Checklist zelfevaluatie **Richtlijnen GDPR - USS**	**Questionnaire évaluation** **Lignes directrices de conduite GDPR - USS**	Si la réponse est NO ou NA, veuillez commenter. Indien het antwoord NO of NA is, gelieve commentaar bij te zetten.			
Vragen	Questions	Antwoorden / Réponses			Commentaar / Commentaire
		YES	**NO**	**NA**	
5. Gegevensbeschermingseffectbeoordeling (GEB)	5. Analyse d'impact relative à la protection des données (AIPD)				
a) Heeft het ESS de nodige middelen om een effectbeoordeling voor de werkgever/klant uit te voeren?	a) Le SSA dispose-t-il des moyens nécessaires pour réaliser une analyse d'impact pour le compte de l'employeur/du client ?				
b) Heeft het ESS in zijn algemene voorwaarden contractueel afgesproken dat hij op vraag van de klant assisteert bij het doen nakomen van de DPIA-verplichtingen?	b) Le SSA a-t-il contractuellement convenu dans ses conditions générales qu'il assiste, à la demande du client, au contrôle du respect des obligations de l'AIPD ?				
c) Heeft het ESS een risico analyse gemaakt van de verwerkingsactiviteiten die worden uitgevoerd in opdracht van de klanten?	c) Le SSA a-t-il fait une analyse des risques des activités de traitement réalisées pour les clients ?				
6. Register van de verwerkingsactiviteiten	6. Registre des activités de traitement				
a) Heeft het ESS een register van de verwerkingsactiviteiten opgesteld?	a) Le SSA a-t-il établi un registre des activités de traitement ?				
b) Heeft het ESS de categorieën van de verwerkte persoonsgegevens geïnventariseerd?	b) Le SSA a-t-il établi un inventaire des catégories de données personnelles traitées ?				
c) Zijn minstens de kerntaken van het ESS opgenomen in het register van de verwerkingsactiviteiten?	c) Au moins toutes les tâches principales du SSA sont-elles répertoriées dans le registre des activités de traitement ?				
d) Wordt het register van de verwerkingsactiviteiten minstens jaarlijks bijgewerkt door het ESS?	d) Le registre des activités de traitement est-il actualisé par le SSA au moins chaque année ?				

7. Subverwerkers	7. Sous-traitants ultérieurs				
a) Heeft het ESS een lijst van subverwerkers opgesteld?	a) Le SSA a-t-il établi une liste de ses sous-traitants ?				
b) Is de lijst van de subverwerkers van het ESS minstens op verzoek toegankelijk voor de relevante partijen?	b) La liste des sous-traitants du SSA est-elle au moins accessible à la demande des parties concernées ?				
c) Heeft het ESS een voorafgaandelijke schriftelijke toestemming voor het gebruik van subverwerkers van de klant bekomen?	c) Le SSA a-t-il obtenu du client une autorisation écrite générale préalable pour le recours à des sous-traitants ?				
d) Heeft het ESS verwerkersovereenkomsten afgesloten met zijn subverwerkers?	d) Le SSA a-t-il conclu un contrat de traitement avec ses sous-traitants ?				
e) Heeft het ESS een werkwijze bepaald om de klant te informeren bij wijziging of toevoeging van subverwerkers?	e) Le SSA a-t-il une méthode de travail pour informer le client du changement ou de l'ajout des sous-traitants ?				
f) Heeft het ESS een werkwijze bepaald met het oog op het behandelen van een eventueel bezwaar van een klant tegenover een subverwerker?	f) Le sous-traitant a-t-il une méthode de travail pour traiter une plainte éventuelle d'un client par rapport à un sous-traitant ultérieur ?				
8. Doorgifte aan derden van persoonsgegevens	8. Transfert de données personnelles à des tiers				
a) Geeft het ESS alleen persoonsgegevens door in kader van de kerntaken of in opdracht van de klant?	a) Le SSA transmet-il uniquement des données personnelles dans le cadre des missions principales ou à la demande du client ?				
9. Bewaartermijnen	9. Délais de conservation				
a) Heeft het ESS een dataretentiebeleid waarin de bewaarduur bepaald wordt voor elk verwerkt gegeven of document?	a) Le SSA a-t-il une politique de rétention des données dans laquelle la durée de conservation est précisée pour chaque donnée ou document ?				
b) Heeft het ESS procedures uitgewerkt om de verwijdering en/of anonimisering van documenten en data te garanderen?	b) Le SSA a-t-il mis des procédures au point permettant de garantir la suppression et/ou l'anonymisation de documents et de données ?				
c) Leeft het ESS de bewaartermijnen na, zoals bepaald in de richtlijnen?	c) Le SSA respecte-t-il les délais de conservation mentionnés dans le code de conduite ?				
d) Laat het ESS de klant toe om een specifieke aanvraag te doen tot het verwijderen of anonimiseren van gegevens?	d) Le SSA autorise-t-il le client à formuler une demande de suppression ou d'anonymisation personnalisée ?				

10. Verantwoordelijke voor de gegevensbescherming		10. Responsable à la protection des données					
a) Heeft het ESS een DPO (Data Protection Officer) of een verantwoordelijke voor de gegevensbescherming aangesteld?		a) Le SSA a-t-il nommé un DPO ou un responsable à la protection des données ?					
b) Werden de contactgegevens van de verantwoordelijke voor de gegevensbescherming bekendgemaakt?		b) Les coordonnées du responsable à la protection des données sont-elles publiées ?					
11. Datalekken		11. Fuite de données					
a) Heeft het ESS een meldingsprocedure bepaald om de verwerkingsverantwoordelijke te informeren ingeval van datalek.		a) Le SSA a-t-il une procédure pour informer le responsable du traitement d'une fuite de données ?					
b) Heeft het ESS een werkwijze uitgewerkt met het oog op het beheer van datalekken?		b) Le SSA a-t-il mis en place une méthode pour gérer les fuites de données ?					
c) Stelt het ESS een register op waarbij alle datalekken worden geregistreerd?		c) Le SSA recense-t-il toutes les fuites de données ?					
d) Is het ESS bereid bijstand te verlenen aan de klant bij een datalek?		d) Le SSA est-il disposé à offrir du support au client en cas de fuite de données ?					
12. Informatiebeveiliging – Technische en organisatorische maatregelen		12. Sécurité informatique - Mesures techniques et organisationnelles					
12.1. Beveiligingsbeleid en organisatie van informatiebeveiliging		12.1. Politique de sécurité et organisation de la sécurité de l'information					
a) Heeft het ESS een algemeen gegevensbeschermingsbeleid geïmplementeerd?		a) Le SSA a-t-il mis en place une politique générale de protection des données ?					
b) Wordt het gegevensbeschermingsbeleid regelmatig beoordeeld door het ESS?		b) Le SSA effectue-t-il des contrôles réguliers sur le respect de la politique de protection des données ?					

12.2. Veilig personeelsbeleid	12.2. Sécurité des ressources humaines				
a) Neemt het ESS een vertrouwelijkheidsclausule op in de arbeidsovereenkomsten?	a) Le SSA incorpore-t-il dans les contrats de travail des clauses de confidentialité ?				
b) Maakt het ESS haar medewerkers bewust van haar verplichtingen m.b.t. gegevensbescherming?	b) Le SSA fait-il prendre conscience à ses collaborateurs de ses obligations en matière de protection des données ?				
c) Worden de toegangsrechten van medewerkers tijdig ingetrokken als de arbeidsovereenkomst eindigt ?	c) Les droits d'accès sont-ils bien retirés à temps lors de la fin d'un contrat de travail au sein du SSA ?				
12.3. Beheer van de bedrijfsmiddelen	12.3. Gestion des biens économiques				
a) Beschikt het ESS over een inventaris van IT middelen en media?	a) Un inventaire des biens IT existe-t-il au sein du SSA ?				
b) Zijn er regels verbonden aan het gebruik van de bedrijfsmiddelen?	b) Existe-t-il des règles pour l'utilisation des biens économiques ?				
c) Recupereert het ESS haar middelen bij contractafloop?	c) Le SSA récupère-t-il ses outils de travail lors de la fin du contrat ?				
12.4. Toegangscontrole	12.4. Contrôle d'accès				
a) Beschikt het ESS over een autorisatiebeheersysteem dat de toegang tot de informatiesystemen van het ESS controleert?	a) Le SSA dispose-t-il d'un système de gestion des autorisations qui contrôle l'accès aux systèmes d'information du SSA ?				
b) Heeft elk individu die toegang heeft tot systemen die klantengegevens bevatten, een aparte, unieke ID/gebruikersnaam?	b) Chaque individu qui a accès aux systèmes qui contiennent des données des clients a-t-il un ID/nom d'utilisateur individuel et unique ?				
c) Zijn de gebruikte wachtwoorden ten minste acht tekens lang?	c) Les mots de passe utilisés comptent-ils au moins 8 caractères ?				
d) Wordt de toegang tot persoonsgegevens beperkt op basis van de functie?	d) L'accès aux données est-il limité par profil ?				
e) Wordt de toegang tot het netwerk op gepaste wijze beschermd (bv. via firewalls, security appliances)?	e) L'accès au réseau est-il protégé de façon adéquate (p. ex. via firewalls, security appliances) ?				
12.5. Cryptografie	12.5. Cryptographie				
a) Gebruikt het ESS erkende cryptografische standaarden als het persoonsgegevens versleutelt?	a) Le SSA utilise-t-il des standards cryptographiques reconnus lorsqu'il crypte des données personnelles ?				

12.6. Fysieke beveiliging en beveiliging van de omgeving	12.6. Sécurité physique et sécurisation de l'environnement				
a) Beperkt het ESS toegang tot zijn gebouwen tot bevoegde medewerkers?	a) Le SSA limite-t-il l'accès à ses bâtiments aux collaborateurs compétents ?				
b) Bestaat er een formele procedure m.b.t. de toegang tot de datacenters en wordt toegang periodiek beoordeeld?	b) Existe-t-il une procédure formelle concernant l'accès aux centres de données et cet accès fait-il l'objet d'une évaluation périodique ?				
c) Zijn de datacenters beveiligd tegen stroomuitval/brand om beschikbaarheid van gegevens te garanderen?	c) Les centres de données sont-ils protégés contre les pannes de courant et les incendies afin de garantir la disponibilité des données ?				
12.7. Operationele beveiliging	12.7. Sécurité opérationnelle				
a) Zorgt het ESS voor back-ups van zijn data?	a) Le SSA organise-t-il des back-ups de ses données ?				
b) Bewaart het ESS kopieën van klantengegevens en gegevensherstelprocedures op een andere plaats dan waar de primaire computerapparatuur die de klantengegevens verwerkt, zich bevindt?	b) Le SSA conserve-t-il des copies des données des clients et des procédures de réparation des données à un autre endroit qu'à l'endroit du serveur primaire qui traite les données des clients ?				
c) Registreert het ESS de toegang tot en het gebruik van zijn informatiesystemen die klantendata bevatten in een logboek?	c) Le SSA consigne-t-il dans un journal l'accès à et l'utilisation de ses systèmes d'information qui contiennent des données des clients ?				
d) Beschikt het ESS over anti-malwarecontroles om te helpen voorkomen dat kwaadaardige software ongeautoriseerde toegang tot klantengegevens krijgt?	d) Le SSA dispose-t-il de contrôles anti-malware pour permettre d'éviter qu'un software malin ait un accès non autorisé aux données des clients ?				
e) Worden de updates inzake beveiliging opgevolgd en geïnstalleerd?	e) Les mises à jour relatives à la sécurité sont-elles suivies et installées ?				
12.8. Communicatiebeveiliging	12.8. Sécurité des communications				
a) Versleutelt het ESS alle klantengegevens die worden verzonden via publieke, niet-vertrouwde netwerken?	a) Le SSA sécurise-t-il toutes les données des clients qui sont envoyées via des réseaux publics non sécurisés ?				

12.9. Verwerving, ontwikkeling en onderhoud van informatiesystemen		12.9. Acquisition, développement et entretien des systèmes informatiques					
a) Worden de vereisten voor gegevensbescherming geanalyseerd en geïmplementeerd bij de start van een ontwikkeling (Security and Privacy by design)?		a) Les exigences en matière de protection des données sont-elles analysées et implémentées dès le début d'un développement (Security and Privacy by Design) ?					
b) Worden toegangsrechten tot productie beperkt tot enkel de medewerkers van de ESS die in het kader van hun functie toegang nodig hebben tot de productieomgeving die een scheiding tussen ontwikkeling en productie waarborgt?		b) Les droits d'accès à la production sont-ils limités uniquement aux collaborateurs des SSA qui, dans le cadre de leur fonction, ont besoin d'un accès à l'environnement de production qui garantit une séparation entre le développement et la production ?					
c) Heeft het ESS een proces om ervoor te zorgen dat wijzigingen in operationele systemen en toepassingen plaatsvinden op een gecontroleerde wijze?		c) Le SSA dispose-t-il d'un processus pour veiller à ce que des modifications dans des systèmes opérationnels et des applications se fassent de manière contrôlée ?					
12.10. Leveranciersrelaties		12.10. Relations avec les fournisseurs					
a) Worden de beveiliging en privacy praktijken van een leverancier/partner met betrekking tot gegevensverwerking geëvalueerd bij de selectie van leveranciers?		a) La sécurisation et les pratiques en matière de vie privée d'un fournisseur/partenaire concernant le traitement des données sont-elles évaluées lors de la sélection des fournisseurs ?					
b) Worden verplichtingen inzake gegevensbescherming formeel opgenomen in leverancierscontracten?		b) Les obligations en matière de protection des données sont-elles reprises formellement dans les contrats avec les fournisseurs ?					
12.11. Beheer van informatiebeveiligingsincidenten		12.11. Gestion des incidents liés à la sécurité de l'information					
a) Werden meldingsprocedures ingevoerd voor de kennisgeving van incidenten aan klanten?		a) Les procédures de communication des incidents envers les clients sont-elles en place ?					

12.12. Bedrijfscontinuïteit	12.12. Continuité de l'entreprise				
a) Bestaat er een Disaster Recovery Plan (herstellingsplannen) voor de datacentra waarin zich informatiesystemen van het ESS bevinden die klantengegevens verwerken?	a) Existe-t-il un plan de Disaster Recovery pour les centres de données dans lesquels se trouvent des systèmes d'information du SSA qui traitent des données des clients ?				
b) Beschikt het ESS over procedures voor het herstellen van klantengegevens in hun laatst geback-upte staat voor het tijdstip waarop ze verloren gegaan zijn of vernietigd werden?	b) Le SSA dispose-t-il de procédures afin de rétablir les données des clients dans leur dernière version sauvegardée au cas où celles-ci seraient perdues ou détruites ?				
12.13. Naleving	12.13 Respect				
a) Wordt de naleving van informatiebeveiligingscontroles op periodieke basis geëvalueerd?	a) Le respect des contrôles de sécurisation des informations est-il évalué de manière périodique ?				
13. Rechten van de betrokkene	13. Droits de la personne concernée				
a) Heeft het ESS procedures uitgewerkt met het oog op de naleving van de rechten van de betrokkene?	a) Le SSA a-t-il mis en place des procédures pour respecter les droits de la personne concernée ?				
b) Is het ESS in staat binnen 14 kalenderdagen op de vraag van een klant betreffende de uitoefening van de rechten van de betrokkene te reageren?	b) Le SSA peut-il répondre dans les 14 jours calendrier à la demande d'un client concernant les droits de la personne concernée ?				
c) Garandeert het ESS redelijke bijstand aan haar klant/werkgever om de werkgever toe te laten adequaat te antwoorden op vragen van betrokkenen?	c) Le SSA garantit-il une assistance convenable à son client/employeur afin de permettre à l'employeur de répondre de manière adéquate aux questions des intéressés ?				