Ligne directrice sécurité de l'information et vie privée

Principes clés

(BLD KERN)

TABLE DES MATIÈRES

1. Introduction

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

Ces lignes directrices de sécurité de l'information et à la vie privée créent les conditions nécessaires pour une exécution fiable du traitement de l'information dans le chef des institutions publiques de sécurité sociale (IPSS) intégrées au réseau de la Banque Carrefour de la sécurité sociale.

Il est essentiel pour les partenaires au sein de la sécurité sociale de connaître ces lignes directrices de sécurité de l'information et à la vie privée, de les valider, de les communiquer et de les intégrer.

Le présent document décrit les principes clés de la sécurité de l'information et de la vie privée.

2. Principes clés de la sécurité de l'information et de la vie privée

L'organisation souscrit les principes clés suivants relatifs à la sécurité de l'information et à la vie privée pour l'ensemble des informations et systèmes d'information relevant de la responsabilité de l'organisation:

1. Mettre au point une politique claire et précise relative à la sécurité de l'information et à la vie privée, la valider, la communiquer et l'actualiser afin de garantir la disponibilité, l'intégrité et la confidentialité en adéquation avec les objectifs de l'organisation.
2. Intervenir conformément aux lignes directrices de sécurité de l'information et à la vie privée et aux lois et réglementations belges et européennes applicables afin de respecter les obligations et d'éviter des amendes.
3. Mettre au point une approche formelle des risques relatifs à la sécurité de l'information et à la vie privée, valider, communiquer et maintenir cette approche, afin de maîtriser, dans meilleurs les délais, de manière cohérente et effective, les risques pertinents, en adéquation avec les attentes de l'organisation.
4. Définir les responsabilités et rôles précis de l'ensemble du personnel interne et externe et des organisations concernés en ce qui concerne la sécurité de l'information et la vie privée, les valider, les communiquer et assurer leur suivi.
5. Traduire les lignes directrices de sécurité de l'information et à la vie privée dans des procédures et directives pratiques documentées en fonction de la situation spécifique de l'organisation et sur la base d'une évaluation des risques.
6. Appliquer le "Security and Privacy by design"[1] au cours du cycle de vie complet des informations dans l'organisation afin de développer des systèmes efficaces, fiables et de qualité, à savoir depuis la création jusqu'à la suppression ou l'archivage des informations.
7. Améliorer en permanence le niveau de la sécurité de l'information et de la vie privée au moyen d'un plan pluriannuel actualisé et de campagnes de sensibilisation régulières à l'attention du personnel interne et externe et des organisations concernés[2] afin de réduire les coûts des infractions et de sauvegarder la réputation et la confiance au niveau du traitement des données.

[1] "Security and Privacy by design" signifie que dès le début du développement d'un nouveau projet ou processus/une prestation de service, une réflexion est menée sur les mesures nécessaires relatives à la sécurité de l'information et à la vie privée. A cet égard, il est essentiel que toutes les mesures prises soient simples et conviviales et soient dans le même temps constituées de plusieurs couches de protection. "Security and Privacy by design" est différent du "Security et Privacy by default" parce que dans ce dernier cas, on choisit toujours l'option la plus sûre ou dont la priorité est la plus élevée, cette option n'étant pas toujours l'option la plus conviviale.

[2] Le Comité sectoriel de la sécurité sociale peut en demander une copie.

8. En cas de sous-traitance du traitement des données à des tiers, élaborer les mesures de contrôle nécessaires, les valider et assurer leur suivi à des intervalles réguliers, puisque l'organisation demeure responsable de la sécurité de l'information et de la vie privée.
9. Élaborer à des intervalles réguliers un compte rendu sur l'état d'avancement de la sécurité de l'information et de la vie privée afin de valider l'applicabilité, l'exhaustivité, l'adéquation et l'effectivité de la sécurité de l'information et de la vie privée. Les dérogations, problèmes ou incidents constatés feront l'objet d'un suivi en temps utile par des actions/sanctions appropriées en adéquation avec les procédures internes de l'organisation. Des incidents ou infractions majeurs en rapport avec des données à caractère personnel sont toujours remontés vers les instances compétentes[3].
10. Harmoniser, au préalable et par écrit, toutes les dérogations présentant un risque significatif par rapport aux lignes directrices de sécurité de l'information et à la vie privée et les faire approuver par le Comité sectoriel de la sécurité sociale[4].

Annexe A: Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description du changement	Date approbation	Date entrée en vigueur
2017		V2017	Première version y compris UE GDPR	07/03/2017	07/03/2017

Erreurs et omissions

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

Définitions

Pour garantir la cohérence en ce qui concerne la terminologie et les notions utilisées à travers les divers documents détaillant la politique à suivre, toutes les définitions relatives à la sécurité de l'information et à la protection de la vie privée sont regroupées dans un document spécifique : "Définitions normes minimales sécurité de l'information et protection de la vie privée".

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

[3] Les incidents peuvent toujours être remontés vers le service de sécurité de l'information, vers le CERT.BE. La remontée vers la commission de la protection de la vie privée dans les 72 heures est obligatoire lorsque des données à caractère personnel sont impliquées. http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR

[4] appliquer ou expliquer principe ("comply or explain principle")