Gedragscode GDPR- USS	Code de conduite GDPR- USS
1. Definities	**1. Définitions**
1.1. Definities die in de GDPR gehanteerd worden zijn in bijlage 1 opgenomen.	1.1. Les définitions utilisées dans le GDPR sont reprises à l'annexe 1.
1.2. ESS: Erkend Sociaal Secretariaat	1.2. SSA : Secrétariat Social Agréé
1.3. GDPR: General Data Protection Regulation. In het Nederlands afgekort als AVG (Algemene Verordening Gegevensbescherming).	1.3. GDPR : General Data Protection Regulation. Abrégé en français "RGPD" (le Règlement Général sur la Protection des Données).
1.4. GBA: Gegevensbeschermingsautoriteit, de toezichthoudende autoriteit op de bescherming van persoonsgegevens binnen België.	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. Subverwerker: de onderaannemer die door het sociaal secretariaat wordt aangesteld om een deel van het verwerkingsproces van het ESS voor de verwerkingsverantwoordelijke op te nemen, waarbij ook persoonsgegevens worden verwerkt.	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: Unie Sociale Secretariaten	1.6. USS : Union des Secrétariats Sociaux
2. Inleiding	**2. Introduction**
2.1. 90 % van de werkgevers in de privésector in België doet beroep op een ESS voor hun sociale administratie. Het ESS verwerkt in het kader van haar bedrijfsvoering persoonsgegevens en vindt het belangrijk dat met deze persoonsgegevens zorgvuldig wordt omgegaan en dat deze vertrouwelijk worden behandeld. Om die reden wenst de USS een gedragscode te hanteren waarbij afspraken gemaakt worden over de concrete toepassing van de GDPR voor de sector van de sociale secretariaten in hun rol als verwerker. De gedragscode definieert een kader waarbinnen gegarandeerd kan worden dat persoonsgegevens van werknemers van de klanten van de sociale	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 un code de conduite qui formalise l'application concrète du GDPR dans le secteur des secrétariats sociaux en tant que sous-traitants. Le code de conduite définit 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.

secretariaten op een uniforme manier worden verwerkt en aan dezelfde strikte beschermingsmaatregelen voldoen. 2.2. De sectorale gedragscode (verder 'gedragscode') voor de verwerking van persoonsgegevens onder de GDPR lijst op bevattelijke wijze de krachtlijnen van het door de USS gevoerde informatiebeschermingsbeleid op. 2.3. De gedragscode: • is bindend voor het ESS dat de gedragscode ondertekent; • bevat richtlijnen hoe er moet worden omgegaan met persoonsgegevens in het kader van de dienstverlening; • draagt bij tot de transparantie van door de sector gehanteerde verwerkingsmethoden van persoonsgegevens; • biedt aanknopingspunten voor de Gegevensbeschermingsautoriteit ("GBA") om te beoordelen of de verwerking van de persoonsgegevens volgens de geldende wet- en regelgeving geschiedt; • wil een antwoord bieden op de rechtmatige verwachtingen van opdrachtgevers dat persoonsgegevens van hun medewerkers op een correcte manier zullen worden verwerkt.	2.2. Le code de conduite sectoriel (ci-après dénommé "le code de conduite") relatif au traitement des données à caractère personnel dans le cadre du GDPR liste clairement les lignes de force de la stratégie en matière de protection des données mise en œuvre par l'USS. 2.3. Le code de conduite : • est contraignant pour le SSA qui signe le code de conduite • 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 loi 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. Toepassingsgebied	## 3. Champ d'application
De gedragscode is van toepassing op het ESS dat in België erkend en gevestigd is voor de uitvoering van haar kerntaken in België. De gedragscode is enkel van toepassing op het verwerken van persoonsgegevens in het kader van de kerntaken van het ESS, met name: • loonberekeningen en bijhorende documenten • aangiftes aan de Overheid en andere derde partijen • innen en doorstorten van RSZ-bijdragen en bedrijfsvoorheffing	Le code de conduite s'applique au SSA agréé et établi en Belgique pour l'exécution de sa mission principale en Belgique. Le code de conduite s'applique exclusivement au traitement des données à caractère personnel dans le cadre des tâches principales du SSA : • calculs de salaires et documents y afférents • déclarations aux autorités et autres tierces parties • perception et versement des cotisations ONSS et du précompte professionnel

• sociaal en arbeidsrechtelijk juridisch advies met betrekking tot de sociale administratie van de werkgever De verwerkingsdoeleinden van het ESS als verwerker zijn de uitvoering van bovenstaande kerntaken. In het kader van de uitoefening van deze kerntaken verwerkt het ESS geen bijzondere categorieën van persoonsgegevens zoals beschreven in artikel 9 van de GDPR. De door de klant/werkgever aangeleverde data, die niet noodzakelijk zijn voor de uitvoering van de kerntaken van het ESS, vallen buiten het toepassingsgebied van deze sectorale gedragscode.	• 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 ce code de conduite sectoriel.
## 4. Relatie ESS – klant/werkgever	## 4. Relation SSA – client/employeur
4.1. Het ESS is in het kader van de uitvoering van haar kerntaken steeds verwerker. De verwerkingsverantwoordelijke hierbij is steeds de klant/werkgever. 4.2. De rechtsgrond voor het ESS is het contract met de klant/werkgever en de toepasselijke wettelijke verplichtingen die het ESS heeft als mandataris.	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. Gegevensbeschermings-effectbeoordeling	## 5. Analyse d'impact relative à la protection des données
Als verwerker dient het ESS geen gegevensbeschermingseffectbeoordeling of Data Protection Impact Assessment (verder "DPIA") uit te voeren. Een DPIA is immers een verplichting die enkel op de verwerkingsverantwoordelijke rust. De USS wijst er bovendien op dat de GBA aangeeft dat loonadministratie en administratie van personeel verwerkingsactiviteiten zijn waarvoor er geen DPIA verplichting is (Bijlage 3 van Aanbeveling nr. 01/2018 van 28 februari 2018).	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 »). Un 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).

Niettemin engageert het ESS zich om: • op verzoek, haar klanten bijstand te verlenen bij het doen nakomen van de DPIA-verplichtingen uit hoofde van artikel 35 van de GDPR • een risicoanalyse te maken van de verwerkingsactiviteiten die worden uitgevoerd in opdracht van de klanten opdat de gepaste en noodzakelijke technische en organisatorische maatregelen kunnen worden genomen (zie ook artikel 12 van deze gedragscode).	Le SSA s'engage cependant à : • aider ses clients à respecter leurs obligations AIPD (Analyse d'impact de la protection des données) 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 ce code de conduite).
## 6. Register van verwerkingsactiviteiten	## 6. Registre des activités de traitement
Het ESS houdt conform artikel 30.2 van de GDPR een intern register van verwerkingsactiviteiten bij.	Conformément à l'article 30.2 du GDPR, le SSA tient un registre interne des activités de traitement.
## 7. Subverwerkers	## 7. Sous-traitants ultérieurs
Het ESS, dat beroep doet op subverwerkers voor de uitvoering van haar kerntaken: • sluit met de subverwerker een verwerkersovereenkomst af die minimaal dezelfde verplichtingen inzake gegevensbescherming bevat als in de respectievelijke verwerkingsovereenkomst die het ESS met haar klant(en) afsluit; • garandeert dat de klant zijn voorafgaandelijke schriftelijke toestemming geeft voor het inzetten van subverwerkers. Dit kan de vorm aannemen van een algemene of een specifieke toestemming; • heeft een werkwijze om elke klant voorafgaandelijk te informeren over de toevoeging of vervanging van subverwerkers; • heeft een werkwijze om een bezwaar van een klant af te handelen; • houdt een lijst bij van hun subverwerkers. Deze lijst is minstens op verzoek beschikbaar.	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.

Het ESS beschouwt de volgende derden niet als haar subverwerkers: • de instellingen van Sociale Zekerheid; • de FOD Financiën; • de regionale overheden; • de organisaties aan wie het ESS persoonsgegevens van de werknemers van de klant doorgeeft op basis van instructies van de klant, maar waarmee het ESS geen contractuele band heeft, zoals onder meer leveranciers van maaltijdcheques, leasemaatschappijen, groepsverzekeringen en fondsen voor bestaanszekerheid.	Le SSA ne considère pas les tiers suivants comme étant des sous-traitants ultérieurs : • 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. Doorgifte aan derden van persoonsgegevens	**8. Transfert de données personnelles à des tiers**
Het ESS geeft enkel gegevens door in het kader van haar kerntaken of op formele instructie van de klant. Deze instructie kan in een overeenkomst vervat zitten of onder een andere vorm geregistreerd worden (bv. via online tool).	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. Bewaartermijnen	**9. Délais de conservation**
9.1. <u>Bewaartermijnen voor de klant/werkgever, als verwerkingsverantwoordelijke, voor het bewaren van documenten waar voor hem een wettelijke verplichting tot bewaren op rust:</u> Het ESS bewaart de documenten vermeld in bijlage 2.1, die ze effectief verwerken als onderdeel van hun kerntaken, minimaal gedurende de bewaartermijnen zoals opgelijst in bijlage 2.1. te rekenen van af het jaar volgend op de periode waarop het document betrekking heeft, tenzij anders overeengekomen met de klant/werkgever. 9.2. <u>Bewaartermijnen voor het ESS, als verwerker, voor het bewaren van de documenten waar voor hem een wettelijke verplichting tot bewaren op rust:</u> Het ESS bewaart de documenten vermeld in bijlage 2.2, die ze effectief verwerken	9.1. <u>Délais de conservation pour le client/l'employeur, en tant que responsable du traitement, pour la conservation des documents pour lesquels il est soumis à une obligation légale de conservation :</u> 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. <u>Délais de conservation pour le SSA, en tant que sous-traitant, pour la conservation des documents pour lesquels il est soumis à une obligation légale de conservation :</u> Le SSA conserve les documents mentionnés à l'annexe 2.2 qu'il traite effectivement dans

als onderdeel van hun kerntaken, gedurende de bewaartermijnen zoals opgelijst in bijlage 2.2. te rekenen van af het jaar volgend op de periode waarop het document betrekking heeft.	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. <u>Dataretentiebeleid</u> Het ESS heeft een dataretentiebeleid dat rekening houdt met het principe van artikel 5.1.e van de GDPR (opslagbeperking). In dit beleid is minstens opgenomen dat het ESS de verwijdering/anonimisering zal doorvoeren uiterlijk 7 jaar na het beëindigen van de arbeidsovereenkomst tussen de klant en zijn werknemer en uiterlijk 7 jaar na het beëindigen van de overeenkomst tussen het ESS en de klant, behoudens afwijkend akkoord met de klant. Deze termijn van 7 jaar begint te lopen op de eerste dag van het jaar na het beëindigen van de arbeidsovereenkomst van de werknemer of het contract met de klant. Na het verstrijken van de bewaartermijn worden deze gegevens binnen een redelijke termijn verwijderd of geanonimiseerd.	9.3. <u>Politique de rétention des données</u> 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.
Dit dataretentiebeleid bevat minstens de volgende elementen: • Of de klant al dan niet de mogelijkheid heeft om het verwijderen of anonimiseren van de persoonsgegevens zelf te beheren; • Hoe het ESS omgaat met het bewaren/verwijderen/anonimiseren van persoonsgegevens • De bewaartermijnen per categorie van persoonsgegevens van werknemers	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. Verantwoordelijke gegevensbescherming	## 10. Responsable de la protection des données
Het ESS engageert zich om een verantwoordelijke aan te duiden voor de gegevensbescherming en het naleven van deze gedragscode. Deze verantwoordelijke is	Le SSA s'engage à désigner un responsable pour la protection des données et à respecter ce code de conduite. Ce responsable est également la personne de contact dans le cadre de la

ook contactpersoon in het kader van de gegevensbescherming. Het ESS publiceert de contactgegevens waarop deze contactpersoon bereikbaar is. De USS engageert zich om een stuurgroep gegevensbescherming te installeren die bestaat uit de verantwoordelijken gegevensbescherming van de sociale secretariaten die lid zijn van de USS. De opdracht van deze stuurgroep is onder meer om: • nieuwe ontwikkelingen op het vlak van gegevensbescherming op te volgen; • best practices binnen de sector uit te wisselen; • een jaarlijkse review van deze gedragscode en de vragenlijst voor de zelfevaluatie uit te voeren.	protection des données. Le SSA publie les données de cette personne de contact. L'USS s'engage à créer un groupe de pilotage 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 ce code de conduite et du questionnaire pour l'auto-évaluation.
## 11. Datalekken	## 11. Fuites de données
Van zodra het ESS kennis heeft genomen van een datalek, informeert het de betrokken klant/werkgever (verwerkingsverantwoordelijke) hierover zonder onredelijke vertragingen. Het ESS heeft standaardprocedures uitgewerkt voor het melden aan de klant en het beheer van datalekken. Het ESS zal, op basis van de beschikbare informatie, de redelijke bijstand verlenen aan de verwerkingsverantwoordelijke bij het afhandelen van een datalek. Het is de verantwoordelijkheid van de verwerkingsverantwoordelijke (klant/werkgever) om na te gaan of de betrokkenen/GBA eventueel dienen ingelicht te worden over een datalek. Tenzij expliciet anders afgesproken met de klant, zal het ESS de betrokkenen/GBA niet inlichten over een datalek.	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. Informatiebeveiliging – Technische en organisatorische maatregelen	12. Sécurité informatique – Mesures techniques et organisationnelles
Het ESS implementeert de beveiligingsmaatregelen om persoonsgegevens te beschermen, zoals beschreven in bijlage 3. Deze bijlage geeft een overzicht van de belangrijkste maatregelen die het ESS minimaal garandeert.	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. Rechten van de betrokkene	13. Droits de la personne concernée
Indien het ESS vragen van betrokkenen ontvangt tot uitoefening van hun rechten, dan maakt het ESS deze uiterlijk binnen de 14 kalenderdagen over aan de klant/werkgever. Het ESS geeft de redelijke bijstand aan haar klant/werkgever om de werkgever toe te laten adequaat te antwoorden op vragen van betrokkenen. Het ESS heeft standaardprocedures uitgewerkt voor de toepassing van het uitoefenen van de rechten van de betrokkenen.	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. Naleving van de gedragscode	14. Respect du code de conduite
Het ESS bevestigt jaarlijks schriftelijk aan de USS dat ze de gedragscode naleeft. Het ESS doet een jaarlijkse zelfevaluatie van de toepassing van deze gedragscode binnen zijn ESS op basis van een vragenlijst, opgenomen in bijlage 4. Bij problemen van niet naleving van de code, zal de USS dit melden aan het betrokken ESS.	Le SSA confirme annuellement par écrit à l'USS qu'il respecte le code de conduite. Le SSA réalise une auto-évaluation annuelle de l'application de ce code de conduite au sein de son SSA sur base d'un questionnaire, repris à l'annexe 4. En cas de problèmes de non-respect du code, l'USS le mentionnera au SSA concerné.

Bijlage 1: begripsbepalingen	Annexe 1 : définitions
In deze Gedragscode wordt verstaan onder: **Definities gekopieerd vanuit de GDPR:** **Persoonsgegeven**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon **Bijzondere categorieën persoonsgegevens:** Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon of gegevens over gezondheid of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. • **Genetische gegevens:** persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon; • **Biometrische gegevens:** persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de	Aux fins du présent code de conduite, 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,

fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens; • **Gegevens over gezondheid:** persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;	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 ;
Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;	**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;
Betrokkene: een geïdentificeerde of identificeerbare natuurlijke persoon	**Personne concernée** : une personne physique identifiée ou identifiable
Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;	**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 ;
Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de	**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 ;

verwerkingsverantwoordelijke persoonsgegevens verwerkt;	
Derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;	**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 ;
Functionaris Gegevensbescherming: De functionaris voor gegevensbescherming ziet toe op de gegevensverwerkingen binnen de organisatie.	**Délégué à la protection des données (DPO)** : Le délégué à la protection des données contrôle les traitements de données au sein de son organisation.
Datalek – inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;	**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) - Gegevensbeschermingseffectbeoordeling: is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen en daarna maatregelen te kunnen nemen om de risico's te verkleinen. In het Nederlands afgekort als GEB (GegevensBeschermingsEffectbeoordeling)	**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).

Bijlage 2: Wettelijke bewaartermijnen voor de categorieën van verwerkte persoonsgegevens voor het uitvoeren van de kerntaken:	Annexe 2 : délais légaux de conservation pour les catégories de données à caractère personnel traitées dans le cadre des tâches principales :
2.1. <u>Wettelijke verplichtingen voor de klant/werkgever:</u> Het ESS bewaart de volgende documenten minimaal gedurende de volgende bewaartermijnen: • algemene gegevens: o de vaste gegevens werknemer (identificatiegegevens, adres, bruto loon, enz.): 5 jaar o de opgave lonen en prestaties: 5 jaar o alle briefwisseling tussen de klant/werkgever en het ESS die persoonsgegevens bevat: 5 jaar • loonberekeningen: o de berekende gegevens van de werknemer (detail loonberekening): 5 jaar o de loonbrief: 5 jaar o de individuele rekening: 5 jaar o de boekhouddocumenten lonen: 7 jaar • bijhorende documenten bij de loonberekening: o het bedrijfswagenattest: 5 jaar o het algemeen personeelsregister: 5 jaar o de documenten loonbeslag: 5 jaar o de documenten loonoverdracht: 5 jaar o de documenten loondelegatie: 5 jaar o de documenten bij het einde van de arbeidsovereenkomst (het tewerkstellingsattest, het vakantie-attest,…): 5 jaar o de fiscale fiches 281.XX: 7 jaar o de sociale balans: 7 jaar • aangiftes aan de Overheid en andere derde partijen: o de DMFA kwartaalaangifte: 3 jaar o de aangiftes fondsen voor bestaanszekerheid: 3 jaar o de Dimona aangifte: 5 jaar	2.1. <u>Obligations légales pour le client/l'employeur :</u> Le SSA conserve les documents suivants au moins pendant les délais de conservation suivants : • données générales : o les données fixes du travailleur (identification, adresse, salaire brut, etc.) : 5 ans o l'aperçu des salaires et des prestations : 5 ans o tout échange de courrier entre le client/l'employeur et le SSA qui contient des données à caractère personnel : 5 ans • calculs de salaires : o les données du travailleur qui ont été calculées (détail calcul des salaires) : 5 ans o la fiche de paie : 5 ans o le compte individuel : 5 ans o les documents comptables relatifs aux salaires : 7 ans • les documents complémentaires relatifs au calcul de salaire : o l'attestation de voiture de société : 5 ans o le registre général du personnel : 5 ans o les documents saisie sur salaire : 5 ans o les documents transfert de salaire : 5 ans o les documents délégation de salaire : 5 ans o les documents à la fin du contrat de travail (l'attestation de travail, l'attestation de vacances, …) : 5 ans o les fiches fiscales 281.XX : 7 ans o le bilan social : 7 ans • déclarations aux autorités et autres tierces parties : o la déclaration trimestrielle DMFA : 3 ans o les déclarations fonds de sécurité d'existence : 3 ans o la déclaration Dimona : 5 ans

o de Aangifte Sociaal Risico werkloosheid: 5 jaar o de Aangifte Sociaal Risico ziekte: 5 jaar o de aangifte bedrijfsvoorheffing: 7 jaar	o la Déclaration Risque Social chômage : 5 ans o la Déclaration Risque Social maladie : 5 ans o la déclaration précompte professionnel : 7 ans
2.2. Specifieke wettelijke verplichting voor het ESS:	2.2. Obligation spécifique légale pour le SSA :
De wettelijke basis voor de specifieke wettelijke verplichtingen voor het ESS is terug te vinden in artikel 48 van het KB van 1 juli 2006: Art.48§1.3°: Het erkend sociaal secretariaat is ertoe gehouden voor ieder van de aangesloten werkgevers, op een plaats in België, een volledig dossier betreffende de toepassing van de sociale wetten samen te stellen en bij te houden voor het geheel van het personeel van de aangesloten werkgevers en dat toelaat de juistheid van de aangiften na te gaan en waarvan de ambtenaren en beambten beoogd bij artikel 31 van de wet inzage kunnen nemen; de inhoud van dit dossier wordt bekendgemaakt in de onderrichtingen aan de sociale secretariaten.	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.
De concrete invulling van het artikel 48 van het KB van 1 juli 2006 is terug te vinden in de onderrichtingen van de RSZ m.b.t. het werkgeversdossier:	La concrétisation de l'article 48 de l'AR du 1er juillet 2006 figure dans les instructions ONSS concernant le dossier employeur :
Overzicht van de elementen die deel uitmaken van het "Uniek werkgeversdossier": Het werkgeversdossier zal in uitvoering van de bepalingen van artikel 48§1.3° van het KB van 28/11/1969, volgende documenten of informatie op papier en/of onder elektronische vorm bevatten, en dit voor het geheel van het personeel van de aangesloten werkgevers: a) Het aansluitingscontract van de werkgever bij het ESS; b) De procuratie aan het ESS; c) Een fiche per werknemer met zijn/haar individuele gegevens (= inlichtingsfiche); d) De geschreven loonsopdrachten en/of de geautomatiseerde loonsopdrachten die de	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

nodige informatie bevatten op vlak van de door de werknemers geleverde prestaties; zodanig dat kan worden nagegaan dat de input van de werkgever correct vertaald werd in de DmfA-aangifte, en dat de sociale bijdragen correct berekend werden; e) De loonafrekeningen zoals gedefinieerd in de Wet op de loonbescherming (Wet van 12 april 1965); f) De individuele rekeningen van alle werknemers (identificatiegegevens van de werknemer) in overeenstemming met het KB van 8 augustus 1980 omtrent het bijhouden van de sociale documenten; g) Alle briefwisseling tussen de werkgever en het ESS, die een impact heeft of kan hebben op de verplichtingen waarvoor het sociaal secretariaat een mandaat kreeg van de werkgever (ook onder elektronische vorm); h) Desgevallend, indien het ESS de opdracht gekregen heeft om de nettolonen via de bankinstelling van de werkgever aan de werknemers te laten storten, de documenten aan de hand waarvan deze stortingsopdracht kan worden aangetoond; i) De ontvangen vakantiegeldattesten die gediend hebben als basis voor de berekening van het vakantiegeld bij de nieuwe werkgever (indien nodig zal er mits een termijnstelling een opvraging gebeuren); j) Een overzicht van de op de diverse documenten gebruikte codes aangevuld met het detail van de code (nog verder te concretiseren); k) Een kopie van de overeenkomst met de betrokken werkgever(s) of het huishoudelijk reglement van het ESS t.o.v. zijn aangesloten leden. Concreet betekent dit dat voor het ESS de wettelijke bewaartermijnen voor de categorieën van verwerkte persoonsgegevens voor het uitvoeren van hun kerntaken, waar voor hen een specifieke verplichting van bewaren van 5 jaar op rust, de volgende zijn:	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 :

• De vaste gegevens werknemer (identificatiegegevens, adres, bruto loon, enz.) • De opgave van de lonen en de prestaties • Alle briefwisseling tussen de klant/werkgever en het ESS die persoonsgegevens bevat • De berekende gegevens van de werknemer (detail loonberekening) • De loonbrief • De individuele rekening • De documenten om een stortingsopdracht aan te tonen (als het ESS de nettolonen laat storten) • De documenten bij het einde van de arbeidsovereenkomst (het tewerkstellingsattest, het vakantieattest,..)	• 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, …)

Bijlage 3: Informatiebeveiliging – Technische en organisatorische maatregelen	Annexe 3 : Sécurité informatique – Mesures techniques et organisationnelles
Het ESS heeft de nodige beveiligingsmaatregelen geïmplementeerd om persoonsgegevens te beschermen. Hieronder volgt een overzicht van de belangrijkste maatregelen die het ESS minimaal garandeert.	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. **Domein:** Beveiligingsbeleid en Organisatie van informatiebeveiliging **Praktijken:** **Eigenaarschap voor beveiliging en gegevensbescherming**. Het ESS heeft een verantwoordelijke aangewezen die mee verantwoordelijk is voor het coördineren en controleren van de gegevensbeschermingsregels en -procedures. **Verantwoordelijkheden**. De informatiebeveiligingsverantwoordelijkheden van medewerkers zijn gedefinieerd en toegewezen. Het management vereist van alle werknemers en aannemers dat ze informatiebeveiliging toepassen in overeenkomst met het geldende beleid en de procedures van de organisatie.	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. **Domein:** Veilig personeelsbeleid **Praktijken:** **Vertrouwelijkheidsverplichtingen.** ESS medewerkers zijn onderworpen aan vertrouwelijkheidsverplichtingen en deze verplichtingen worden formeel opgenomen in arbeidsovereenkomsten en/of arbeidsreglement. **Bewustmaking**. Het ESS organiseert op geregelde tijdstippen de gepaste sensibilisatieacties voor hun medewerkers.	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.

Beëindiging. Toegangsrechten worden bij beëindiging van de samenwerking tijdig ingetrokken, in overeenstemming met de beveiligingsadministratieprocedures.	**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. <u>Domein:</u> Beheer van bedrijfsmiddelen **<u>Praktijken:</u>** **Inventaris van bedrijfsmiddelen.** Het ESS houdt een inventaris bij van alle IT-materiaal en media die het gebruikt. **Behandeling van bedrijfsmiddelen** - Regels voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen zijn geïdentificeerd en geïmplementeerd - Werknemers en externe partijen geven alle bedrijfsmiddelen in hun bezit terug na stopzetting van hun tewerkstelling, contract of overeenkomst - Het ESS beschikt over procedures voor het veilig vernietigen van media en afgedrukt materiaal die vertrouwelijke data bevatten	**3. <u>Domaine</u> :** Gestion des biens économiques **<u>Pratiques</u> :** **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>Domein:</u> Toegangscontrole **<u>Praktijken:</u>** **Toegangsautorisatie** - Het ESS implementeert en handhaaft een autorisatiebeheersysteem dat de toegang controleert tot systemen die klantengegevens bevatten. - Elk individu die toegang heeft tot systemen die klantengegevens bevatten, heeft een aparte, unieke ID/gebruikersnaam. - Het ESS beperkt de toegang tot klantengegevens tot die personen die dergelijke toegang nodig hebben om hun functie uit te voeren. **Authenticatie** - Het ESS maakt gebruik van standaardpraktijken die voldoen aan industrienormen om gebruikers te identificeren en te authentiseren die zich proberen toegang te verschaffen tot de	**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

netwerk- of informatiesystemen van het ESS. - Indien authenticatiemechanismen gebaseerd zijn op wachtwoorden, dan vereist het ESS dat de wachtwoorden ten minste acht tekens lang zijn. - Het ESS handhaaft praktijken om de vertrouwelijkheid en integriteit van wachtwoorden te garanderen wanneer ze worden toegekend en verstrekt, en tijdens de opslag. **Netwerktoegang**. Het ESS implementeert de nodige controlemaatregelen (bv. firewalls, security appliances) die een redelijke mate van zekerheid bieden dat toegang tot zijn netwerk op gepaste wijze wordt beschermd.	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>Domein:</u> Cryptografie **<u>Praktijken:</u>** Versleuteling van vertrouwelijke data gebeurt aan de hand van erkende cryptografische standaarden (bv Transport Layer Security).	**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>Domein:</u> Fysieke beveiliging en beveiliging van de omgeving **<u>Praktijken:</u>** **Fysieke toegang tot faciliteiten.** - Het ESS beperkt de toegang tot faciliteiten waar vertrouwelijke informatie wordt verwerkt tot hiervoor bevoegde medewerkers. - Fysieke toegang tot datacentra wordt uitsluitend toegekend volgens een formele autorisatieprocedure, en toegangsrechten worden periodiek beoordeeld. **Bescherming tegen verstoringen.** Het ESS gebruikt verschillende systemen die voldoen aan industrienormen om zijn datacentra te beschermen tegen gegevensverlies als gevolg van stroomuitval en brand.	**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. <u>Domein:</u>	**7. <u>Domaine</u> :**

Beveiliging van de bedrijfsactiviteiten (operationele beveiliging) **Praktijken:** **Gegevensherstel** - Het ESS maakt op periodieke basis back-ups van klantengegevens voor hersteldoeleinden in overeenstemming met een overeengekomen back-up beleid. - Het ESS bewaart kopieën van klantengegevens en gegevensherstelprocedures op een andere plaats dan waar de primaire computerapparatuur die de klantengegevens verwerkt, zich bevindt. **Kwaadaardige Software**. Het ESS voert anti-malwarecontroles uit om te helpen voorkomen dat kwaadaardige software ongeautoriseerde toegang tot klantengegevens krijgt. **Beveiligingsupdates**. Beveiligingsupdates worden opgevolgd en geïnstalleerd. **Logboekregistratie**. Het ESS registreert de toegang tot en het gebruik van zijn informatiesystemen die klantendata bevatten, met inbegrip van de gebruikers ID, de tijd en de desbetreffende activiteit.	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. **Domein:** Communicatiebeveiliging **Praktijken:** **Transfer buiten eigen netwerk.** Het ESS versleutelt klantengegevens die worden verzonden via publieke, niet-vertrouwde netwerken. **Informatieoverdracht**. Overdracht van klantengegevens aan derde partijen geschiedt enkel op instructie van de klant.	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 sûrs. **Transferts d'informations**. Le transfert de données des clients à des tiers se fait uniquement sur les instructions du client.
9. **Domein:** Verwerving, ontwikkeling en onderhoud van informatiesystemen **Praktijken:**	9. **Domaine :** Acquisition, développement et entretien des systèmes informatiques **Pratiques :**

Beveiligingsvereisten. Van bij de start van een ontwikkeling worden de vereisten voor gegevensbescherming geanalyseerd en geïmplementeerd (security en privacy by design). **Scheiding van ontwikkeling en productie.** Toegangsrechten tot productie worden beperkt tot enkel de medewerkers van de sociale secretariaten die in het kader van hun functie toegang nodig hebben tot de productieomgeving. **Controle over wijzigingen**. Het ESS (of haar IT-dienstenleverancier) heeft een wijzigingsbeheerproces geïmplementeerd om ervoor te zorgen dat wijzigingen in operationele systemen en toepassingen plaatsvinden op een gecontroleerde wijze.	**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. <u>Domein:</u> Leveranciersrelaties **<u>Praktijken:</u>** **Keuze van leveranciers**. Het ESS handhaaft een selectieproces waarbij het de beveiliging en privacy praktijken van een leverancier/partner met betrekking tot gegevensverwerking evalueert. **Contractuele verplichtingen**. Leveranciers met toegang tot klantengegevens zijn onderworpen aan verplichtingen inzake gegevensbescherming en deze worden formeel opgenomen in leverancierscontracten.	**10. <u>Domaine</u> :** Relations aux fournisseurs **<u>Pratiques</u> :** **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. <u>Domein:</u> Beheer van informatiebeveiligings-incidenten **<u>Praktijken:</u>** **Notificatie van incidenten**. In geval van een informatiebeveiligingsincident dat impact heeft op de vertrouwelijkheid of integriteit van klantengegevens, zal het ESS, zonder onredelijke vertraging, de klant hiervan informeren.	**11. <u>Domaine</u> :** Gestion des incidents liés à la sécurité informatique **<u>Pratiques</u> :** **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. <u>Domein:</u> Bedrijfscontinuïteit	**12. <u>Domaine</u> :** Continuité de l'entreprise

Praktijken: **Noodherstel**. Het ESS verzekert het bestaan van een noodherstelplan voor de datacentra waar zich informatiesystemen van het ESS bevinden die klantengegevens verwerken. **Redundantie**. Het ESS beschikt over redundante opslag en procedures voor gegevensherstel die ontworpen zijn met als doel klantengegevens te herstellen in hun laatst geback-upte staat voor het tijdstip waarop ze verloren gegaan zijn of vernietigd werden.	**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. Domein: Naleving **Praktijken:** **Beveiligingsevaluaties**. De naleving van informatiebeveiligingscontroles wordt op periodieke basis geëvalueerd.	**13. Domaine :** Respect **Pratiques :** **Évaluations de la sécurité**. Le respect des contrôles de la sécurité informatique est évalué périodiquement.

Bijlage 4: Vragenlijst voor jaarlijkse evaluatie naleving gedragscode	Annexe 4 : Questionnaire pour l'évaluation annuelle du respect du code de conduite
Zie WORD document	Voir document WORD