traitement n'intervienne;

b) veiller à ne pas refuser un service à une entité principale ayant refusé de fournir des IIP qui ne sont pas pertinentes pour ce service;

c) trouver, lorsque la législation le prévoit, un moyen pratique permettant aux entités principales de faire objection au traitement de leurs IIP. Les entités principales devraient disposer de plusieurs moyens différents d'exercer leur droit de consentement (par exemple par courrier postal, par courrier électronique ou par téléphone);

d) accuser réception de la déclaration d'objection dans le délai prévu par la loi ou défini dans la politique de l'organisation;

e) analyser les cas dans lesquels les moyens pratiques choisis ne fonctionnent plus et trouver des solutions de secours, si nécessaire, pour permettre aux entités principales de continuer d'exercer leur droit de faire objection en temps utile;

f) s'assurer que les IIP sont classées, étiquetées et stockées d'une manière qui facilite l'exercice du droit d'objection, et que les entités principales peuvent exercer leur droit d'objection en temps utile et gratuitement;

g) confirmer l'identité de l'entité principale ou de son représentant agréé qui fait objection au traitement. Il convient de ne demander que le minimum d'informations nécessaires à cette vérification, de ne conserver ces informations que le temps requis pour vérifier l'identité et de supprimer ces informations de manière sécurisée une fois qu'elles ne sont plus utiles;

h) s'assurer, si le droit d'objection doit avoir un fondement juridique, que les entités principales exerçant ce droit ont présenté des motifs raisonnables de leur objection. Tout refus de se conformer à une objection doit indiquer en détail les raisons pour lesquelles le contrôleur des IIP considère que ces motifs ne sont pas légitimes;

i) s'assurer que toutes les organisations avec lesquelles les IIP ont été partagées sont informées de toute objection exprimée par l'entité principale, et qu'elles se conforment à toute objection valable; et

j) offrir aux entités principales, lorsque c'est possible, la possibilité de choisir certains éléments du traitement de leurs IIP plutôt que de devoir accepter ou refuser l'ensemble du traitement.

Autres informations concernant la protection des IIP

Dans certaines situations, suivant la législation applicable, il peut être inutile ou impossible de proposer un mécanisme permettant d'exercer un choix lorsqu'on recueille des informations disponibles au public. Par exemple, il n'est pas nécessaire de fournir un mécanisme pour offrir un choix aux entités principales des IIP lorsqu'on extrait leur nom et leur adresse d'une base de données publique ou d'un journal.

A.4 Légitimité et définition du but

A.4.1 Légitimité du but

Objectif: S'assurer que le ou les buts du traitement des IIP sont conformes à la législation applicable et ont un fondement juridique.

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour faire en sorte que le traitement des IIP soit conforme à la législation applicable et qu'il soit fondé sur le plan juridique.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) déterminer si le traitement proposé peut être entrepris pour un motif juridique distinct de celui qui a obtenu le consentement (par exemple par décision des forces de l'ordre, pour des raisons de sécurité publique, en vertu d'une obligation légale ou au regard des objectifs légitimes du contrôleur des IIP);

b) déterminer si le traitement proposé repose sur un motif juridique (c'est-à-dire qu'il a été décidé par les forces de l'ordre, qu'il repose sur un motif lié à la sécurité publique ou qu'il découle d'une obligation légale) interdisant à l'entité principale d'exercer un choix concernant le traitement de ses IIP;

NOTE – Si le recueil ou le traitement des IIP s'effectue à l'échelle internationale, la nécessité d'obtenir un consentement et la procédure à appliquer peuvent différer selon le cadre juridique en vigueur.

c) déterminer l'autorité (le fondement) juridique autorisant le traitement des IIP, que ce soit de manière générale ou à l'appui d'un programme ou d'un système d'information particulier; et

d) intégrer des procédures garantissant que le traitement est conforme à l'ensemble des règlements applicables et à leur interprétation par les autorités compétentes. Il convient de prendre en compte le contexte général du traitement pour établir la légitimité de son but. Il faut notamment prendre en considération la relation sous-jacente entre le contrôleur des IIP et les entités principales, l'évolution scientifique et technologique et les changements intervenant dans les comportements sociétaux et culturels.

Les organisations devraient se doter de procédures garantissant que le traitement des IIP n'est pas effectué d'une manière contraire, ou potentiellement contraire, à des obligations légales, et notamment à des dispositions statutaires, au droit coutumier ou à des conditions contractuelles.

Si l'organisation dispose d'un comité d'entreprise ou d'un syndicat, la législation en vigueur peut exiger que des consultations soient menées avec ces organes pour établir la légitimité d'un but lorsque les personnes concernées sont des employés.

Les responsables du programme devraient mener des consultations avec la personne chargée de la protection des IIP (parfois appelée Directeur des données personnelles) ou avec toute autre personne ayant une fonction équivalente, ainsi qu'avec le conseiller juridique pour déterminer si le recueil des IIP est autorisé au titre d'un programme ou d'une activité. Cette autorisation devrait être formulée par écrit.

A.4.2 Définition du but

Objectif: Définir le but dans lequel les IIP sont recueillies, au plus tard au moment où ce recueil intervient, et restreindre l'utilisation ultérieure de ces informations aux seules activités visant à atteindre ce but original.

Mesure de contrôle

Les organisations devraient indiquer à l'entité principale des IIP qu'elles vont recueillir le ou les buts pour lesquels ces informations sont collectées, ainsi que le ou les buts dans lesquels les informations vont être traitées. Cette communication doit intervenir avant ou pendant le recueil des IIP, et avant que les informations ne soient traitées dans un ou des buts qui n'auraient pas encore été communiqués à l'entité principale.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient communiquer le ou les buts à l'entité principale des IIP avant que les informations ne soient recueillies ou utilisées pour la première fois dans un nouveau but. Elles devraient à cette fin employer des termes clairs et adaptés aux circonstances, et fournir des explications suffisantes sur la nécessité de traiter des IIP sensibles.

Les conditions statutaires autorisent souvent expressément un recueil et une utilisation spécifiques des IIP. Lorsque ces conditions sont rédigées de manière générale et sont donc sujettes à interprétation, les organisations devraient s'assurer, en consultation avec le Directeur des données personnelles et le conseiller juridique, qu'il existe un rapport clair entre l'autorisation générale et tout recueil particulier des IIP.

Une fois que les buts spécifiques ont été recensés, ils doivent être clairement décrits dans la documentation ou les formulaires connexes concernant le respect des données personnelles que les organisations emploient pour recueillir des IIP. En outre, pour éviter tout recueil ou emploi non autorisé des IIP, le personnel qui manipule ces informations doit être formé aux conditions de recueil dans l'organisation.

Les organisations devraient:

a) déterminer quelles sont les IIP utiles à leurs procédures de fonctionnement, et uniquement à ces procédures;

b) distinguer de manière logique les IIP qui sont utiles à chacune de ces procédures;

c) gérer les différents droits d'accès conformément aux procédures de fonctionnement (notamment la gestion de la paie, des demandes de vacances et des promotions) et mettre en place un environnement informatique dédié aux systèmes qui vont traiter les IIP les plus sensibles; et

d) vérifier régulièrement que les IIP sont distinguées de manière efficace et qu'aucun nouveau destinataire et aucune interconnexion n'ont été ajoutés.

A.5 Limites du recueil d'informations

Objectif: Restreindre le recueil des IIP aux informations qui sont situées dans le périmètre défini par la législation applicable et sont strictement nécessaires au(x) but(s) défini(s).

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour restreindre le recueil des IIP au type et au volume minimum d'informations requises pour atteindre le(s) but(s) décrit(s) dans la note d'information sur le respect de la vie privée (voir A.9.1) et aux informations qui sont situées dans le périmètre défini par la législation ou la réglementation applicables.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) restreindre le recueil des IIP aux éléments minimums nécessaires pour atteindre les buts décrits dans la note d'information sur le respect de la vie privée (voir A.9.1) et pour lesquels l'entité principale des IIP a donné son consentement;

b) s'abstenir de recueillir des IIP sensibles, sauf si ce recueil a été légalement autorisé ou si un consentement a été obtenu; et

c) limiter le volume d'informations qu'elles recueillent indirectement auprès ou à propos d'une entité principale (par exemple via des journaux d'accès en ligne, des journaux système).

Les organisations devraient définir le(s) but(s) du traitement des IIP, les informations nécessaires pour atteindre ce(s) but(s) et les informations qu'il n'est pas nécessaire de recueillir, et s'assurer que seules les informations essentielles sont collectées.

Elles devraient déterminer avec soin les IIP qui doivent être recueillies pour atteindre un but particulier avant de procéder au recueil. Elles ne devraient pas recueillir d'IIP de manière indiscriminée.

Les organisations devraient régulièrement réexaminer le ou les buts pour lesquels elles recueillent des IIP afin de s'assurer qu'ils sont toujours d'actualité. Elles devraient aussi réexaminer les IIP qu'elles recueillent pour vérifier qu'il s'agit toujours du minimum d'informations requis pour atteindre ce(s) but(s).

Les organisations ne devraient pas recueillir d'IIP sensibles, comme par exemple des numéros d'identification nationale, sauf si ce recueil est légalement autorisé ou qu'elles ont obtenu un consentement explicite.

Autres informations concernant la protection des IIP

Sous certaines juridictions, certaines catégories d'IIP (par exemple l'origine ethnique, les opinions politiques ou religieuses ou toute autre croyance, des données personnelles concernant la santé, l'activité sexuelle ou les condamnations pénales, etc.) peuvent être considérées comme sensibles. Ces juridictions peuvent imposer des restrictions ou des conditions au recueil de ce type d'informations. Les organisations devraient alors tenir compte de ces restrictions ou conditions lorsqu'elles décident de recueillir des IIP.

A.6 Réduction des informations au minimum

Objectif: Réduire le nombre d'IIP traitées au strict minimum nécessaire pour atteindre les buts légitimes du contrôleur des IIP, et limiter la divulgation des IIP au plus petit nombre possible de parties intervenant dans le traitement des données personnelles.

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour réduire le nombre d'IIP traitées au strict minimum nécessaire pour atteindre les buts légitimes du contrôleur des IIP (ainsi, une organisation peut chercher à accroître ou développer ses opérations commerciales, de telle sorte que le nombre d'IIP qu'elle traite et qu'elle stocke va légitimement augmenter).

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) veiller à l'adoption du principe de "besoin de connaître", c'est-à-dire que l'accès aux IIP devrait être réservé uniquement aux personnes ayant besoin de ces informations pour s'acquitter de leurs tâches officielles et atteindre le but légitime pour lequel les IIP sont traitées;

b) effectuer ou proposer par défaut, chaque fois que possible, des interactions et des transactions qui ne nécessitent pas d'identifier les entités principales des IIP;

c) limiter la possibilité de relier les IIP recueillies à des personnes;

d) effectuer une première évaluation des IIP conservées par l'organisation; établir et respecter un calendrier de révision pour s'assurer que seules les IIP définies dans la note d'information sont recueillies, et que ces IIP sont toujours nécessaires pour atteindre les buts commerciaux visés;

e) limiter la transmission de documents électroniques contenant des IIP au plus petit nombre possible de parties qui en ont besoin dans leur travail;

f) déterminer quelles IIP devraient être anonymisées et désidentifiées en fonction du contexte, du format sous lequel les IIP sont stockées (par exemple des champs de bases de données ou des extraits de textes) et des risques recensés;

g) désidentifier les informations ainsi définies; et

h) supprimer et éliminer les IIP dès lors que le but du traitement des IIP n'a plus lieu d'être, lorsqu'il n'existe pas d'obligation juridique de conservation des IIP ou lorsque cette conservation n'est pas possible; et

i) déterminer s'il est possible d'employer des technologies renforçant la protection de la vie privée (PET), et quelles technologies peuvent être appliquées.

L'ensemble minimal d'éléments d'IIP nécessaire à l'organisation pour atteindre son but commercial peut représenter un sous-ensemble des IIP que l'organisation est autorisée à recueillir.

Les IIP devraient être réparties en informations obligatoires ou facultatives aux fins du recueil. Les organisations ne devraient recueillir que les IIP dont la présence est obligatoire pour qu'elles soient en mesure de fournir leur service. S'agissant des IIP facultatives, les organisations devraient obtenir le consentement exprès des entités principales avant de les collecter. Elles ne devraient pas refuser de fournir un service à une entité principale des IIP ayant refusé de donner des IIP facultatives.

Le Directeur des données personnelles et le conseiller juridique devraient exiger des responsables du programme une justification du traitement proposé des IIP pour s'assurer qu'il s'agit bien du minimum d'informations nécessaire au système d'information ou à l'activité pour atteindre le but légalement autorisé.

NOTE 1 – L'anonymisation, telle que définie dans la norme ISO/CEI 29100, est un processus par lequel des IIP sont modifiées de manière irréversible de sorte que l'entité principale des IIP ne puisse plus être identifiée directement ou indirectement, soit par le contrôleur des IIP agissant seul, soit avec la collaboration de toute autre partie. Ce processus implique forcément une perte d'informations (irréversible). Dans certains cas, la simple suppression d'une partie des données peut permettre d'atteindre l'objectif souhaité.

NOTE 2 – Une description de certaines technologies de désidentification des données qui renforcent la protection de la vie privée, à utiliser pour décrire et concevoir des mesures de désidentification conformément aux principes de protection des données personnelles énoncés dans la norme ISO/CEI 29100, devrait faire l'objet d'une future norme internationale. D'une manière générale, pour qu'un processus de désidentification soit conforme à la législation, la désidentification est effectuée par exemple en supprimant ou en généralisant les attributs, et en prenant des mesures robustes tant sur plan organisationnel que technique.

NOTE 3 – Lorsque des IIP sont traitées dans un but particulier, ce traitement est réduit au strict minimum nécessaire pour atteindre le but souhaité, sans avoir à divulguer des informations excessives sur l'entité principale. Si par exemple il faut indiquer le lieu de résidence d'une personne répondant à une enquête sur le trafic routier, il est préférable de n'indiquer que des points de repère situés à proximité, et non l'adresse précise.

NOTE 4 – Il peut souvent arriver que l'analyse d'un jeu de données anonymisées révèle l'identité des entités principales lorsque le jeu est de taille réduite. Il est donc conseillé de ne pas constituer de jeu de données de taille inférieure à un seuil défini, par exemple 10 entrées. Ce seuil doit être établi avec précaution en fonction de la structure de répartition des données.

Les organisations devraient aussi réduire leurs risques en matière de données personnelles et de sécurité en réduisant le volume d'IIP qu'elles stockent, le cas échéant. Elles devraient procéder à un examen initial, puis à des examens ultérieurs des IIP qu'elles détiennent pour s'assurer, dans toute la mesure du possible, que ces données sont exactes, pertinentes, complètes et bien situées dans le temps.

Elles devraient d'ailleurs être encouragées à réduire le volume d'IIP qu'elles détiennent jusqu'au minimum nécessaire pour pouvoir atteindre le but commercial qu'elles se sont fixées. Elles devraient donc établir et publier un calendrier d'examens périodiques de leurs données pour compléter leur examen initial.

En menant des examens à intervalles réguliers, les organisations réduisent leur risque, s'assurent de ne recueillir que les données définies dans la note d'information et font en sorte que les données recueillies restent pertinentes et nécessaires.

A.7 Limites d'utilisation, de conservation et de divulgation

A.7.1 Limites d'utilisation, de conservation et de divulgation

Objectif: Limiter l'utilisation et la divulgation d'IIP effectuées dans des buts précis, explicites et légitimes, et ne pas conserver d'IIP plus longtemps que nécessaire pour atteindre les objectifs déclarés ou pour se conformer à la législation en vigueur.

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour limiter le traitement des IIP effectué dans des buts légitimes et définis et pour ne conserver les IIP que le temps nécessaire pour atteindre les buts déclarés ou pour se conformer à la législation en vigueur.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) limiter l'utilisation, la conservation et la divulgation (y compris le transfert) d'IIP aux opérations nécessaires pour atteindre des buts précis, explicites et légitimes; et

b) configurer leurs systèmes d'information de manière à consigner la date à laquelle les IIP sont recueillies, créées ou mises à jour, ainsi que la date à laquelle elles sont supprimées ou archivées conformément à un calendrier de conservation agréé.

Conseils de mise en œuvre pour l'utilisation des IIP

Les organisations devraient:

a) isoler (c'est-à-dire archiver, sécuriser et interdire d'accès) les IIP lorsque les buts définis ont été atteints mais que la conservation des IIP reste obligatoire en vertu de la législation applicable;

b) employer des techniques ou méthodes adéquates pour garantir une suppression ou une destruction sécurisées des IIP (originaux, copies et archives);

c) n'employer des IIP que pour atteindre les objectifs convenus ou communiqués aux entités principales avant ou pendant le recueil, et obtenir le consentement de celles-ci, le cas échéant, avant toute nouvelle opération;

d) limiter au strict minimum l'accès officiellement autorisé de tiers extérieurs aux systèmes de l'organisation et aux IIP. Si cet accès est réellement nécessaire aux activités de l'organisation, il convient de suivre les procédures d'approbation adéquates;

e) confirmer que les systèmes des tiers extérieurs auxquels des systèmes de l'organisation peuvent être connectés disposent bien des mécanismes de sécurité appropriés avant d'autoriser la connexion;

f) réexaminer régulièrement les mécanismes de sécurité mis en place par les tiers extérieurs pour s'assurer que ces mécanismes continuent de répondre aux exigences de l'organisation en matière de sécurité. Si l'examen révèle que ces mécanismes ne sont plus satisfaisants, le tiers extérieur doit être déconnecté jusqu'à ce qu'il ait démontré que des mécanismes adéquats ont été remis en place;

g) installer des mécanismes d'authentification adéquats pour les personnes souhaitant accéder aux IIP à distance. Tous les accès aux IIP doivent être consignés; et

h) informer le public, par une note d'information, de tout changement intervenu dans les IIP recueillies au cours du processus de contrôle de la sécurité.

Conseils de mise en œuvre pour la conservation des IIP

Dans certaines circonstances, en raison de la législation, des IIP peuvent être conservées plus longtemps que les buts définis de l'organisation ne l'exigent. Les organisations devraient:

a) conserver les IIP uniquement pendant la durée autorisée pour atteindre les buts définis dans la notice d'information, ou pendant la période prévue par la législation et par les organisations, et les détruire rapidement après l'expiration de ce délai;

b) s'il leur faut conserver les IIP plus longtemps que les buts définis ne l'exigent, prendre des mesures (comme la désidentification) pour protéger ces informations;

c) définir des délais de conservation des IIP qui sont limités dans le temps et adaptés aux buts du traitement;

d) confirmer que le système d'information peut détecter l'expiration du délai de conservation;

e) s'assurer que le délai de conservation convenu est respecté et que les IIP sont ensuite supprimées;

f) mettre en place une fonction qui supprime automatiquement les IIP à l'expiration de leur délai de conservation. Cette suppression devraient intervenir immédiatement ou aussitôt que possible;

g) déterminer quels éléments devraient faire l'objet d'une désidentification en fonction du contexte, du format de stockage des IIP (champs de bases de données ou extraits de textes) et des risques recensés;

h) désidentifier les éléments de données ainsi définis; et

i) choisir les moyens (notamment une destruction partielle, le hachage, le hachage par clé et l'indexation) nécessaires pour protéger les IIP si celles-ci ne peuvent être désidentifiées.

Conseils de mise en œuvre pour la divulgation des IIP

Les organisations devraient:

a) s'abstenir de divulguer des IIP à des tiers extérieurs sans en avoir préalablement informé l'entité principale et avoir obtenu son consentement, sauf si la législation autorise par ailleurs cette divulgation. L'information et le consentement de l'entité principale ne sont pas nécessairement requis lorsque la divulgation s'adresse à des tiers internes (par exemple des employés) dont le besoin de connaître est reconnu; et

b) mettre en place des mécanismes robustes de protection du transfert des IIP, fondés notamment sur le chiffrement des données et la protection de leur intégrité.

Les IIP concernant les employés devraient être détruites (c'est-à-dire supprimées de manière sécurisée ou archivées) conformément à la législation et à la réglementation en vigueur, dans le respect des politiques de destruction de l'organisation et, le cas échéant, avec le consentement de l'employé concerné.

A.7.2 Effacement sécurisé de fichiers temporaires

Objectif: Prendre les mesures techniques nécessaires pour effacer des fichiers temporaires dans le délai imparti.

Mesure de contrôle

Les fichiers et documents temporaires susceptibles de contenir des IIP devraient être supprimés dans un délai défini par écrit.

Conseils de mise en œuvre de la protection des IIP

Dans le cadre de leur utilisation normale, les systèmes d'information peuvent créer des fichiers temporaires susceptibles de contenir des IIP. Ces fichiers sont propres à une application ou un système particuliers, mais ils peuvent parfois permettre de remonter à ces informations, notamment lorsqu'ils sont associés à la mise à jour de bases de données ou à l'exploitation de tout autre logiciel. En général, les fichiers temporaires ne sont plus utiles une fois que le traitement des informations concernées est achevé; toutefois, dans certaines circonstances, ils ne peuvent être supprimés automatiquement. La durée pendant laquelle ces fichiers sont utilisés n'est pas toujours connue à l'avance, mais une

procédure de nettoyage de la mémoire devrait permettre de recenser les fichiers temporaires concernés et de déterminer combien de temps s'est écoulé depuis leur dernière utilisation.

Les systèmes d'information employés pour traiter des IIP devraient effectuer régulièrement des vérifications afin de veiller à ce que les fichiers temporaires non utilisés depuis un certain temps aient bien été supprimés.

A.7.3 Notification de la divulgation d'IIP

Objectif: S'assurer que le prestataire de services chargé de traiter les IIP a informé le contrôleur des IIP de toute demande juridiquement contraignante de divulguer ce type d'informations.

Mesure de contrôle

Le contrat entre le contrôleur des IIP et le prestataire de services chargé de traiter les IIP devrait stipuler que le prestataire doit informer le contrôleur, selon la procédure et dans le délai prévus dans le contrat, de toute demande juridiquement contraignante de divulguer des IIP adressée par des forces de l'ordre ou par toute autre autorité, sauf si la législation interdit par ailleurs cette divulgation.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient prendre des mesures (par exemple en prévoyant des obligations contractuelles) pour s'assurer:

a) que les prestataires de services chargés de traiter les IIP consultent le contrôleur des IIP avant d'accepter toute demande juridiquement contraignante de divulguer des IIP, sauf si la législation interdit par ailleurs cette divulgation; et

b) que ces prestataires acceptent toute demande de divulguer des IIP prévue dans leur contrat puisque cette demande a été autorisée par le contrôleur des IIP compétent, sauf si la législation interdit par ailleurs cette divulgation.

A.7.4 Consignation des divulgations d'IIP

Objectif: S'assurer que les divulgations d'IIP à des tiers sont consignées.

Mesure de contrôle

La divulgation d'IIP à de tierces parties devrait être consignée, en précisant notamment quelles IIP ont été divulguées, à qui elles ont été communiquées, quand et dans quel but.

Conseils de mise en œuvre de la protection des IIP

Des IIP peuvent être divulguées dans le cadre du fonctionnement normal de l'organisation. Ces divulgations devraient être consignées. Toute divulgation supplémentaire à des tiers, intervenant notamment dans le cadre d'enquêtes ou d'audits externes licites, doit également être consignée. Les enregistrements devraient indiquer la source de la divulgation et l'identité de l'autorité à laquelle les IIP ont été divulguées.

A.7.5 Déclaration de recours à des sous-traitants pour traiter des IIP

Objectif: S'assurer que les prestataires de services chargés de traiter les IIP ont dûment déclaré leur éventuel recours à des sous-traitants.

Mesure de contrôle

Tout prestataire de services chargé de traiter les IIP qui souhaite recourir à des sous-traitants pour effectuer cette tâche doit le déclarer au contrôleur des IIP préalablement à ce recours.

Conseils de mise en œuvre de la protection des IIP

La possibilité de recourir à un sous-traitant pour traiter des IIP doit être prévue dans le contrat entre le prestataire chargé de ce traitement et le contrôleur des IIP. Le contrat doit préciser que le sous-traitant ne peut être recruté qu'après autorisation du contrôleur. Le prestataire chargé de traiter les IIP devrait informer le contrôleur en temps utile de toute modification prévue à cet égard, afin que le contrôleur soit en mesure de s'opposer à cette modification ou de mettre fin à la possibilité de recruter un sous-traitant.

La déclaration publique devrait indiquer qu'il sera fait appel à des sous-traitants et préciser le nom de ceux-ci, mais elle ne doit divulguer aucun détail concernant les activités de l'organisation. Elle doit aussi indiquer les pays dans lesquels les

sous-traitants peuvent traiter des données et les moyens que les sous-traitants peuvent employer pour se conformer aux obligations imposées par le prestataire, voire pour aller au-delà de ces obligations.

Si l'on estime que la déclaration publique d'informations concernant les sous-traitants accroît le risque de sécurité au-delà des limites acceptables, cette déclaration devrait être soumise à un engagement de non-divulgation et/ou ne devrait être effectuée qu'à la demande du contrôleur des IIP. Celui-ci devrait être prévenu que les informations concernant les sous-traitants auxquels il est fait appel sont tenues à sa disposition.

A.8 Exactitude et qualité

Objectif: S'assurer que les IIP traitées sont exactes, complètes, à jour, adéquates et pertinentes au regard de leur usage prévu.

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour faire en sorte que les IIP directement ou indirectement recueillies auprès d'une entité principale présentent la qualité requise.

Conseils de mise en œuvre de la protection des IIP

Pour atteindre cet objectif de qualité, les IIP traitées doivent être exactes et précises, complètes, à jour, adéquates et pertinentes au regard de leur usage prévu.

Les organisations devraient:

a) établir des procédures de recueil des IIP qui contribuent à garantir leur exactitude et leur qualité;

b) recueillir les IIP de telle sorte que toute modification soit détectable après leur collecte auprès de la source faisant autorité;

c) Après le recueil ou la création des IIP, confirmer, dans toute la mesure du possible, l'exactitude et la pertinence de ces informations, et s'assurer qu'elles sont complètes et bien situées dans le temps;

d) pour les IIP recueillies auprès d'une source distincte de l'entité principale, s'assurer de leur fiabilité avant de les traiter;

e) vérifier, par des moyens appropriés, la validité et le bien-fondé des demandes de correction présentées par l'entité principale avant d'effectuer toute modification des IIP, le cas échéant;

f) vérifier régulièrement et au besoin corriger toute IIP inexacte ou obsolète qui doit être utilisée par des programmes ou des systèmes; et

g) publier des directives permettant de garantir et maximiser l'exactitude, la complétude, l'adéquation et la pertinence des informations diffusées. Les organisations devraient prendre des mesures raisonnables pour confirmer l'exactitude des IIP. Ces mesures peuvent notamment consister à corriger et valider les adresses à mesure qu'elles sont recueillies ou saisies dans les systèmes d'information, en se servant d'interfaces de programmation d'applications (API) pour automatiser cette vérification.

Lorsque les IIP ont une nature relativement sensible (par exemple lorsqu'il s'agit de la confirmation annuelle des revenus d'un foyer fiscal découlant d'un bénéfice récurrent), les organisations devraient intégrer des mécanismes dans les systèmes d'information et élaborer des procédures pour définir à quelle fréquence et par quelle méthode les informations doivent être actualisées.

Pour réduire dans toute la mesure du possible le risque d'inexactitude des IIP, celles-ci devraient être saisies directement dans les systèmes d'information par l'entité principale des IIP sans qu'un intermédiaire ne soit chargé de les transcrire. Néanmoins, si cette transcription des IIP est inévitable, les organisations devraient permettre à l'entité principale de valider les informations transcrites. Cette procédure contribue à rectifier les erreurs avant que le traitement d'IIP inexactes n'entraîne de dommages conséquents.

Autres informations concernant la protection des IIP

Les différents types de mesures prises pour préserver la qualité des données peuvent dépendre de la nature et du contexte des IIP, ainsi que de la manière dont celles-ci ont été obtenues et vont être exploitées. Les mesures visant à valider l'exactitude d'IIP sensibles devraient avoir une portée plus étendue que celles qui concernent des IIP moins sensibles. Il peut être nécessaire de prendre des mesures supplémentaires pour valider les IIP obtenues auprès de sources distinctes des entités principales ou de leurs représentants agréés.

A.9 Ouverture, transparence et notes d'information

A.9.1 Note d'information sur le respect de la vie privée

Objectif: S'assurer que les notes d'information sur le respect de la vie privée sont suffisamment détaillées, compréhensibles et faciles à trouver.

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour communiquer aux entités principales des IIP une note d'information sur les buts du traitement des IIP.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) adresser aux entités principales une note d'information concrète sur:

   1) leurs activités ayant une incidence sur le respect de la vie privée, en précisant notamment, mais pas uniquement, la manière dont elles recueillent, utilisent, partagent, protègent et suppriment de façon sécurisée les IIP;

   2) l'autorité en vertu de laquelle elles recueillent les IIP;

   3) les choix dont les entités principales disposent, le cas échéant, vis-à-vis de la manière dont les organisations utilisent leurs IIP et les conséquences de l'expression ou de l'absence d'expression de ces choix; et

   4) la possibilité de s'opposer au traitement;

b) fournir des mécanismes d'information et de consentement adaptés aux besoins de fonctionnement de chaque organisation;

c) revoir leurs notes d'information pour prendre en compte les changements de pratique ou de politique ayant une incidence sur les IIP, ou les changements d'activité ayant une incidence sur le respect de la vie privée, avant que ces changements n'interviennent ou aussi rapidement que possible après les changements;

d) s'assurer que la note d'information est complète et adaptée au public ciblé, selon la nature des IIP, les moyens pratiques choisis pour diffuser la note et la nature des relations entre le contrôleur des IIP et les entités principales;

e) présenter les informations de manière claire pour qu'elles puissent être comprises par une personne peu habituée aux nouvelles technologies de l'information, à l'Internet ou au jargon juridique;

f) s'assurer que la note d'information a été adressée avant ou pendant le recueil des IIP;

g) s'assurer que les IIP ne peuvent être recueillies sans que la note d'information n'ait été diffusée;

h) trouver d'autres solutions si les moyens pratiques habituels ne fonctionnent plus;

i) prévoir un moyen de démontrer que la note d'information a bien été diffusée, dans la mesure du possible;

j) si la note d'information figure sur un support matériel, l'afficher sur un panneau susceptible d'être vu par les entités principales des IIP, ou exiger que la note ou le document soient signés ou paraphés; et

k) établir une politique sur la mise en place d'étiquettes et de panneaux permettant d'informer les entités principales des IIP de la technologie employée [par exemple des systèmes fondés sur la télévision en circuit fermé (CCTV), le wifi ou les puces d'identification par radiofréquences (RFID)].

Dans la mesure du possible, la note d'information devrait être affichée bien en vue sur le lieu où les IIP vont être recueillies (l'emplacement physique, mais aussi le site web de l'organisation) sans que l'entité principale n'ait besoin de la demander.

A.9.2 Ouverture et transparence

Objectif: Communiquer aux entités principales des IIP des informations claires et facilement accessibles sur les politiques, les procédures et les pratiques du contrôleur des IIP concernant le traitement des IIP.

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour communiquer aux entités principales des IIP des informations pertinentes sur leurs politiques, procédures et pratiques en matière de traitement des IIP.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) communiquer aux entités principales des IIP des informations claires et facilement accessibles sur les politiques, les procédures et les pratiques du contrôleur des IIP concernant le traitement de ces données;

b) indiquer aux entités principales les choix du contrôleur et les moyens mis en œuvre par celui-ci pour limiter l'accès à leurs informations ainsi que le traitement, la correction et la suppression de celles-ci.

En outre, les organisations devraient:

a) indiquer quelles sont les IIP qu'elles entendent recueillir et dans quel but;

b) indiquer comment elles entendent utiliser les IIP dans leurs processus internes;

c) dans le cas où elles vont partager les IIP avec des tiers externes, indiquer les catégories de tiers concernées et le but du partage;

d) préciser si les entités principales des IIP peuvent consentir à des utilisations ou des partages particuliers de leurs informations, et comment elles peuvent exprimer leur consentement;

e) indiquer combien de temps les IIP vont être conservées;

f) indiquer si elles entendent revendre ou transmettre des données pour que celles-ci soient traitées par des organismes spécialisés dans leur analyse. Dans ce cas, elles devraient fournir des informations détaillées sur les risques auxquels les IIP sont exposées;

g) expliquer comment les entités principales des IIP peuvent accéder à leurs informations pour en demander la modification ou la correction, le cas échéant;

h) montrer de quelle manière les IIP seront protégées;

i) s'assurer que les entités principales ont bien accès aux informations concernant des activités liées à leur vie privée et sont en mesure de communiquer avec le Directeur des données personnelles;

j) fournir, sur demande, des informations concernant les atteintes à des données personnelles qui résultent ou peuvent résulter d'une violation perpétrée par le demandeur d'IIP, ainsi que toute mesure connexe que le demandeur pourrait avoir prise pour limiter les risques supplémentaires découlant de cette violation.

Les organisations devraient en outre employer différents moyens pour informer le public de leurs pratiques en matière de protection des données personnelles, en particulier, mais pas uniquement, des rapports d'évaluation des incidences sur la vie privée, des rapport concernant les données personnelles, des pages publiques sur leur site web, des courriels, des blogs et des publications périodiques (par exemple un bulletin trimestriel). Elles devraient aussi mettre à la disposition du public des adresses de courriel et/ou des numéros de téléphone pour recueillir ses réactions ou acheminer ses questions vers des services spécialisés dans les pratiques concernant la protection de la vie privée.

A.10 Participation et accès de l'entité principale des IIP

A.10.1 Accès de l'entité principale des IIP

Objectif: Permettre aux entités principales des IIP d'accéder à leurs informations, de les réviser et de vérifier leur exactitude et leur complétude.

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour permettre aux entités principales des IIP d'accéder à leurs informations et d'en obtenir la rectification ou la suppression.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) déterminer quels sont les moyens pratiques à mettre en œuvre pour permettre aux entités principales des IIP d'exercer leur droit d'accès (lorsque celui-ci est prévu par la législation). Ces personnes devraient pouvoir exercer leur droit en temps utile, par des moyens faciles à trouver et à comprendre, ces moyens devant être analogues à ceux qui ont été initialement employés pour recueillir les IIP (c'est-à-dire par courrier postal et/ou électronique);

b) analyser les cas dans lesquels les moyens pratiques choisis ne fonctionnent plus et trouver des solutions de secours, si nécessaire;

c) permettre aux entités principales des IIP d'accéder à leurs informations conservées par les organisations afin de vérifier leur exactitude et de demander des corrections, le cas échéant;

d) répondre, dans la mesure du possible, par des moyens analogues à ceux qui ont été initialement employés pour formuler la demande (si par exemple la demande a été adressée par courrier postal, la réponse devrait être envoyée par le même moyen);

e) publier des règles et autres réglementations régissant la manière dont les entités principales peuvent accéder aux IIP conservées dans les systèmes des organisations;

f) permettre aux entités principales de contester directement ou indirectement l'exactitude ou la complétude de leurs IIP, et de demander leur modification, leur correction ou leur suppression selon les besoins et les possibilités, compte tenu du contexte;

g) établir des procédures permettant aux entités principales d'exercer ces droits de manière simple, rapide et efficace, en évitant tout retard (ainsi, les réponses devraient être envoyées conformément à la législation ou la réglementation en vigueur, ou en application de la politique de l'organisation) ou tout coût inutiles;

h) instaurer une procédure pour informer les entités principales ayant présenté une demande de l'état d'avancement de celle-ci et du processus nécessaire à son traitement (on pourra notamment répondre par courrier postal ou électronique en précisant que la demande a bien été reçue et en indiquant la date à laquelle le demandeur peut espérer une réponse). Si la demande concerne des archives, le contrôleur des IIP peut annoncer une date de réponse en prenant une certaine marge, pour autant qu'il informe le demandeur de la durée moyenne de traitement des demandes et qu'il annonce un délai de réponse raisonnable;

i) dans la mesure autorisée par la législation, s'assurer que le droit d'accès peut toujours être exercé;

j) s'assurer que l'accès aux IIP est réservé à la personne concernée par ces informations ou à un agent agréé par celle-ci. Il peut donc être nécessaire d'exiger des personnes demandant un accès de s'identifier et de s'authentifier de manière satisfaisante. Les exigences concernant l'identification et l'authentification peuvent être définies dans la législation ou la réglementation applicables;

k) si l'identification et l'authentification du demandeur sont exigées, déterminer la manière la plus adéquate de le faire, sauf disposition contraire de la législation ou de la réglementation. Les organisations ne devraient demander que le minimum d'informations nécessaires pour établir l'identité de manière satisfaisante. Ces informations devraient être dûment sécurisées et ne devraient être conservées que le temps nécessaire;

l) s'assurer que les IIP ne sont envoyées qu'à l'entité principale pertinente et que leur transmission est sécurisée;

m) s'assurer que toutes les informations demandées par les entités principales peuvent être fournies tout en protégeant les IIP des autres entités principales;

n) indiquer, par le biais de notes d'information sur le respect de la vie privée, si les organisations entendent appliquer une taxe d'accès, comme la législation peut le prévoir dans certaines juridictions; et

o) exiger de tout prestataire de services chargé de traiter des IIP qu'il aide le contrôleur des IIP à faciliter l'exercice des droits de l'entité principale concernant l'accès, la correction et la suppression de ses données.

L'accès accordé aux entités principales des IIP permet à celles-ci de réexaminer les informations qui les concernent et qui sont stockées dans les systèmes d'information des organisations. Cet accès doit être simple et peu coûteux et être accordé en temps utile. Les processus mis en place par les organisations pour accorder cet accès peuvent différer selon les ressources, les dispositions légales ou d'autres facteurs.

A.10.2 Correction et participation

Objectif: Transmettre toute demande de modification, de correction ou de suppression aux prestataires de services chargé de traiter des IIP et aux tiers auxquels des données personnelles ont été divulguées.

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour permettre aux entités principales de corriger, modifier ou supprimer les IIP qu'elles conservent, sauf si la législation ou la réglementation contient des dispositions contraires. Elles devraient aussi mettre en place un mécanisme permettant de communiquer ces corrections, modifications ou suppressions aux prestataires de services chargés de traiter des IIP et, dans toute la mesure du possible, aux tiers auxquels des IIP ont été divulguées.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) s'assurer que l'entité principale est toujours en mesure d'exercer son droit de correction;

b) analyser les cas dans lesquels les moyens pratiques choisis ne fonctionnent plus et trouver des solutions de secours, si nécessaire;

c) dans la mesure autorisée par la législation ou la réglementation pertinente, s'assurer que les entités principales peuvent exercer leur droit de correction;

d) vérifier l'exactitude des corrections demandées;

e) s'assurer que les entités principales ayant présenté une demande de correction ont reçu confirmation de la réception de celle-ci;

f) s'assurer que les tiers auxquels des IIP ont pu être envoyées sont informés des corrections apportées; et

g) accorder aux entités principales un accès limité aux IIP qu'elles souhaitent corriger, modifier ou supprimer.

A.10.3 Gestion des plaintes

Objectif: Mettre en place des procédures internes efficaces de traitement des plaintes et de correction à l'intention des entités principales des IIP.

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour traiter de manière efficace les plaintes déposées par des entités principales.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient mettre en place une procédure de gestion des plaintes et mettre à disposition un point de contact chargé de recevoir les plaintes, les courriers exprimant des préoccupations et les questions adressés par des entités principales à propos des pratiques de l'organisation en matière de protection de la vie privée. Ce point de contact serait aussi chargé de répondre à ces demandes.

Les organisations devraient également instaurer des mécanismes de gestion des plaintes faciles à trouver et à utiliser pour les entités principales, et publier toutes les informations nécessaires pour que celles-ci puissent déposer leur plainte (notamment en fournissant les coordonnées du Directeur des données personnelles ou de tout autre personne chargée de recevoir les plaintes).

Ces procédures de gestion des plaintes devraient comporter des mécanismes de suivi pour s'assurer que toutes les plaintes reçues sont examinées et traitées de manière adéquate et en temps utile. Elles devraient notamment permettre de prendre des mesures correctives pour donner suite à la plainte.

Autres informations concernant la protection des IIP

Les plaintes, les préoccupations et les questions des entités principales peuvent constituer une source extérieure d'informations précieuses qui peuvent permettre, à terme, d'améliorer les modèles de fonctionnement, l'exploitation des technologies, les pratiques en matière de traitement de données et les mesures de protection des données personnelles et de la sécurité.

A.11 Responsabilité

A.11.1 Gouvernance

Objectif: Etablir un système de gouvernance efficace pour traiter les IIP.

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour établir un système de gouvernance régissant le traitement des IIP de manière efficace.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) charger une personne particulière d'élaborer, de mettre en place et d'entretenir à l'échelle de toute l'organisation un système de gouvernance et un programme de gestion des données personnelles pour faire en sorte de se conformer à toutes les lois et réglementations concernant le traitement des IIP par des programmes et des systèmes d'informations. La personne désignée pourrait être nommée Directeur des données personnelles. Il est également possible qu'un membre du conseil d'administration assume cette responsabilité avec l'aide d'un professionnel spécialisé, qui peut être un prestataire extérieur;

b) s'assurer que la personne désignée dispose des compétences requises pour superviser le traitement des IIP;

c) s'assurer que la personne désignée intervienne sur toutes les questions touchant à la protection des IIP et puisse rendre compte directement à la haute direction en temps utile;

d) fournir à la personne désignée le personnel, les locaux, les équipements et les autres ressources nécessaires pour qu'elle puisse s'acquitter de ses tâches;

e) mettre en place un processus permettant d'observer l'évolution de la législation et des politiques concernant la vie privée afin de détecter les changements susceptibles d'avoir une incidence sur le programme de protection des IIP;

f) élaborer, diffuser et mettre en œuvre des politiques et procédures pratiques de protection des IIP pour régir la protection de ces informations et les mesures de contrôle de la sécurité visant les programmes, les systèmes d'information ou les technologies employées pour traiter des IIP;

g) actualiser régulièrement les plans, politiques et procédures de protection des IIP; et

h) contrôler régulièrement les résultats de l'organisation en matière de protection des IIP. Un membre de la haute direction ou du conseil d'administration devrait diriger cette activité en s'appuyant notamment des mesures quantitatives et des évaluations des risques et des cas de violation. Des analyses de ce type devraient être effectuées non seulement en cas de besoin, mais aussi de manière régulière sans avoir été déclenchées par un événement particulier.

A.11.2 Evaluation des incidences sur la vie privée

Objectif: Mettre en place une procédure d'évaluation des incidences sur la vie privée et appliquer cette procédure en cas de besoin.

Mesure de contrôle

Si une organisation est amenée à traiter des IIP, elle doit mettre en place les procédures nécessaires pour mener une EIVP.

Conseils de mise en œuvre de la protection des IIP

Une évaluation des risques concernant les données personnelles est généralement effectuée par une organisation qui prend ses responsabilités au sérieux et dont le comportement vis-à-vis des entités principales des IIP est satisfaisant. Sous certaines juridictions, une EIVP peut être nécessaire pour se conformer à des prescriptions légales ou réglementaires. La norme ISO/CEI 29134 contient un certain nombre de conseils dans ce domaine.

Les organisations devraient prendre en compte les actifs, les menaces, les vulnérabilités et les mesures de protection (existantes et envisagées) pour évaluer ces risques. Elles devraient documenter:

a) les résultats de l'EIVP, et notamment les IIP faisant l'objet d'un traitement;

b) les risques recensés en matière de données personnelles; et

c) les mesures de limitation des risques proposées.

A.11.3 Exigences visant les prestataires et les sous-traitants en matière de protection des données personnelles

Objectif: S'assurer, par le biais de contrats ou d'autres moyens tels que des politiques internes obligatoires, que les tiers auxquels sont communiquées des IIP garantissent à celles-ci un niveau de protection au moins équivalent à celui des organisations.

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour s'assurer que les prestataires de services et les sous-traitants chargés de traiter des IIP ont pris des mesures garantissant un niveau de protection adéquat de ces informations.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) définir, dans l'accord sur les niveaux de service, les exigences en matière de protection des IIP auxquelles les prestataires doivent satisfaire;

b) contrôler et auditer la mise en œuvre des mesures prises à cet égard par les prestataires;

c) définir les fonctions et les responsabilités des prestataires de services et des sous-traitants en matière de protection des IIP;

d) définir contractuellement l'objet et le délai de la prestation du service, ainsi que la portée de celui-ci, la manière dont les IIP seront traitées et le but de ce traitement, et les types d'IIP à traiter;

e) préciser les conditions dans lesquelles un prestataire chargé de traiter des IIP devrait retourner les informations ou les supprimer de manière sécurisée après avoir achevé son service, ou à la fin de tout contrat régissant ce service, ou encore à la demande du contrôleur des IIP;

f) prévoir une clause de confidentialité contraignante aussi bien pour le prestataire que pour l'ensemble de ses employés susceptibles d'avoir accès aux IIP;

g) s'assurer que le prestataire ne communique pas les IIP à des tiers, même à des fins de conservation, à moins qu'il ne soit spécifiquement autorisé à le faire en vertu du contrat;

h) définir l'obligation du prestataire d'informer le contrôleur des IIP en cas d'atteinte à des données ayant une incidence sur les IIP;

i) imposer contractuellement au prestataire d'informer le contrôleur des IIP de tout changement pertinent concernant les services qu'il fournit, et en particulier l'exécution de fonctions supplémentaires; et

j) documenter et communiquer selon les besoins toutes les politiques, procédures et pratiques en matière de protection des IIP.

Les organisations devraient consulter leur conseiller juridique, leur Directeur des données personnelles et leurs responsables des contrats pour s'informer des lois, directives, politiques ou réglementations susceptibles d'avoir une incidence sur la mise en œuvre de ces mesures de contrôle.

NOTE – Les autres conseils de mise en œuvre figurant au § 15.1.2 sont également appliqués.

Autres informations concernant la protection des IIP

Les prestataires de services et les sous-traitants chargés de traiter des IIP peuvent notamment être des bureaux de services, des fournisseurs d'informations, des spécialistes du traitement de l'information et tout autre organisme spécialisé dans la mise en place de systèmes d'information, dans les services informatiques ou dans les applications externalisées.

A.11.4 Contrôle et audit de la protection des données personnelles

Objectif: Contrôler et auditer les mesures de protection des IIP ainsi que l'efficacité de la politique interne de protection de ces informations.

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour contrôler et auditer régulièrement les mesures de protection des données personnelles ainsi que l'efficacité de la politique interne de protection de ces données.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) contrôler et auditer régulièrement les opérations de traitement des IIP, notamment celles qui visent des IIP sensibles, pour s'assurer qu'elles respectent la législation et la réglementation applicables ainsi que les conditions des contrats;

b) contrôler et auditer régulièrement les mesures et politiques de protection des IIP pour s'assurer qu'elles respectent la législation et la réglementation applicables ainsi que les conditions des contrats;

c) s'assurer que les audits sont effectués par des personnes qualifiées et indépendantes (qu'elles soient internes ou externes à l'organisation); et

d) si leurs audit sont effectués par des ressources internes, charger régulièrement un tiers externe de mener un audit pour disposer d'une évaluation indépendante.

A.11.5 Sensibilisation et formation à la protection des IIP

Objectif: Sensibiliser et former convenablement à la protection des IIP le personnel du contrôleur des IIP ayant accès à ces informations.

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour former convenablement le personnel du contrôleur des IIP.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) instaurer et conserver une stratégie globale de formation et de sensibilisation pour s'assurer que le personnel comprenne ses responsabilités et les procédures en matière de protection des IIP;

b) mettre en place des mécanismes permettant de tenir le personnel chargé de protéger les IIP informé de l'évolution de l'environnement réglementaire, contractuel et technologique lorsque cette évolution peut avoir une incidence sur la manière dont les organisations s'acquittent de leurs obligations en la matière;

c) assurer régulièrement (par exemple chaque année) ou selon les besoins (par exemple après un incident) une formation de base sur la protection des IIP, ainsi qu'une formation ciblée par fonction. Ces formations sont particulièrement importantes pour les personnes qui traitent des IIP de manière relativement peu fréquente; et

d) s'assurer, à intervalles réguliers, que le personnel accepte officiellement (manuellement ou par voie électronique) ses responsabilités en matière de protection des IIP.

A.11.6 Rapports sur la protection des IIP

Objectif: Etablir, diffuser et actualiser des rapports sur la protection des IIP.

Mesure de contrôle

Les organisations devraient établir, diffuser selon les besoins et actualiser des rapports (par exemple sur des atteintes aux données personnelles, ou des rapports d'enquête ou d'audit) destinés à la haute direction et au personnel chargé de contrôler la protection des IIP. Ces rapports permettent de montrer que les organisations assument leurs responsabilités vis-à-vis des obligations imposées par la législation ou la réglementation en matière de protection des IIP.

Conseils de mise en œuvre de la protection des IIP

En s'appuyant sur des rapports externes et internes concernant la protection des IIP, les organisations devraient promouvoir la responsabilité et la transparence dans ce domaine. Ces rapports aident aussi les organisations à faire le point sur les progrès accomplis en termes de respect des obligations de protection des IIP, ainsi qu'au regard des mesures prises dans ce domaine. Ils permettent à chaque organisation de comparer les résultats de ses différents services, de détecter ses vulnérabilités et les lacunes de ses politiques ou de leur mise en œuvre, et de recenser les modèles les plus efficaces.

A.12 Sécurité des informations

Objectif: S'assurer que les IIP sont correctement protégées en s'appuyant sur les conclusions d'une évaluation des risques.

Mesure de contrôle

Les IIP conservées et protégées par l'organisation devraient bénéficier de mesures de protection adéquates qui devraient être choisies en fonction des conclusions d'une évaluation des risques ou d'une EIVP.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) protéger les IIP par des mesures adéquates aux niveaux opérationnel, fonctionnel et stratégique pour garantir l'intégrité, la confidentialité et la disponibilité de ces informations, et en particulier les protéger contre certains risques tels qu'un accès non autorisé, la destruction, l'utilisation, la modification, la divulgation ou la perte tout au long de leur cycle de vie;

b) choisir des prestataires pour traiter les IIP ainsi que les contrats correspondants de manière à offrir des garanties suffisantes en termes de contrôle organisationnel, physique et technique des processus appliqués aux IIP, et s'assurer que ces mesures de contrôle sont bien appliquées;

c) prendre des mesures de protection de la sécurité qui soient fondées sur des prescriptions légales, des normes de sécurité, les résultats d'une évaluation systématique des risques de sécurité effectuée conformément à la norme ISO 31000, et les résultats d'une analyse coûts-avantages;

d) restreindre l'accès aux IIP en ne l'accordant qu'aux personnes en ayant besoin pour s'acquitter de leurs tâches, et limiter cet accès aux informations dont elles ont précisément besoin;

e) trouver des solutions aux vulnérabilités et aux risques détectés grâce à des évaluations de risque ou à des audits; et

f) réexaminer et réévaluer régulièrement les mesures de contrôle dans le cadre d'un processus permanent de gestion des risques de sécurité.

Il arrive que les prescriptions en matière de sécurité soient définies dans certaines lois sur la protection des données personnelles. Leur mise en œuvre devrait alors être confiée aux personnes chargées d'assurer la sécurité des données.

La conception et la mise en œuvre des mesures de sécurité sont soumises au principe de diligence due.

A.13 Respect de la vie privée

A.13.1 Respect de la vie privée

Objectif: Se prémunir contre les violations d'obligations légales, statutaires, réglementaires, contractuelles ou découlant de politiques relatives aux données personnelles, et contre les violations de toute autre prescription dans ce domaine.

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour s'assurer que leur traitement des IIP est conforme aux obligations en la matière.

Conseils de mise en œuvre de la protection des IIP

Les organisations devraient:

a) établir un rapport annuel détaillant les risques courants, exposant la situation dans le domaine du respect de la vie privée et comportant un résumé des mesures en cours d'application; et

b) appliquer des processus bien définis de réaction en cas d'atteinte à des données personnelles. Sous certaines juridictions, il peut notamment être obligatoire d'informer les entités principales des IIP ainsi que d'autres autorités (par exemple les personnes responsables de la protection des données).

A.13.2 Restrictions au transfert de données transnational sous certaines juridictions

Objectif: Protéger les IIP lorsqu'elles sont transférées vers d'autres pays.

Mesure de contrôle

Les organisations devraient prendre les mesures nécessaires pour s'assurer que tout transfert d'IIP vers d'autres pays s'effectue conformément aux prescriptions en matière de respect de la vie privée.

Conseils de mise en œuvre de la protection des IIP

Lorsqu'il est nécessaire de transférer des IIP vers un pays distinct du territoire sur lequel les IIP sont stockées, la réglementation de certaines juridictions relative à la protection des données personnelles peut prévoir un certain nombre de restrictions, qui sont fréquemment choisies parmi les éléments suivants:

a) la notification de l'autorité chargée de protéger ces données;

b) l'approbation de ladite autorité, en particulier si les données sont sensibles;

c) une analyse permettant de s'assurer que les IIP transférées bénéficient dans le pays de destination d'une protection équivalente à celle du pays d'origine; et

d) l'application de dispositions propres au transfert de données, par exemple des clauses contractuelles types ou des règles d'entreprise contraignantes (REC).

Les organisations devraient aussi déterminer si des restrictions particulières s'appliquent au transfert prévu et s'y conformer avant d'effectuer le transfert.

Bibliographie

- BSI 10012, *Specification for a personal information management system* (en anglais seulement).
- Commission européenne, *Rapport d'évaluation concernant la directive sur la conservation des données* (directive 2006/24/CE), 2011.
- ISO/CEI 27000:2016, *Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Vue d'ensemble et vocabulaire*.
- ISO/CEI 27001, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences*.
- ISO/CEI 27005, *Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information*.
- ISO/CEI 27009, *Technologies de l'information – Techniques de sécurité – Application de l'ISO/CEI 27001 à un secteur spécifique – Exigences*.
- ISO/CEI 27018, *Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII*.
- ISO/CEI 29134, *Technologies de l'information – Techniques de sécurité – Etude d'Impacts sur la Vie Privée – EIVP*.
- *Electropedia de la CEI*. Disponible (consultée le 06.07.2017) à l'adresse: http://www.electropedia.org/.
- *Plate-forme de navigation en ligne de l'ISO*. Disponible (consultée le 06.07.2017) à l'adresse: http://www.iso.org/obp.
- *Base de données des termes et définitions de l'UIT*. Disponible (consultée le 07.07.2017) à l'adresse: http://www.itu.int/ITU-R/go/terminology-database.
- KCS, *Personal information management system*, décembre 2011 (en anglais seulement).
- Publication spéciale du NIST 800-53, Annexe J, *Security and privacy controls for federal information systems and organizations*, juillet 2011 (en anglais seulement).
- Publication spéciale du NIST 800-122, *Guide to protecting the confidentiality of personally identifiable information (PII)*, avril 2010 (en anglais seulement).

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2017