Richtlijnen voor de toepassing van de GDPR bij de sociale secretariaten

1. Definities

1.1. Definities die in de GDPR gehanteerd worden zijn in bijlage 1 opgenomen.

1.2. ESS: Erkend Sociaal Secretariaat

1.3. GDPR: General Data Protection Regulation. In het Nederlands afgekort als AVG (Algemene Verordening Gegevensbescherming).

1.4. GBA: Gegevensbeschermingsautoriteit, de toezichthoudende autoriteit op de bescherming van persoonsgegevens binnen België.

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.

1.6. USS: Unie Sociale Secretariaten

2. Inleiding

2.1. 90 % van de werkgevers in de privésector in België doet een 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 richtlijnen 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. Deze richtlijnen definiëren een kader waarbinnen gegarandeerd kan worden dat persoonsgegevens van werknemers van de klanten van de sociale secretariaten op een uniforme manier worden verwerkt en aan dezelfde strikte beschermingsmaatregelen voldoen.

2.2. De sectorale richtlijnen (verder 'richtlijnen) voor de verwerking van persoonsgegevens onder de GDPR lijsten op bevattelijke wijze de krachtlijnen van het door de USS gevoerde informatiebeschermingsbeleid op.

2.3. Dit document:

- bevat richtlijnen over 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.

3. Toepassingsgebied

De richtlijnen zijn van toepassing op het ESS dat in België erkend en gevestigd is voor de uitvoering van haar kerntaken in België.
De richtlijnen zijn 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
- 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 richtlijnen.

4. Relatie ESS – klant/werkgever

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.

5. Gegevensbeschermings-effectbeoordeling

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).

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 richtlijnen).

6. Register van verwerkingsactiviteiten

Het ESS houdt conform artikel 30.2 van de GDPR een intern register van verwerkingsactiviteiten bij.

7. Subverwerkers

Het ESS, dat een 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.

Het ESS beschouwt de volgende derden niet als haar subverwerkers, ondanks het feit dat deze partijen persoonsgegevens vanuit het ESS ontvangen:

- 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.

8. Doorgifte aan derden van persoonsgegevens

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 een online tool).

9. Bewaartermijnen

9.1. <u>Bewaartermijnen voor de klant/werkgever, als verwerkingsverantwoordelijke, voor het bewaren van documenten waar voor de klant/werkgever 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. Bewaartermijnen voor het ESS, als verwerker, voor het bewaren van de documenten waar voor het ESS een wettelijke verplichting tot bewaren op rust:

Het ESS bewaart de documenten vermeld in bijlage 2.2, die ze effectief verwerken 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.

9.3. Dataretentiebeleid

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.

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

10. Verantwoordelijke gegevensbescherming

Het ESS engageert zich om een verantwoordelijke aan te duiden voor de gegevensbescherming en het naleven van deze richtlijnen. Deze verantwoordelijke is 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 data protection 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 richtlijnen en de vragenlijst voor de zelfevaluatie uit te voeren.

11. Datalekken

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.

12. Informatiebeveiliging – Technische en organisatorische maatregelen

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.

13. Rechten van de betrokkene

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.

14. Naleving van de richtlijnen

Het ESS doet een jaarlijkse zelfevaluatie van de toepassing van de richtlijnen op basis van een vragenlijst, opgenomen in bijlage 4 en bevestigt schriftelijk op basis van deze zelfevaluatie aan de USS dat ze de richtlijnen heeft nageleefd.

Bij problemen van niet naleving van deze richtlijnen, zal de USS dit melden aan het betrokken ESS.

Bijlage 1: begripsbepalingen

In deze richtlijnen 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 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;

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;

Betrokkene: een geïdentificeerde of identificeerbare natuurlijke persoon

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;

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de 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;

Functionaris Gegevensbescherming:
De functionaris voor gegevensbescherming ziet toe op de gegevensverwerkingen binnen de organisatie.

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;

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)

Bijlage 2: Wettelijke bewaartermijnen voor de categorieën van verwerkte persoonsgegevens voor het uitvoeren van de kerntaken:

2.1. Wettelijke verplichtingen voor de klant/werkgever:

Het ESS bewaart de volgende documenten minimaal gedurende de volgende bewaartermijnen:

- algemene gegevens:
  - de vaste gegevens werknemer (identificatiegegevens, adres, bruto loon, enz.): 5 jaar
  - de opgave lonen en prestaties: 5 jaar
  - alle briefwisseling tussen de klant/werkgever en het ESS die persoonsgegevens bevat: 5 jaar

- loonberekeningen:
  - de berekende gegevens van de werknemer (detail loonberekening): 5 jaar
  - de loonbrief: 5 jaar
  - de individuele rekening: 5 jaar
  - de boekhouddocumenten lonen: 7 jaar

- bijhorende documenten bij de loonberekening:
  - het bedrijfswagenattest: 5 jaar
  - het algemeen personeelsregister: 5 jaar
  - de documenten loonbeslag: 5 jaar
  - de documenten loonoverdracht: 5 jaar
  - de documenten loondelegatie: 5 jaar
  - de documenten bij het einde van de arbeidsovereenkomst (het tewerkstellingsattest, het vakantie-attest,…): 5 jaar
  - de fiscale fiches 281.XX: 7 jaar
  - de sociale balans: 7 jaar

- aangiftes aan de Overheid en andere derde partijen:
  - de DMFA kwartaalaangifte: 3 jaar
  - de aangiftes fondsen voor bestaanszekerheid: 3 jaar
  - de Dimona aangifte: 5 jaar
  - de Aangifte Sociaal Risico werkloosheid: 5 jaar
  - de Aangifte Sociaal Risico ziekte: 5 jaar
  - de aangifte bedrijfsvoorheffing: 7 jaar

2.2. Specifieke wettelijke verplichting voor het ESS:

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.

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:

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 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:

- 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,..)

Bijlage 3: Informatiebeveiliging – Technische en organisatorische maatregelen

Het ESS heeft de nodige beveiligingsmaatregelen geïmplementeerd om persoonsgegevens te beschermen. Hieronder volgt een overzicht van de belangrijkste maatregelen die het ESS minimaal garandeert.

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.

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.

Beëindiging. Toegangsrechten worden bij beëindiging van de samenwerking tijdig ingetrokken, in overeenstemming met de beveiligingsadministratieprocedures.

3. **Domein:**

Beheer van bedrijfsmiddelen

Praktijken:

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

4. **Domein:**

Toegangscontrole

Praktijken:

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 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.

5. **Domein:**

Cryptografie

Praktijken:

Versleuteling van vertrouwelijke data gebeurt aan de hand van erkende cryptografische standaarden (bv Transport Layer Security).

6. **Domein:**

Fysieke beveiliging en beveiliging van de omgeving

Praktijken:

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.

7. **Domein:**

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.

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.

9. Domein:

Verwerving, ontwikkeling en onderhoud van informatiesystemen

Praktijken:

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.

10. Domein:

Leveranciersrelaties

Praktijken:

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.

11. **Domein:**

Beheer van informatiebeveiligings-incidenten

Praktijken:

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.

12. **Domein:**

Bedrijfscontinuïteit

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.

13. **Domein:**

Naleving

Praktijken:

Beveiligingsevaluaties. De naleving van informatiebeveiligingscontroles wordt op periodieke basis geëvalueerd.

Bijlage 4: Vragenlijst voor jaarlijkse evaluatie naleving richtlijnen
Zie WORD document