Federal Information Security Policy Guideline

Guide pour la protection des données à caractère personnel

21/11/2019

FISPDOC07 V2.1

Remarque importante : ce document est un guide qui résulte d'une collaboration entre des experts en sécurité de l'information des différents services fédéraux (SPF, OIP, IPSS). Les mesures proposées sont considérées comme des avis raisonnablement applicables de manière commune à tous les services fédéraux. Elles se basent sur des normes internationales, des bonnes pratiques dans le domaine de la sécurité de l'information ainsi que sur les expériences des participants au groupe de travail FISP.

Si des mesures plus strictes sont nécessaires à un service fédéral pour des raisons réglementaires ou pour d'autres raisons formelles et contraignantes, il va de soi que ces mesures prévalent sur celles décrites dans le présent guide.

FISP

Groupe de travail

.be

TABLE DES MATIÈRES

Contenu du présent document

Orientation du document

Ce document fait partie intégrante de la méthodologie relative à la sécurité de l'information au sein de l'administration fédérale (projet FISP).

Objectif de sécurité du document

Ce document décrit les exigences en matière de sécurité de l'information telles que définies par le règlement général sur la protection des données (RGPD). Il contient également une catégorisation standardisée basée sur l'interprétation du groupe de travail FISP.

Champ d'application

Ce guide pour le respect de la vie privée et la sécurité s'applique à toutes les informations personnelles traitées par l'administration fédérale (et ses prestataires de services).

Confidentialité du document

Distribution publique

Clause de non-responsabilité

Les informations contenues dans ce document ne peuvent pas être utilisées individuellement comme documentation de référence. Ce document ne peut pas servir de substitut à la législation, mais vise à guider le lecteur dans la prise de mesures de sécurité appropriées et l'évaluation des catégories de données à caractère personnel.

Responsabilités

Ce document est destiné au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de l'administration fédérale, aux sous-traitants de l'information (y compris les sous-traitants de systèmes d'informations) ainsi qu'aux autres intervenants dans des domaines connexes (ex. le gestionnaire de documents).

Propriétaire

Le groupe de travail FISP est propriétaire du présent document.

Introduction

Avec l'utilisation accrue des informations personnelles, leur valeur, le partage de celles-ci entre services et la complexité croissante des systèmes ICT, il est plus difficile pour une organisation de garantir la protection des données et de se conformer aux différentes lois applicables. Les intervenants dans le domaine de la protection des données peuvent éviter toute incertitude et méfiance en traitant correctement les problèmes et en empêchant l'exploitation abusive d'informations personnelles.

Afin d'éviter toute confusion, nous employons les termes « **protection des données** » pour désigner la protection et la gestion des **données personnelles** telles qu'elles sont décrites dans le **RGPD**.

Les termes « **sécurité de l'information** » renvoient quant à eux aux mesures plus générales en matière de sécurité des **données d'entreprises** relevant des BSG et de la norme ISO 27001.

La protection des données à caractère personnel recoupe donc en partie la gestion de l'information et la sécurité de l'information, et s'est vu doter d'une nouvelle dimension avec la publication et l'entrée en vigueur du RGPD du Parlement européen et du Conseil. Tout gouvernement est soumis aux règles du RGPD dès qu'il traite des données à caractère personnel.

La sécurité de l'information (ainsi que la protection des données) repose sur trois piliers qui doivent être accordés entre eux : « PPT » ou « Personnes, Processus et Technologie ». Il est essentiel que chacune de ces trois activités soit maintenue en équilibre afin d'assurer une sécurité suffisante.

Ce document n'est qu'une synthèse sommaire des exigences en matière de protection des données définies par le RGPD. Son but n'est pas d'aligner les règles de votre organisation sur celles du RGPD. Il ne se veut pas non plus une interprétation du RGPD, mais propose une série de mesures pratiques de sécurité en vue de garantir la protection des données. En outre, il contient une catégorisation standardisée définie par le groupe de travail FISP. Tous les principes du RGPD qui n'ont pas été abordés restent d'application, tout comme les autres lois, réglementations et mesures globales de sécurité qui s'appliquent à votre organisation fédérale.

Cadre légal

Les organisations sont tenues pour diverses raisons de protéger les données à caractère personnel : pour se conformer aux exigences légales et réglementaires, pour exercer leur responsabilité d'entreprise, pour renforcer la confiance du consommateur...

Règlement général sur la protection des données (RGPD)

Il existe plusieurs obligations légales visant à garantir la protection de données. Les organisations fédérales doivent donc agir dans le respect des lois spécifiques qui s'appliquent à leur cas. Le règlement général sur la protection des données du Parlement européen et du Conseil approuvé le 27 avril 2016 est récemment entré en vigueur à la date du 25 mai 2018 (RGPD)[1]. À celui-ci s'ajoute la loi fédérale belge du 30 juillet 2018 dans laquelle le gouvernement belge s'est efforcé d'adapter sa propre réglementation.

L'idée principale de ce nouveau règlement est que les personnes physiques doivent avoir le contrôle de leurs données à caractère personnel. C'est pourquoi le RGPD contient une liste d'exigences et de directives que l'on peut résumer en trois concepts : transparence - personnes concernées - sécurité. Vous trouverez évidemment d'autres principes dans la norme ISO/IEC 29100.

Transparence : l'on exige de l'organisation qu'elle comprenne et contrôle parfaitement le traitement des données (collecte, conservation, processus, droits d'accès...). Les processus doivent être documentés et, dans la plupart des cas, l'organisation doit informer la personne concernée des activités de traitement (avec certaines exceptions).

Personnes concernées : conformément au RGPD (art. 4, § 1er), une personne physique identifiée ou identifiable. Le règlement vise à protéger les personnes et prévoit davantage de droits pour les personnes dites concernées. Chaque organisation doit donc en tenir compte et mettre en place un processus / une procédure pour répondre à la demande de la personne concernée.

Sécurité : outre la documentation et les droits des personnes concernées, l'organisation doit protéger de manière suffisante toutes les données qu'elle traite et prendre les mesures de sécurité adéquates.

Traitement

Le terme 'traitement' tel que défini à l'article 4, § 2 du RGPD couvre presque toutes les actions : la collecte, la conservation, l'enregistrement, l'envoi, la consultation, l'utilisation, l'adaptation, la structuration...

Le 'responsable du traitement' (le donneur d'ordre du traitement de l'information) est la partie qui détermine la catégorie (ou la sensibilité, la confidentialité) de l'information et qui communique avec le 'destinataire'. Le sous-traitant est l'organisation qui traite des données à caractère personnel pour le compte du responsable du traitement.

Pour pouvoir traiter des données à caractère personnel, les personnes concernées doivent être informées du traitement. Il faut leur communiquer les finalités, la façon dont sont traitées les données, le type de données collectées, l'identité des destinataires de ces données et les droits dont elles disposent en matière de protection des données.

[1] Art. 3 du RGPD

Qu'entend-on par 'données à caractère personnel' ?

L'article 4 1) du RGPD définit les 'données à caractère personnel' comme suit : *« toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ; ».*

Il s'agit donc de toutes les informations qui concernent directement une personne ou qui permettent de remonter jusqu'à cette personne, même indirectement.

Les données électroniques ou techniques – comme des noms d'utilisateur, des adresses réseau (MAC), des adresses IP, des comptes de médias sociaux et même des tweets – qui peuvent être reliées à une personne physique individuelle sont elles aussi considérées comme des données à caractère personnel.

Rôles et responsabilités

Une autorité publique doit nommer un DPO, ou délégué à la protection des données. Comme le stipule l'article 37, § 3 du RGPD, un seul délégué à la protection des données peut être désigné pour plusieurs autorités publiques ou organismes publics, compte tenu de leur structure organisationnelle et de leur taille.

Il est par ailleurs possible de faire appel à un délégué à la protection des données externe. Il incombe également à la direction de prévoir les mesures minimales pour se conformer au RGPD et de fournir les preuves utiles à cet égard.

Consultez le kit de démarrage FISP pour en savoir plus sur les rôles et responsabilités.

Protection des données dès la conception et par défaut

Conformément aux principes de « protection des données dès la conception et par défaut » du RGPD, l'on attend d'une organisation fédérale qu'elle tienne compte des dernières évolutions en matière de protection des données lorsqu'elle (ou avant qu'elle) lance un nouveau processus ou projet[2]. En prenant en compte les mesures de protection des données dès le début du développement, l'on est en règle avec la réglementation en vigueur plus tôt et l'on évite les coûts supplémentaires qu'aurait engendré la prise de ces mesures à un stade ultérieur.

Les organisations fédérales sont donc encouragées à mettre en œuvre des mesures techniques et organisationnelles dès les premières étapes de la conception des opérations de traitement, de manière à préserver dès le départ les principes en matière de protection des données. Par défaut, elles doivent s'assurer que les données à caractère personnel sont traitées selon le niveau le plus élevé de protection[3]. La protection par défaut peut être considérée comme une partie de la protection dès la conception.

Protection des données dès la conception

La protection dès la conception stipule que chaque action en lien avec le traitement de données à caractère personnel que pose une entreprise doit l'être à des fins de protection des données. Cela comprend les projets internes, le développement de produits, le développement de logiciels, les systèmes IT et bien plus encore. Dans la pratique, cela signifie que tous les départements (et pas seulement le département IT) qui traitent des données à caractère personnel doivent s'assurer que la protection des données est intégrée dans un système tout au long du cycle de vie du système ou du processus. Dès le développement d'applications, de services et de produits traitant des données, le responsable du traitement prend donc les mesures techniques et organisationnelles adéquates pour mettre en œuvre les principes relatifs à la protection des données.

La protection dès la conception débute par une évaluation de la sécurité et une évaluation de l'impact sur la vie privée (PIA). En fonction de la situation, il peut être également nécessaire de réaliser une analyse d'impact relative à la protection des données (AIPD, mieux connue sous son abréviation en anglais : DPIA). Celle-ci peut aider à définir clairement les mesures qu'il faut prendre lors de la création d'un nouveau service ou de la conception d'un nouveau traitement de données.

L'article 35 du RGPD et la décision du Secrétariat Général n° 1/2019 du 16 janvier 2019 précisent dans quels cas une AIPD est requise[4].

Les mesures techniques et organisationnelles qui sont abordées dans la suite de ce document portent spécifiquement sur la **protection des données à caractère personnel** et pas sur l'organisation du RGPD au sein de l'autorité ou de l'organisme public. Il existe par ailleurs d'autres mesures pour la protection dès la conception qui ne s'appliquent pas uniquement aux données à caractère personnel (c'est la **protection des données**), mais à **tous les types de données d'entreprise** (donc la **sécurité de l'information**). Celles-ci restent aussi d'application. Le contrôle d'accès qui sert à limiter l'accessibilité des profils utilisateur dès le départ de sorte que ceux-ci ne soient pas accessibles par défaut à un nombre illimité de personnes en est un exemple. Pour y arriver, on peut par exemple utiliser :

[2] Art. 25 du RGPD
[3] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_fr
[4] https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/01_2019_SG.pdf

- un coffre-fort de données électroniques ;
- un contrôle d'accès physique ;
- un contrôle d'accès logique ;
- l'authentification et l'autorisation ;
- [5]…

Sur le plan organisationnel, il faudrait passer à la tenue d'une matrice d'autorisation et de journaux de bord[6]. L'accès doit aussi être établi sur la base d'un principe de *need-to-know* et *need-to-access*. Toutefois, quand il est impossible d'intégrer dès le départ le contrôle d'accès requis, il y a encore une solution alternative qui consiste à prévoir des journaux d'accès pouvant être vérifiés rétrospectivement.

Protection des données par défaut

Afin d'être en mesure de démontrer qu'elles respectent le RGPD, les organisations fédérales doivent également adopter des **règles internes** et mettre en œuvre des mesures qui respectent les principes de protection des données par défaut. Le principe de base est que les données à caractère personnel ne peuvent pas être traitées, et que par défaut, seules celles qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel sont rendues accessibles à un nombre déterminé de personnes physiques uniquement par l'intervention de la personne physique concernée. Pour ce faire, l'on peut par exemple prévoir :

- un paramètre par défaut « data friendly » ;
- **une obligation d'information** sur chaque application / processus concernant la façon dont les données sont traitées, les mesures de sécurité prises, la finalité... pour garantir la transparence ;
- que les données à caractère personnel ne soient jamais visibles publiquement par défaut. Ce principe de cloisonnement des données à caractère personnel vaut pour toutes les applications ICT : des paramètres du navigateur à une application d'entreprise ;
- une interface utilisateur transparente ;
- …

Sur le plan organisationnel, il faudrait passer à l'enregistrement des consentements (avec opt-in) et des permissions.

Exigences obligatoires en matière de protection des données à caractère personnel

Documentation des activités de traitement[7]

Selon le principe de responsabilité, l'organisation fédérale doit tenir des documents démontrant qu'elle garantit la protection des données à caractère personnel conformément au RGPD. Toutes les actions et tous les documents réalisés à chaque stade du traitement doivent être régulièrement mis à jour afin de garantir une protection constante et adéquate des données.

[5] Pour les mesures pratiques, nous vous renvoyons au document 'FISP - IAM & PAM'.
[6] Pour plus d'informations sur le logging, consultez le document « FISP - Guide pour le logging».
[7] Art. 30 du RGPD

Vue d'ensemble des activités de traitement

Dès le début du projet, chaque organisation doit tenir une vue d'ensemble des activités de traitement qui sont réalisées[8]. Comme une description des mesures de sécurité techniques et organisationnelles, entre autres. Pour ce faire, elle peut par exemple :

- établir un registre sous forme écrite ou format électronique ;
- tenir un registre des atteintes à la sécurité (fuites de données à caractère personnel) ;
- tenir un registre du processus de suppression des données à caractère personnel ;
- …

Minimisation des données[9]

Conformément au principe de la proportionnalité, les organisations fédérales doivent déterminer quelles sont les données à caractère personnel minimales nécessaires à la mission / au traitement, et seules ces données peuvent être traitées. Si des données à caractère personnel ne sont pas requises pour le traitement, elles ne peuvent pas être collectées ni traitées. Pour ce faire, l'on peut :

- collecter les données qui sont strictement nécessaires ou supprimer directement les données inutiles ;
- appliquer une clause de non-responsabilité (disclaimer) sur chaque application / processus concernant la façon dont les données sont traitées, les mesures de sécurité prises, la finalité... ;
- adapter les formulaires (web) à compléter de sorte que l'on sache clairement quels champs doivent être obligatoirement remplis et ceux qui sont facultatifs ;
- …[10]

Sur le plan organisationnel, il faudrait définir clairement l'objectif et y énumérer les données nécessaires.

Suppression / délais de conservation[11]

Le RGPD prévoit grosso modo quatre phases pour la conservation de données à caractère personnel (certains modèles comprennent des étapes plus détaillées, mais cela va trop loin dans le cadre de ce document).

1. **La phase de création** : c'est le début du cycle dans lequel les données sont créées, extraites ou collectées, chez l'utilisateur même, par l'organisation même ou par d'autres organisations (des parties tierces ou d'autres responsables du traitement).
2. **La phase de conservation** : les données sont conservées d'une manière ou d'une autre pour être utilisées plus tard (ou immédiatement).
3. **La phase d'utilisation** :
    a. **Utilisation active** : c'est la période durant laquelle l'organisation fédérale a encore besoin des données. Les données à caractère personnel sont uniquement traitées en vue d'atteindre la/les finalité(s) de traitement définie(s) par le responsable du traitement. L'organisation fédérale ne doit pas encore archiver les données à caractère personnel durant cette phase.
    b. **L'archivage** : c'est la période durant laquelle l'organisation fédérale a peut-être encore besoin des données à caractère personnel ou durant laquelle l'on décide de les archiver. Durant cette phase, les données sont conservées pour des raisons administratives ou des obligations juridiques. Par

[8] Il y a des exceptions à l'article 30 du RGPD.
[9] Art. 5, alinéa 1er, point c) du RGPD
[10] Plusieurs obligations se trouvent aussi dans la loi « Only Once ».
[11] Art. 5, alinéa 1er, point e) du RGPD

exemple quand un traitement ultérieur est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques. Il faut également tenir compte de la loi relative aux archives.

4. **La phase de suppression** : il s'agit de la phase durant laquelle l'organisation fédérale n'a nullement besoin / n'a plus besoin des données à caractère personnel, il n'y a plus de finalité de traitement. Il faut s'assurer, durant cette phase, que les données à caractère personnel ne sont plus conservées, du moins plus sous la forme de données à caractère personnel.

Les données doivent être finalement supprimées, détruites ou anonymisées dans le respect des délais de conservation légaux prévus dans la législation et la réglementation. L'organisation fédérale devra également fournir des preuves de ce processus.

Sur le plan technique, l'on peut répondre à ces exigences de protection par :

- la suppression automatique ;
- le marquage des données après l'expiration du délai de conservation ;
- des « sticky policies » ou règles associées aux données et indissociables de celles-ci ;
- le « data fading » ou masquage de données ;
- un journal ou un rapport d'audit qui fournit la preuve de la suppression ;
- …

Sur le plan organisationnel, il est conseillé d'élaborer une politique qui reprend les délais de conservation et règle la gestion des déchets électroniques (tant les anciens documents que les anciens appareils qui peuvent contenir des informations).

Mesures techniques supplémentaires pour la protection des données à caractère personnel

À l'issue de l'évaluation de la sécurité, de la PIA et de l'éventuelle AIPD, l'organisation fédérale peut prendre des mesures de protection supplémentaires. Au moins une des mesures de protection supplémentaires reprises ci-dessous doit être mise en place.

Une fois les mesures techniques et organisationnelles mises en œuvre, il faut également tester et évaluer l'efficacité de ces mesures à intervalles réguliers.

En outre, l'organisation fédérale devra prendre les mesures requises pour garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ainsi que prévoir une procédure permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique.

Anonymisation des données à caractère personnel

L'anonymisation permet de garantir qu'il est impossible de revenir à la base de l'information originale.

IMPORTANT : l'anonymisation garantit en TOUTE circonstance qu'il est impossible d'identifier des personnes. Par contre, quand il est possible d'identifier des personnes grâce à d'autres sources (même à un stade ultérieur, avec d'autres techniques ou des techniques plus récentes), l'on parle alors de pseudonymisation.

Il faut donc faire bien attention à ne plus parler de données anonymisées quand une personne peut être identifiée à l'aide de différentes sources de données, de la corrélation d'informations... Dans la pratique, la vraie anonymisation est un processus particulièrement complexe, et l'on utilise la pseudonymisation jusqu'à un niveau

où l'identification devient vraiment très difficile ou coûteuse. Mais le progrès technique permet de rendre possible beaucoup de choses qui n'existaient pas auparavant. Il convient donc d'être très attentif afin que les données restent toujours suffisamment protégées.

Chiffrement / codage

Le cryptage ou chiffrement est l'une des mesures techniques à laquelle on peut recourir pour protéger des informations dès le début. Si elle opte pour cette technique, l'organisation doit aussi tenir compte du fait qu'elle doit pouvoir répondre aux demandes des personnes concernées et doit donc pouvoir retrouver rapidement des informations. Il existe différents types de cryptage :

- le cryptage de clé publique ;
- le cryptage de disque ;
- le pseudo-identificateur polymorphe ;
- …

Pour plus d'informations, nous vous renvoyons au document, Guide pour la cryptographie (FISPDOC03).

Pseudonymisation des données à caractère personnel

La pseudonymisation consiste à remplacer des informations permettant d'identifier une personne par des identifiants factices. Pour ce faire, l'on peut par exemple :

- se défaire des caractéristiques qui permettent d'identifier directement ;
- avoir recours au hachage ;
- masquer les données (« data masking ») ;
- brouiller les données (« data obfuscation ») ;
- utiliser la segmentation en unités (« tokenization ») ;
- …

Sur le plan organisationnel, il faudrait élaborer une politique visant à conserver séparément les données d'identification et les autres données.

Les organisations fédérales devraient s'efforcer d'appliquer un maximum ces mesures dans le cadre du processus des journaux d'audit. Par exemple, si l'organisation fédérale agit en tant que sous-traitant, elle ne peut conserver qu'un identifiant de tâche et un identifiant utilisateur, et demander au responsable du traitement de tracer le vrai nom de l'utilisateur. Pour plus d'informations sur le logging, consultez le document « FISP - Guide pour le logging»..

Logging de « qui / quoi / quand »

Le logging permet de savoir qui a consulté certaines données ou un certain dossier à quel moment. Voir le « FISP - Guide pour le logging»..

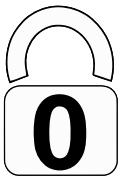
Protection des données à caractère personnel en pratique

Catégorisation de l'information

Afin de se conformer aux règles, chaque organisation doit être en mesure de répondre à la demande de toute personne de faire valoir ses droits (accès, modification, effacement...). La classification des données s'avère donc particulièrement utile et importante pour pouvoir répondre à cette demande. Celle-ci doit tenir compte des données à caractère personnel qui sont traitées par l'organisation. L'organisation fédérale doit être en mesure d'identifier et de localiser de telles données à caractère personnel « sensibles » pour pouvoir ensuite les protéger correctement.

Dans le but de garantir une certaine uniformité dans l'approche des données à caractère personnel, l'administration fédérale souhaite travailler avec plusieurs définitions standard de types de données courantes. Ces données à caractère personnel et leur relation spécifique avec la catégorisation de l'information permettent d'interpréter de façon uniforme les mesures nécessaires pour empêcher un usage inapproprié ou abusif des données à caractère personnel. L'objectif final est de traiter les données à caractère personnel le plus correctement et de manière aussi transparente que possible ainsi que de respecter les droits de chaque individu.

Consultez le kit de démarrage FISP pour en savoir plus sur les différents types de données.

Catégorie	Generieke informatie benaming van het type persoonsinformatie
	➢ Aucun type de données standard relatives aux données à caractère personnel n'a été identifié dans la catégorie d'information 0.
	➢ Coordonnées professionnelles
	➢ Loisirs et intérêts ➢ Coordonnées personnelles ➢ Données d'identification ➢ Caractéristiques personnelles ➢ Habitudes de consommation ➢ Caractéristiques de l'habitation ➢ Études, expérience et formation ➢ Profession et poste ➢ Données financières et fiscales ➢ Mode de vie ➢ Composition du ménage ➢ Données de localisation ➢ Renseignements / Détails du contrat entre le travailleur et l'employeur ➢ Évaluation et prestations ➢ Données de sécurité sociale ➢ Numéro de Registre national, numéro d'identification de la sécurité sociale

	➢ Données et traitements physiques, médicaux et psychiques ➢ Données juridiques et judiciaires ➢ Données raciales ou ethniques ➢ Données sur l'orientation sexuelle ➢ Croyances et convictions politiques, philosophiques ou religieuses ➢ Enregistrements audio et vidéo ➢ Données génétiques et biométriques ➢ Statuts et permis
	Informations spécifiques relevant de l'art. 23 du RGPD comme les informations personnelles ayant une influence sur la sécurité nationale, la sécurité publique, l'exécution des demandes de droits civils….

Gestion du document

Historique

Date	Auteur	Version	Description des modifications
27/05/2019	BOSA	V0.1	Première ébauche
24/06/2019	BOSA	V0.2	Mise à jour sur la base des commentaires
28/08/2019	BOSA	V0.3	Mise à jour sur la base des commentaires
03/09/2019	BOSA	V0.4	Mise à jour sur la base des commentaires du CCB
18/09/2019	BOSA	V1.0	Mise à jour sur la base des commentaires
7/10/2019	BOSA	V2.0	Mise à jour sur la base des commentaires pendant la validation
21/11/2019	FISP Workgroup	V2.1	Distribution publique

Approbations

Date	Approbateur(s)	Version
21/11/2019	FISP Workgroup	v2.1

Sources

Ce document a été rédigé à l'aide des sources suivantes :

- ISO/CEI 29100
- ISO/CEI 27001, 27002, 27701
- Normes ISO gratuites (parmi lesquelles ISO 29100 et ISO 27000)
- Règlement (UE) 2016/679 du Parlement européen et du Conseil / 27 avril 2016 (GDPR/RGPD)
- Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel
- Dossier thématique de l'Autorité de protection des données (https://www.autoriteprotectiondonnees.be/reglement-sur-la-protection-des-donnees)
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_fr

Lien avec une autre politique

Dépendance de documents internes

Réf.	*Titre*
FISPDOC04	*Guide pour le logging et le monitoring*
FISPDOC05	*Guide pour la sécurisation et la gestion des identités et des accès de base (IAM), et des accès privilégiés (PAM)*
FISPDOC03	*Guide pour la cryptographie*

Positionnement de la politique par rapport à la norme ISO 27001

Section	*Objectifs et mesures de référence*	*En relation (X = Oui)*
4	*Contexte de l'organisation*	
5	*Leadership*	
6	*Planification*	
7	*Support*	
8	*Fonctionnement*	
9	*Évaluation des performances*	
10	*Amélioration*	

Positionnement de la politique par rapport à la norme ISO 27002

Section	*Objectifs et mesures de référence*	*En relation (X = Oui)*	*Objectifs/Mesures (Détail)*
A5	*Politique de sécurité de l'information*		
A6	*Organisation de la sécurité de l'information*		
A7	*Sécurité des ressources humaines*		
A8	*Gestion des actifs*		
A9	*Contrôle d'accès*		
A10	*Cryptographie*		
A11	*Sécurité physique et environnementale*		
A12	*Sécurité liée à l'exploitation*		
A13	*Sécurité des communications*		
A14	*Acquisition, développement et maintenance des systèmes d'information*		
A15	*Relations avec les fournisseurs*		
A16	*Gestion des incidents liés à la sécurité de l'information*		
A17	*Sécurité de l'information dans la gestion de la continuité de l'activité*		
A18	*Conformité*		