Ligne directrice sécurité de l'information & vie privée :

sécurité de la sous-traitance à des tiers

(BLD OUTS)

TABLE DES MATIÈRES

1. Introduction

Le présent document fait intégralement partie de la méthodologie relative à la 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).

Le présent document décrit les directives relatives à la sécurité de l'information pour la gestion des relations avec des tiers (fournisseurs).

2. Sécurité de la sous-traitance à des tiers

Toute organisation souscrit les directives suivantes relatives 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:

En cas de sous-traitance, l'organisation doit s'assurer de ce qui suit:

1. les obligations[1] en matière de traitement de données à caractère personnel doivent être établies contractuellement.
2. les conditions relatives à la sécurité de l'information et à la vie privée doivent faire l'objet d'un accord avec les tiers et sont documentées afin de réduire les risques relatifs à l'accès des tiers aux moyens d'information
3. toutes les conditions pertinentes relatives à la sécurité de l'information et à la vie privée doivent être définies et doivent faire l'objet d'un accord avec chacun de ces tiers qui lisent, traitent, enregistrent, communiquent les informations de l'organisation ou fournissent des éléments d'infrastructure TIC
4. les contrats conclus avec les tiers doivent comprendre toutes les conditions permettant de traiter les risques liés à la sécurité de l'information et à la vie privée qui sont afférents aux services TIC
5. l'organisation doit régulièrement effectuer un monitoring de la prestation de service de tiers et doit évaluer et auditer cette prestation de service
6. les adaptations de la prestation de service par des tiers, dont notamment l'actualisation et l'amélioration des politiques, procédures et mesures relatives à la sécurité de l'information et à la vie privée existantes, doivent être gérées. Lors de la gestion, il y a lieu de tenir compte du caractère critique des systèmes et processus en question et de la réévaluation des risques

1 L'organisation demeure responsable de la sécurité de l'information et de la vie privée du traitement, y compris du traitement chez le(s) sous-traitant(s).

Annexe A: Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description du changement	Date approbation	Date entrée en vigueur
2003		V2003	Première version	10/09/2003	01/10/2003
2004		V2004	Deuxième version	11/02/2004	01/12/2004
2017		V2017	Intégration 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 de politique, 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 sécurité de l'information et protection de la vie privée".

Annexe B: Références

Ci-dessous figurent les documents qui ont servi de source d'inspiration pour le présent document:

- ISO, “ISO/IEC 27001:2013 Information Security Management System Requirements”, septembre 2013, 23 p.
- ISO, “ISO/IEC 27002:2013 Code of Practice for Information Security Management”, septembre 2013, 80 p.
- SANS, “A security guide for acquiring outsourced service”, Avril 2017, 20 p.
- ISACA, “COBIT 5 for Information Security”, Mai 2012, 220 p.

Ci-dessous figurent les références aux sites web qui ont service de source d'inspiration pour le présent document:

- 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
- http://www.isaca.org/cobit
- https://www.sans.org/reading-room/whitepapers/services/a-security-guide-for-acquiring-outsourced-service-1241
- https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Outsourced-IT-Environments-Audit-Assurance-Program.aspx
- http://www.isaca.org/Knowledge-Center/Research/Documents/Governance-of-Outsourcing_res_Eng_0105.pdf

Annexe C: Directives relatives à la sécurité de la sous-traitance à des tiers

Sécurité de l'information et vie privée dans la gestion des relations avec des tiers

1. Il y a lieu d'établir des directives spécifiques pour la gestion des accès (logiques et physiques) de tiers.
2. Il y a lieu d'identifier et de documenter les différents types de tiers qui ont accès aux informations ou aux systèmes d'information de l'organisation (tels les fournisseurs TIC, les entreprises d'utilité publique).
3. Pour l'exécution d'une mission, il y a lieu d'établir un processus et un cycle de vie standards pour la gestion des relations avec les tiers afin de garantir la sécurité de l'information et la vie privée.
4. Si un tiers fait appel à des sous-traitants, le tiers (l'entrepreneur principal) demeure responsable du respect des conditions relatives à la sécurité de l'information et à la vie privée par le sous-traitant.
5. Les différents types d'accès aux informations (consultation, écriture, modification, suppression) consentis par l'organisation aux différents tiers doivent être définis et les accès doivent être surveillés et contrôlés selon des processus et procédures fixes.
6. Les directives relatives à la sécurité de l'information et à la vie privée doivent, pour chaque type d'information et d'accès, constituer la base pour des contrats individuels avec des tiers. Ces contrats doivent être basés sur les exigences et le profil de risque de l'organisation.
7. Les collaborateurs de l'organisation qui ont des contacts directs avec des tiers doivent être conscientisés aux règles et aux attitudes adéquates, basées sur le type de tiers (tel que l'entreprise d'utilité publique ou le fournisseur TIC) et leur niveau d'accès aux systèmes (d'information) de l'organisation

Traiter la sécurité de l'information et la vie privée dans les contrats avec les tiers

Il y a lieu d'établir des contrats individuels avec tout tiers de la première ligne afin d'assurer qu'il n'y ait pas de malentendu en ce qui concerne les responsabilités des deux parties relatives à la sécurité de l'information et à la vie privée. Selon la nature du « tiers », la relation avec l'organisation peut être définie comme suit:

1. Une législation ou une réglementation qui impose ou autorise une collaboration avec d'autres organismes publics, nationaux ou internationaux.
2. Un contrat qui régit les conditions de la collaboration entre les organismes publics.
3. Les clauses d'un cahier des charges
4. Un contrat explicite entre les deux parties

Ces contrats doivent prendre en considération les directives suivantes:

1. Transparence et communication continues du tiers à l'organisation concernant la sous-traitance à d'autres parties d'activités liées à la mission avec l'organisation, en ce compris concernant les mesures prises relatives à la sécurité de l'information et à la vie privée.
2. La manière selon laquelle l'organisation et le tiers doivent gérer les incidents relatifs à l'accès d'un tiers.
3. Des règles de défense et si nécessaire de réparation afin d'assurer la disponibilité des informations ou des systèmes d'information d'une des deux parties
4. La manière de gérer les informations, les systèmes d'information ou autres moyens d'information qui sont déplacés et la manière d'assurer la sécurité et la vie privée au cours de la période de transfert.
5. Il faut qu'il y ait une description précise des informations qui sont fournies ou abordées ainsi que de la manière dont les informations sont fournies ou abordées.

6. Les données doivent être classifiées selon le schéma de classification de l'organisation. Si nécessaire, les schémas de classification des données ainsi que les mesures respectives relatives à la sécurité de l'information et à la vie privée des deux parties doivent être harmonisées de commun accord.
7. Les conditions légales et réglementaires, en ce compris la cybersécurité, la vie privée, les droits de propriété intellectuelle et les droits d'auteur, doivent être décrites. Il sera également décrit comment il y a lieu satisfaire à ces conditions.
8. L'obligation de toute partie contractante de mettre en œuvre les mesures de contrôle convenues telles le contrôle des accès, le contrôle des niveaux, le monitoring, le rapportage et l'audit.
9. Les obligations dans le chef de tiers pour le respect des conditions relatives à la sécurité de l'information et à la vie privée telles des règles pour un usage licite et si nécessaire un usage non autorisé de données.
10. Il faut qu'il y ait des procédures ou conditions d'autorisation ou de suppression de l'autorisation pour l'accès aux informations de l'organisation ou pour la réception de ces informations, par exemple en établissant une liste explicite des collaborateurs des tiers qui ont un accès autorisé aux informations de l'organisation ou qui reçoivent ces informations.
11. Les conditions et procédures relatives à la sécurité de l'information pour la gestion d'incidents relatifs à la sécurité de l'information et à la vie privée, en particulier la notification et la collaboration lors de la remédiation d'un incident.
12. Les conditions de formation et de conscientisation relatives aux procédures et conditions spécifiques en rapport avec la sécurité de l'information et la vie privée, telles le traitement d'incidents et des procédure d'autorisation.
13. Des personnes de contact pertinentes, en compris la personne de contact pour la sécurité de l'information et la vie privée.
14. Si nécessaire, des conditions de screening pour les collaborateurs des tiers
15. Le droit de l'organisation d'auditer (ou de faire auditer) des processus et des procédures de tiers en rapport avec le contrat.
16. L'obligation dans le chef de tiers de fournir, à titre périodique, un rapport indépendant sur l'effectivité des contrôles et un accord sur la résolution, en temps utile, de problèmes pertinents éventuels mentionnés dans un rapport d'audit.
17. Processus pour la résolution de pannes, de conflits et pour un régime de sortie (exit strategie).

Dans le cadre des marchés publics, les principes généraux du contrat doivent être définis dans un cahier des charges.

Chaîne TIC

Les directives suivantes doivent être prises en considération dans les contrats relatifs à la sécurité de l'information et à la vie privée dans la chaîne ICT (supply chain):

1. Outre les conditions générales relatives à la sécurité de l'information et à la vie privée, il y a aussi lieu de définir des conditions spécifiques relatives à la sécurité de l'information et à la vie privée qui sont applicables à l'acquisition de produits et services liés à l'ICT.
2. Les services et produits de tiers liés à l'ICT qui requièrent que ces tiers doivent éventuellement transmettre à leurs sous-traitants les conditions relatives à la sécurité de l'information et à la vie privée.
3. Il y a lieu d'implémenter un processus de monitoring et des méthodes de validation acceptables permettant de vérifier que les produits et services TIC satisfont aux conditions définies en matière de sécurité de l'information et de vie privée.
4. Il y a lieu de mettre en œuvre un processus d'identification des composants du produit ou de la prestation de service qui sont cruciaux pour la maintenance de la fonctionnalité. Il y a lieu d'accorder une attention particulière aux composants du produit ou des services qui est (sont) sous-traité(s) par un fournisseur.

5. Les tiers doivent garantir à l'organisation que les éléments et services critiques peuvent être tracés tout au long de la chaîne de distribution. Ils doivent par ailleurs aussi garantir que les produits TIC fournis fonctionnent conformément aux attentes, sans fonctions inattendues ou non souhaitées.
6. Il y a lieu de définir des règles pour le partage d'informations relatives à la chaîne ICT et concernant des problèmes éventuels entre l'organisation et les tiers.
7. Il y a lieu de fixer des processus spécifiques de gestion du cycle de vie, des disponibilités et des risques y afférents sur le plan de la sécurité de l'information et de la vie privée d'éléments informatiques. A cet effet, il y a lieu de tenir compte des éléments qui ne sont plus disponibles en raison d'un arrêt de la production, par exemple suite à la faillite d'un tiers ou une technologie désuète qui n'est plus livrable (composants).

Monitoring et évaluation de la prestation de services de tiers

Il y a lieu de rédiger et de mettre en œuvre des processus pour la gestion de la prestation de service entre l'organisation et les tiers. À cet effet, il y a lieu de tenir compte des aspects suivants:

1. Il y a lieu de vérifier la conformité des niveaux de prestation des services par rapport aux contrats
2. Les rapports relatifs à la prestation de service établis par un tiers doivent être vérifiés par l'organisation et par ailleurs, comme convenu, il y a régulièrement lieu d'organiser des réunions relatives à l'état d'avancement
3. Il y a lieu de communiquer les informations relatives aux incidents relatifs à la sécurité de l'information et à la vie privée. Ces informations doivent être évaluées par le tiers et l'organisation comme exigé dans les contrats et les directives et procédures d'appui.
4. Les traces d'audit et les enregistrements d'événements, de problèmes opérationnels, d'échecs, de détection de dysfonctionnements et les interruptions liées aux services fournis doivent être évalués.
5. Les accords conclus par un tiers avec des sous-traitants en ce qui concerne la sécurité de l'information et la vie privée doivent être évalués
6. Les tiers doivent garantir qu'ils sont en mesure d'offrir le niveau de prestation convenu en cas de sinistre ou d'incident grave
7. L'organisation doit veiller à ce que ses collaborateurs disposent des compétences techniques et des moyens requis pour le monitoring des conditions du contrat. Si nécessaire, il y a lieu de prévoir les formations nécessaires

Gestion de la modification de la prestation de services de tiers

Des modifications dans la prestation de service par des tiers, en ce compris la maintenance et l'amélioration de la politique, des procédures et des contrôles relatifs à la sécurité de l'information, doivent être gérées tout en tenant compte du caractère critique des informations, des systèmes, des processus et des produits concernés de l'entreprise et d'une réévaluation des risques. Il y a, à cet effet, lieu de tenir compte des aspects suivants

1. Modifications aux contrats avec les tiers
2. Modifications à la législation et à la réglementation pertinentes
3. Modifications par l'organisation en vue de la mise en œuvre
    a. Améliorations aux services actuellement fournis
    b. Développement de nouveaux systèmes et applications
    c. Modifications ou mises à jour de documents et procédures politiques
    d. Nouvelles mesures de contrôle ou mesures modifiées permettant de résoudre ou d'améliorer les incidents relatifs à la sécurité de l'information et à la vie privée
4. Modifications à la prestation de service par des tiers en vue de la mise en œuvre
    a. Modifications et extensions de réseaux

b. Utilisation des nouvelles technologies
c. Nouveaux produits ou nouvelles versions de produits existants
d. Nouveaux outils et environnements de développement
e. Changement d'endroits physiques
f. Changement de fournisseur
g. Sous-traitance à un autre sous-traitant

Annexe D: Lien avec la norme ISO 27002:2013

Nous vous renvoyons ici aux principales clauses de la norme ISO 27002:2013 en rapport avec le sujet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	
Sécurité des ressources humaines	
Gestion des actifs	
Protection de l'accès	
Cryptographie	
Sécurité physique et environnementale	
Protection des processus	
Sécurité de la communication	
Maintenance et développement de systèmes d'information	
Relations avec les fournisseurs	**Oui**
Gestion des incidents de sécurité	
Aspects de la sécurité de l'information dans la gestion de la continuité	
Respect	

***** EINDE VAN DIT DOCUMENT *****