Lignes directrices pour l'application du GDPR dans les secrétariats sociaux

1. Définitions

1.1. Les définitions utilisées dans le GDPR sont reprises à l'annexe 1.

1.2. SSA : Secrétariat Social Agréé

1.3. GDPR : General Data Protection Regulation. Abrégé en français "RGPD" (le Règlement Général sur la Protection des Données).

1.4. APD : Autorité de protection des données, soit l'autorité de contrôle de la protection des données à caractère personnel en Belgique.

1.5. Sous-traitant ultérieur : le sous-traitant désigné par le secrétariat social afin de prendre en charge une partie du processus de traitement du SSA pour le compte du responsable du traitement, incluant notamment le traitement de données à caractère personnel.

1.6. USS : Union des Secrétariats Sociaux

2. Introduction

2.1. 90 % des employeurs du secteur privé en Belgique font appel à un SSA pour leur administration sociale. Le SSA traite des données à caractère personnel dans le cadre de ses missions et estime qu'il est crucial de traiter lesdites données à caractère personnel avec soin et en toute confidentialité. C'est la raison pour laquelle l'USS entend utiliser des lignes directrices qui formalisent l'application concrète du GDPR dans le secteur des secrétariats sociaux en tant que sous-traitants. Ces lignes directrices définissent un cadre au sein duquel il est possible de garantir que les données à caractère personnel des travailleurs des clients des secrétariats sociaux soient traitées de manière uniforme et soumises aux mêmes mesures de protection strictes.

2.2. Les lignes directrices sectorielles (ci-après "les lignes directrices") relatives au traitement des données à caractère personnel dans le cadre du GDPR listent clairement les lignes de force de la stratégie en matière de protection des données mise en œuvre par l'USS.

2.3. Ce document :

- définit les lignes directrices du traitement des données à caractère personnel traitées dans le cadre de la prestation de service ;
- renforce la transparence à l'égard des méthodes de traitement des données à caractère personnel appliquées par le secteur ;
- fournit à l'Autorité de protection des données ("APD") des pistes lui permettant d'évaluer si le traitement des données à caractère personnel s'effectue bien conformément à la législation et aux réglementations en vigueur ;

- vise à répondre aux attentes légitimes des clients concernant le traitement correct des données à caractère personnel de leurs collaborateurs.

3. Champ d'application

Les lignes directrices s'appliquent au SSA agréé et établi en Belgique pour l'exécution de ses missions principales en Belgique.
Les lignes directrices s'appliquent exclusivement au traitement des données à caractère personnel dans le cadre des tâches principales du SSA, à savoir :

- calculs de salaires et documents y afférents
- déclarations aux autorités et autres tierces parties
- perception et versement des cotisations ONSS et du précompte professionnel
- avis juridique en matière de droit social et de droit du travail concernant l'administration sociale de l'employeur

Les objectifs de traitement du SSA en tant que sous-traitant sont l'exécution des tâches principales ci-dessus.

Dans le cadre de la réalisation de ces tâches principales, le SSA ne traite pas de catégories particulières de données à caractère personnel telles que décrites à l'article 9 du GDPR.
Les données fournies par le client/l'employeur et qui ne sont pas nécessaires à l'exécution des missions principales du SSA ne relèvent pas du champ d'application de ces lignes directrices sectorielles.

4. Relation SSA – client/employeur

4.1 Le SSA est toujours sous-traitant dans le cadre de l'exécution de ses tâches principales. Le responsable du traitement est toujours le client/l'employeur.

4.2 Le fondement juridique pour le SSA est le contrat avec le client/l'employeur et les obligations légales d'application au SSA en tant que mandataire.

5. Analyse d'impact relative à la protection des données

En tant que sous-traitant, le SSA ne doit pas réaliser d'Analyse d'Impact relative à la Protection des Données ou de Data Protection Impact Assessment (ci-après « AIPD »). Une AIPD est en fait une obligation qui ne repose que sur le responsable du traitement.

L'USS souligne par ailleurs le fait que l'APD indique que l'administration des salaires et l'administration du personnel sont des activités de traitements pour lesquelles il n'y a aucune obligation AIPD (Annexe 3 de la Recommandation n° 01/2018 du 28 février 2018).

Le SSA s'engage cependant à :

- aider ses clients, sur demande, à respecter leurs obligations AIPD sur base de l'article 35 du GDPR
- faire une analyse des risques des activités de traitement réalisées pour les clients afin que les mesures techniques et organisationnelles adéquates et nécessaires puissent être prises (voir aussi article 12 de ces lignes directrices).

6. Registre des activités de traitement

Conformément à l'article 30.2 du GDPR, le SSA tient un registre interne des activités de traitement.

7. Sous-traitants ultérieurs

Le SSA qui fait appel à des sous-traitants ultérieurs pour la réalisation de ses tâches principales :

- conclut un contrat de traitement avec le sous-traitant ultérieur qui reprend au moins les mêmes obligations en matière de protection des données que le contrat de traitement respectif que le SSA conclut avec son (ses) client(s) ;
- garantit que le client donne son autorisation écrite préalable pour le recours à des sous-traitants ultérieurs. Cette autorisation peut prendre la forme d'une autorisation écrite générale ou spécifique ;
- a une méthode de travail pour informer chaque client au préalable de l'ajout ou du remplacement des sous-traitants ultérieurs ;
- a une méthode de travail pour traiter une plainte d'un client ;
- tient une liste à jour de ses sous-traitants ultérieurs. Cette liste est au moins disponible sur demande.

Le SSA ne considère pas les tiers suivants comme étant des sous-traitants ultérieurs, malgré le fait que ces parties reçoivent des données à caractère personnel de la part du SSA :

- les organes de la Sécurité Sociale ;
- le SPF Finances ;
- les autorités régionales ;
- les organisations à qui le SSA transmet les données à caractère personnel des travailleurs du client sur base des instructions du client, mais avec lequel le SSA n'a pas de lien contractuel, comme des fournisseurs de chèques-repas par exemples, des sociétés de leasing, des assurances groupe et des fonds de sécurité d'existence.

8. Transfert de données personnelles à des tiers

Le SSA transmet des données uniquement dans le cadre de ses missions principales ou sur instruction formelle du client. Ces instructions peuvent figurer dans un contrat ou être consignées sous une autre forme (p. ex. via un outil en ligne).

9. Délais de conservation

9.1. Délais de conservation pour le client/l'employeur, en tant que responsable du traitement, pour la conservation des documents pour lesquels le client/l'employeur est soumis à une obligation légale de conservation :

Le SSA conserve les documents mentionnés à l'annexe 2.1 qu'il traite effectivement dans le cadre de ses missions principales au moins pendant les délais de conservation tels que mentionnés à l'annexe 2.1 à compter de l'année suivant la période concernée par le document, à moins qu'il n'en ait été convenu autrement avec le client/l'employeur.

9.2. Délais de conservation pour le SSA, en tant que sous-traitant, pour la conservation des documents pour lesquels le SSA est soumis à une obligation légale de conservation :

Le SSA conserve les documents mentionnés à l'annexe 2.2 qu'il traite effectivement dans le cadre de ses missions principales pendant les délais de conservation tels que mentionnés à l'annexe 2.2 à compter de l'année suivant la période concernée par le document.

9.3. Politique de rétention des données

Le SSA a une politique de rétention des données qui tient compte du principe de l'article 5.1.e du GDPR (limite de stockage). Cette politique indique au minimum que le SSA réalisera la suppression/l'anonymisation au plus tard 7 ans après la fin du contrat de travail entre le client et son travailleur et au plus tard 7 ans après la fin du contrat entre le SSA et le client, à moins qu'il n'en ait été convenu autrement avec le client.

Ce délai de 7 ans commence à courir le premier jour de l'année qui suit le terme du contrat de travail du travailleur ou le contrat avec le client. À l'échéance du délai de conservation, ces données sont supprimées ou anonymisées dans un délai raisonnable.

Cette politique de rétention des données reprend au minimum les éléments suivants :

- Si le client a la possibilité ou pas de gérer lui-même la suppression ou l'anonymisation des données à caractère personnel ;
- Comment le SSA gère la conservation/suppression/anonymisation des données à caractère personnel
- Les délais de conservation par catégorie des données à caractère personnel des travailleurs

10. Responsable de la protection des données

Le SSA s'engage à désigner un responsable pour la protection des données et à respecter ces lignes directrices. Ce responsable est également la personne de contact dans le cadre de la protection des données. Le SSA publie les coordonnées de cette personne de contact.

L'USS s'engage à créer un groupe de pilotage *data protection* (« protection des données ») qui se compose des responsables de la protection des données des secrétariats sociaux membres de l'USS. La mission de ce groupe de pilotage consistera entre autres :

- à assurer le suivi des nouvelles évolutions en matière de protection des données ;
- à favoriser un échange de *best practices* au sein du secteur ;
- à réaliser une révision annuelle de ces lignes directrices et du questionnaire pour l'auto-évaluation.

11. Fuites de données

Dès que le SSA prend connaissance d'une fuite de données, il en informe le client/l'employeur concerné (responsable du traitement) dans les meilleurs délais. Le SSA a mis en place des procédures standard pour la notification au client et la gestion des fuites de données.

Le SSA fournira, sur base des informations disponibles, une assistance raisonnable au responsable du traitement lors du traitement d'une fuite de données.
Il incombe au responsable du traitement (client/employeur) de vérifier si les personnes concernées/l'APD doivent éventuellement être informées d'une fuite de données. Le SSA n'informera donc pas les personnes concernées/l'APD d'une fuite de données, à moins qu'il n'en ait été convenu autrement explicitement avec le client.

12. Sécurité informatique – Mesures techniques et organisationnelles

Le SSA met en place les mesures de sécurité nécessaires pour protéger les données à caractère personnel, comme décrit à l'annexe 3. Cette annexe donne un aperçu des principales mesures minimales garanties par le SSA.

13. Droits de la personne concernée

Si le SSA reçoit des demandes des personnes concernées d'exercer leurs droits, le SSA les transmet au client/à l'employeur dans un délai de 14 jours calendrier.

Le SSA apporte l'assistance raisonnable à son client/employeur pour permettre à l'employeur de répondre de façon adéquate aux questions des personnes concernées.

Le SSA a mis en place des procédures standard pour l'application de l'exercice des droits des personnes concernées.

14. Respect des lignes directrices

Le SSA réalise une auto-évaluation annuelle de l'application de ces lignes directrices sur base d'un questionnaire, repris à l'annexe 4, et confirme par écrit à l'USS, sur base de cette auto-évaluation, qu'il respecte les lignes directrices.

En cas de problèmes de non-respect de ces lignes directrices, l'USS le mentionnera au SSA concerné.

Annexe 1 : définitions

Dans ces lignes directrices, on entend par :

(Définitions copiées du GDPR)

Données à caractère personnel : 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;

Catégories spécifiques de données à caractère personnel :
Les données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

- **Données génétiques :** les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question ;
- **Données biométriques :** les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ;
- **Données concernant la santé :** les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ;

Traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telle que 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;

Personne concernée : une personne physique identifiée ou identifiable

Responsable du traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ;

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

Tiers : une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel ;

Délégué à la protection des données (DPO) :
Le délégué à la protection des données contrôle les traitements de données au sein de son organisation.

Fuite de données – violation de données à caractère personnel : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ;

DPIA (Data Protection Impact Assessment) - Analyse d'impact de la protection des données : est un instrument permettant de recenser à l'avance les risques relatifs à la vie privée lors du traitement de données et de prendre ensuite des mesures pour réduire les risques. Abrégé en français "AIPD" (Analyse d'impact de la protection des données).

Annexe 2 : délais légaux de conservation pour les catégories de données à caractère personnel traitées dans le cadre des tâches principales :

2.1. Obligations légales pour le client/l'employeur :

Le SSA conserve les documents suivants au moins pendant les délais de conservation suivants :

- données générales :
  - les données fixes du travailleur (identification, adresse, salaire brut, etc.) : 5 ans
  - l'aperçu des salaires et des prestations : 5 ans
  - tout échange de courrier entre le client/l'employeur et le SSA qui contient des données à caractère personnel : 5 ans

- calculs de salaires :
  - les données du travailleur qui ont été calculées (détail calcul des salaires) : 5 ans
  - la fiche de paie : 5 ans
  - le compte individuel : 5 ans
  - les documents comptables relatifs aux salaires : 7 ans

- les documents complémentaires relatifs au calcul de salaire :
  - l'attestation de voiture de société : 5 ans
  - le registre général du personnel : 5 ans
  - les documents saisie sur salaire : 5 ans
  - les documents transfert de salaire : 5 ans
  - les documents délégation de salaire : 5 ans
  - les documents à la fin du contrat de travail (l'attestation de travail, l'attestation de vacances, …) : 5 ans
  - les fiches fiscales 281.XX : 7 ans
  - le bilan social : 7 ans

- déclarations aux autorités et autres tierces parties :
  - la déclaration trimestrielle DMFA : 3 ans
  - les déclarations fonds de sécurité d'existence : 3 ans
  - la déclaration Dimona : 5 ans
  - la Déclaration Risque Social chômage : 5 ans
  - la Déclaration Risque Social maladie : 5 ans
  - la déclaration précompte professionnel : 7 ans

2.2. Obligation spécifique légale pour le SSA :

La base légale des obligations légales spécifiques pour le SSA figure à l'article 48 de l'AR du 1er juillet 2006 :

Art.48§1. 3° : Le secrétariat social agréé est tenu de constituer et de tenir pour chacun des employeurs affiliés, à un lieu situé en Belgique, un dossier complet relatif à l'application des lois sociales pour l'ensemble du personnel des employeurs affiliés, dossier qui permet de vérifier l'exactitude des déclarations et dont les fonctionnaires et agents visés à l'article 31 de la loi peuvent prendre connaissance ; le contenu de ce dossier est annoncé dans les instructions aux secrétariats sociaux.

La concrétisation de l'article 48 de l'AR du 1er juillet 2006 figure dans les instructions ONSS concernant le dossier employeur :

Récapitulatif des éléments composant le "Dossier unique de l'employeur" :
En exécution des dispositions de l'article 48§ 1,3° de l'AR du 28/11/1969, le dossier unique de l'employeur contiendra les documents ou informations suivants sur papier et/ou sous forme électronique, et ce pour l'ensemble du personnel des employeurs affiliés :

a) Le contrat d'affiliation de l'employeur au SSA ;
b) la procuration donnée au SSA ;
c) Une fiche par travailleur reprenant ses données individuelles (= fiche de renseignements) ;
d) Les données salariales écrites et/ou automatisées contenant des informations au sujet des prestations fournies par les travailleurs ; de sorte qu'il puisse être vérifié si l'input de l'employeur a été correctement transposé dans la déclaration DMFA et si les cotisations sociales ont été correctement calculées ;
e) Les décomptes salariaux tels que définis dans la Loi sur la protection de la rémunération (Loi du 12 avril 1965) ;
f) Les comptes individuels de tous les travailleurs (données d'identification du travailleur) conformément à l'AR du 8 août 1980 concernant la tenue des documents sociaux ;
g) Toute la correspondance entre l'employeur et le SSA qui a ou peut avoir un impact sur les obligations pour lesquelles un secrétariat social a reçu un mandat de l'employeur (également sous forme électronique) ;
h) Le cas échéant, si le SSA a reçu l'ordre de verser aux travailleurs les salaires nets via l'institution bancaire de l'employeur, les documents à l'aide desquels cet ordre de virement peut être démontré ;
i) Les attestations de pécule de vacance reçues qui ont servi de base pour le calcul du pécule de vacances chez le nouvel employeur (si nécessaire, ces documents pourront être réclamés moyennant la fixation d'un délai) ;
j) Un récapitulatif des divers codes utilisés accompagné du détail de ces codes (doit encore être concrétisé) ;
k) Une copie du contrat conclu avec le(s) employeur(s) concerné(s) ou du règlement d'ordre intérieur du SSA vis-à-vis de ses membres affiliés.
Concrètement cela signifie pour le SSA que les délais de conservation légaux des catégories de données à caractère personnel traitées dans le cadre de l'exécution de leurs tâches principales, et pour lesquelles ils ont une obligation spécifique de conservation de 5 ans, sont les suivants :

- les données fixes du travailleur (identification, adresse, salaire brut, etc.)
- l'aperçu des salaires et des prestations
- tout échange de lettre entre le client/l'employeur et le SSA qui contient des données à caractère personnel
- les données du travailleur qui ont été calculées (détail du calcul des salaires)
- la fiche de paie
- le compte individuel
- les documents permettant de démontrer un versement (si le SSA fait verser les salaires nets)
- les documents à la fin du contrat de travail (l'attestation de travail, l'attestation de vacances, …)

Annexe 3 : Sécurité informatique – Mesures techniques et organisationnelles

Le SSA a implémenté les mesures de sécurité nécessaires pour protéger les données à caractère personnel. Ci-dessous un aperçu des principales mesures minimales garanties par le SSA.

1. **Domaine :**

Politique de sécurité et Organisation de la sécurité informatique

Pratiques :

Appropriation pour la sécurité et la protection des données. Le SSA a désigné une personne qui est co-responsable de la coordination et du contrôle des règles et procédures en matière de protection des données.

Responsabilités. Les responsabilités en matière de sécurité informatique des collaborateurs sont définies et attribuées. Le management exige que tous les collaborateurs et entrepreneurs appliquent la sécurité informatique conformément à la politique en vigueur et aux procédures de l'organisation.

2. **Domaine :**

Politique sûre du personnel

Pratiques :

Obligations de confidentialité. Les collaborateurs des SSA sont soumis à des obligations de confidentialité et ces obligations sont reprises formellement dans les contrats de travail et/ou le règlement de travail.

Conscientisation. Le SSA organise régulièrement les actions de sensibilisation adéquates pour ses collaborateurs.

Fin. Les droits d'accès sont retirés à temps lorsque la collaboration s'achève, et ce conformément aux procédures administratives en matière de sécurité.

3. **Domaine :**

Gestion des biens économiques

Pratiques :

Inventaire des biens économiques. Le SSA tient un inventaire à jour de tout le matériel IT et des médias qu'il utilise.

Traitement des biens économiques

- Les règles pour une utilisation acceptable des informations et des biens économiques sont identifiées et implémentées

- Les travailleurs et les parties externes rendent tous les biens économiques en leur possession après l'arrêt de leur emploi ou contrat
- Le SSA dispose de procédures pour la destruction sûre des médias et du matériel imprimé qui contiennent des données confidentielles

4. <u>Domaine</u> :

Contrôle d'accès

<u>Pratiques</u> :

Autorisation d'accès

- Le SSA implémente et maintient un système de gestion des autorisations qui contrôle l'accès aux systèmes qui contiennent les données des clients.
- Chaque individu qui a accès aux systèmes qui contiennent des données des clients a un ID/nom d'utilisateur spécifique, unique.
- Le SSA limite l'accès aux données des clients aux personnes qui ont besoin de cet accès pour remplir leur fonction.

Authentification

- Le SSA utilise des pratiques standard qui répondent aux normes de l'industrie pour identifier et authentifier les utilisateurs qui tentent de s'octroyer l'accès aux systèmes en réseau ou aux systèmes informatiques du SSA.
- Si les mécanismes d'authentification sont basés sur des mots de passe, le SSA exige que les mots de passe comportent au moins huit caractères.
- Le SSA maintient des pratiques pour garantir la confidentialité et l'intégrité des mots de passe lorsqu'ils sont accordés et fournis, ainsi que pendant le stockage.

Accès au réseau. Le SSA implémente les mesures de contrôle nécessaires (p. ex. firewalls, security appliances) qui offrent une certaine sécurité quant à la protection adéquate de l'accès à son réseau.

5. <u>Domaine</u> :

Cryptographie

<u>Pratiques</u> :

Le cryptage des données confidentielles s'organise sur base de standards cryptographiques reconnus (p. ex. Transport Layer Security).

6. <u>Domaine</u> :

Sécurité physique et sécurisation de l'environnement

<u>Pratiques</u> :

Accès physique aux facilités.

- Le SSA restreint aux collaborateurs compétents pour cette tâche l'accès aux facilités où des informations confidentielles sont traitées.
- L'accès physique aux centres de données est exclusivement octroyé selon une procédure d'autorisation formelle, et les droits d'accès sont évalués périodiquement.

Protection contre les dérangements/pannes. Le SSA utilise différents systèmes qui répondent aux normes de l'industrie pour protéger ses centres de données contre les pertes de données à la suite de panne de courant ou d'incendie.

7. Domaine :

Sécurité des activités de l'entreprise (sécurité opérationnelle)

Pratiques :

Récupération des données

- Périodiquement, le SSA fait des back-ups des données des clients à des fins de récupération conformément à la politique de back-up convenue.
- Le SSA conserve des copies des données des clients et des procédures de récupération des données à un autre endroit qu'où se trouve l'appareil informatique primaire qui traite les données des clients.

Software malin. Le SSA mène des contrôles anti-malware pour éviter que le logiciel malin ait accès aux données des clients sans y être autorisé.

Mise à jour de sécurité. Le suivi des mises à jour de sécurité est assuré et celles-ci sont installées.

Enregistrement dans le journal de bord. Le SSA consigne l'accès à et l'utilisation de ses systèmes informatiques qui contiennent des données des clients, en ce compris les users ID, le moment et l'activité en question.

8. Domaine :

Sécurité de la communication

Pratiques :

Transfert en dehors de son propre réseau. Le SSA crypte les données des clients qui sont envoyées via des réseaux publics non sécurisés.

Transferts d'informations. Le transfert de données des clients à des tiers se fait uniquement sur les instructions du client.

9. Domaine :

Acquisition, développement et entretien des systèmes informatiques

Pratiques :

Exigences en matière de sécurité. Dès le début d'un développement, les exigences pour la protection des données sont analysées et implémentées (security et privacy by design).

Séparation du développement et de la production. Les droits d'accès à la production sont limités aux collaborateurs des secrétariats sociaux qui ont besoin d'avoir accès à l'environnement de production dans le cadre de leur fonction.

Contrôle des modifications. Le SSA (ou son prestataire de services IT) a implémenté un processus de gestion des modifications afin de veiller à ce que les modifications dans des systèmes et applications opérationnels se fassent de manière contrôlée.

10. Domaine :
Relations aux fournisseurs

Pratiques :
Choix des fournisseurs. Le SSA maintient un processus de sélection dans lequel il évalue les pratiques en matière de sécurité et de vie privée d'un fournisseur/partenaire lors du traitement des données.

Obligations contractuelles. Les fournisseurs ayant accès aux données des clients sont soumis à des obligations en matière de protection des données et celles-ci sont reprises formellement dans les contrats des fournisseurs.

11. Domaine :
Gestion des incidents liés à la sécurité informatique

Pratiques :
Notification des incidents. En cas d'un incident lié à la sécurité informatique qui a un impact sur la confidentialité ou l'intégrité des données des clients, le SSA en informera le client sans retard irraisonnable.

12. Domaine :
Continuité de l'entreprise

Pratiques :
Récupération d'urgence. Le SSA garantit l'existence d'un plan de récupération d'urgence pour les centres de données où se trouvent les systèmes informatiques du SSA qui traitent des données de clients.

Redondance. Le SSA dispose d'un stockage et de procédures redondants pour la récupération des données. Ceux-ci sont conçus dans le but de récupérer les données des clients dans l'état où elles ont été sauvegardées en dernier juste avant le moment où ces données ont été perdues ou détruites.

13. Domaine :
Respect

Pratiques :
Évaluations de la sécurité. Le respect des contrôles de la sécurité informatique est évalué périodiquement.

Annexe 4 : Questionnaire pour l'évaluation annuelle du respect des lignes directrices
Voir document WORD