Politique relative à la sécurité et à la confidentialité de l'information

Traitement de données à caractère personnel

(BLD PRIV)

TABLE DES MATIÈRES

1. Introduction

Le présent document fait partie intégrante de la méthodologie relative à la sécurité et à la confidentialité de l'information dans la sécurité sociale. Il est destiné aux responsables, aux sous-traitants de l'information, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de la sécurité sociale (IPSS).

Cette politique repose sur le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE (Règlement général sur la protection des données). [1]

Ces politiques s'appliquent au traitement entièrement ou partiellement automatisé de l'organisation, ainsi qu'au traitement de données à caractère personnel[2] reprises dans les fichiers ou destinées à y figurer.

Ce document porte sur les politiques relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la circulation de ces données.

2. Traitement de données à caractère personnel

Toute organisation souscrit aux politiques suivantes relatives à la sécurité et à la confidentialité de l'information pour l'ensemble des informations et systèmes d'information placés sous sa responsabilité.

- L'organisation inventorie régulièrement tous les risques liés à la conformité avec le Règlement européen[3]. Les actions planifiées en conséquence d'un haut risque "résiduel" de non-conformité doivent figurer dans le plan de sécurité et de confidentialité de l'information de l'organisation.
- En fonction du rôle pour un (groupe de) traitement spécifique (sous-traitant ou responsable du traitement), l'organisation exécutera au moins les activités suivantes :
    - Reprise du traitement dans le registre central du responsable du traitement ou du sous-traitant.
    - Justification formelle de la non-réalisation de mesures de contrôle axées sur le respect du Règlement européen[4].

[1] Mieux connu sous l'appellation "European General Data Protection Regulation" (abrégée "EU GDPR") http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[2] On entend par "traitement de l'information" : la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction de données. Cette définition est issue du Règlement européen du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

[3] https://www.privacycommission.be/sites/privacycommission/files/documents/CO-AR-2016-004_FR.pdf

[4] Principe "Appliquer ou expliquer" ("comply or explain principle")

Annexe A : Gestion du document

Gestion des versions

Date	Auteur	Version	Description du changement	Date d'approbation	Date d'entrée en vigueur
2017		V2017	Première version	07/03/2017	07/03/2017

Erreurs et omissions

Si des erreurs ou des problèmes sont constatés à la lecture du présent document, vous êtes prié en tant que lecteur de transmettre au conseiller en sécurité de la sécurité de l'information (CISO) / délégué à la protection des données (DPO) de l'institution une brève description de l'erreur ou du problème ainsi que de sa place dans le document conjointement à vos données de contact.

Définitions

Dans un souci de cohérence de la terminologie et des concepts utilisés dans tous les documents, toutes les définitions relatives à la sécurité et à la confidentialité de l'information sont centralisées dans un document intitulé "Définitions relatives à la sécurité et à la confidentialité de l'information".

Annexe B : Références

Ci-dessous figurent des documents qui ont servi d'inspiration au présent document.

- RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
- ISO, "ISO/IEC 27001:2013 Information Security Management System Requirements", septembre 2013, 23 pages
- ISO, "ISO/IEC 27002:2013 Code of Practice for Information Security Management", septembre 2013, 80 pages
- ISO, "ISO/IEC 29100:2012 Security Techniques - Privacy framework", décembre 2012, 21 pages

Ci-dessous figurent des références aux sites web qui ont servi d'inspiration au présent document :

- http://eur-lex.europa.eu/eli/reg/2016/679/oj
- https://www.privacycommission.be/fr/reglement-general-sur-la-protection-des-donnees-0
- https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
- https://www.enisa.europa.eu/topics/data-protection
- https://www.iso.org/isoiec-27001-information-security.html
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- https://www.iso.org/standard/45123.html
- http://www.isaca.org/privacy

Annexe C : Directives et templates connexes

Pour la réalisation de ces politiques, l'organisation peut utiliser les procédures suivantes :

1. La procédure de demande d'information et la procédure d'analyse d'impact relative à la protection des données ("Privacy Impact Assessment") avec la liste des risques y afférente issue de la politique "Évaluation des risques".
2. Le registre du sous-traitant et du responsable du traitement de la politique "Classification des données".
3. La procédure relative à la violation et à la contrainte issue de la politique "Gestion des incidents".
4. La description de fonction pour le délégué à la protection des données issue de la politique "Aspects liés au personnel".
5. Les dispositions contractuelles en matière de protection des données issues de la politique "Sous-traitance sécurisée à des tiers" et de la politique "Aspects liés au personnel".
6. La communication avec la personne concernée ("déclaration de confidentialité") issue de la politique "Acquisition, conception, développement et maintenance de systèmes d'information".

Annexe D : Lien avec la norme ISO 27002:2013

Nous renvoyons ici à la (aux) clause(s) principale(s) de la norme ISO 27002:2013 relative à l'objet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	
Personnel sûr	
Gestion des moyens d'exploitation	
Sécurisation des accès	
Cryptographie	
Sécurité physique et de l'environnement	
Sécurisation des processus	
Sécurité de la communication	
Achats, maintenance et développement de systèmes d'information	
Relations fournisseurs	
Gestion des incidents de sécurité	
Aspects de sécurité de l'information de la gestion de la continuité	
Respect	**Oui**

***** FIN DU DOCUMENT *****