BELEIDSDOCUMENT

Beleid voor Gegevensbescherming

(Vastgesteld door de RvB Careyn d.d. 16 oktober 2019)

Inhoudsopgave

1. Inleiding

Careyn is een organisatie voor thuiszorg, verpleging en verzorging en wil samen met anderen bijdragen aan een inclusieve, solidaire en duurzame samenleving door verbindingen te leggen en ondersteuning te bieden, voor iedereen die op enig moment in het leven –tijdelijk- een verminderd vermogen ervaart om ‘een thuis’ te creëren.

In het kader van deze maatschappelijke verantwoordelijkheid is een verantwoord privacy beleid van cruciaal belang. Betrokkenen moeten kunnen vertrouwen op een zorgvuldige verwerking van persoonsgegevens en afdoende beveiliging tegen verlies of onrechtmatige verwerking. Organisatie brede aanpak van verwerking en beveiliging van persoonsgegevens is noodzakelijk.

De bescherming van persoonsgegevens wordt in toenemende mate complexer door de snelle technologische ontwikkelingen en strikte (Europese) wetgeving op het gebied van privacy en beveiliging.

Transparantie over de wijze waarop Careyn omgaat met persoonsgegevens én het waarborgen van de privacy is belangrijk voor cliënten en organisatie ter voorkoming van onnodige risico’s; zoals inbreuk op de cliëntveiligheid, financiële schade, juridische gevolgen en imago verlies.

Ter voorkoming van genoemde risico’s treft Careyn in dit beleidsdocument maatregelen op het gebied van informatiebeveiliging, dataminimalisatie en transparantie.

2. Beleid voor Gegevensbescherming

2.1: Doelstelling

Het opstellen van het Gegevensbeschermingsbeleid heeft ten doel het vaststellen van algemene kaders voor zorgvuldig en verantwoord omgaan met persoonsgegevens, het respecteren van de privacy van medewerkers, cliënten en andere betrokkenen, het mitigeren van risico's en het proactief naleven van relevante wet- en regelgeving betreffende privacy.

2.2: Wet- en regelgeving

Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).
In de Algemene Verordening Gegevensbescherming (AVG) zijn regels gesteld over de wijze waarop persoonsgegevens mogen worden verwerkt. De Verordening is vanaf 25 mei 2016 in werking getreden en vanaf 25 mei 2018 rechtstreeks toepasselijk in de Europese Unie. Hiermee vervangt zij vanaf laatstgenoemde datum de Wet bescherming persoonsgegevens (Wbp). De Verordening ziet toe op een versterking en uitbreiding van privacy rechten en een uitbreiding van verantwoordelijkheden voor organisaties.
De Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) regelt met name de rol en positie van de Autoriteit Persoonsgegevens, het gebruik van bijzondere categorieën van persoonsgegevens zoals gegevens betreffende gezondheid en persoon identificerende gegevens, zoals het Burgerservicenummer.

NEN7510
Nederlandse zorginstellingen zijn verplicht te voldoen aan de NEN7510. De NEN7510 is een Nederlandse zorg specifieke norm op het gebied van informatiebeveiliging, afgeleid van de IEC/ISO 27001. De norm geeft invulling aan een deel van de bepalingen uit de Verordening en vormt het kader voor het toezicht op informatiebeveiliging door de Autoriteit Persoonsgegevens (AP).

2.3: Begrippen

Careyn hanteert in het kader van dit Gegevensbeschermingsbeleid en bij verwerking van persoonsgegevens dezelfde begripsbepalingen zoals vastgelegd in de Verordening dan wel in overige van toepassing zijnde wet- of regelgeving. [1]

2.4: Toepassingsgebied

Het Gegevensbeschermingsbeleid heeft betrekking op alle taken en processen waarbij persoonsgegevens worden verwerkt en waarvoor Careyn verantwoordelijk is. Het is van toepassing op de gehele organisatie, dat wil zeggen op alle onderdelen van Careyn. Het is ook van toepassing op de gegevensuitwisseling van Careyn met andere organisaties. Het

[1] Art. 4 AVG (Definities)

beleid richt zich op eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan Careyn.

3. Beleidsuitgangspunten en -beginselen

3.1 Uitgangspunten

Careyn gaat behoorlijk en zorgvuldig om met persoonsgegevens zodat de rechten worden gewaarborgd van personen waarvan gegevens worden verwerkt.

Het Gegevensbeschermingsbeleid is gebaseerd op de volgende beleidsuitgangspunten:

- Careyn voldoet aan bestaande wet- en regelgeving op het gebied van gegevensbescherming.
  Dit omvat in ieder geval de Algemene Wet Gegevensbescherming (AVG) en de NEN7510 normering. Indien extra maatregelen nodig blijken vanuit de risicoanalyse worden deze genomen.
- De volgende wetten, in relatie tot de gegevensbescherming, worden door Careyn in acht genomen:
  - ✓ Wet Geneeskundige Behandelingsovereenkomst (WGBO);
  - ✓ Wet Beroepen in de Individuele Gezondheidszorg (Wet BIG);
  - ✓ Wet kwaliteit, klachten en geschillen zorg (Wkkgz);
  - ✓ Wet Meldplicht Datalekken;
  - ✓ Zorgverzekeringswet (Zvw);
  - ✓ Wet marktordening gezondheidszorg (Wmg);
  - ✓ Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg;
  - ✓ Wet gebruik Burgerservicenummer in de zorg
- Careyn hecht grote waarde aan rechtmatige, behoorlijke, transparante en daarmee kwalitatieve verwerking van persoonsgegevens. Op deze wijze biedt Careyn vertrouwen aan cliënten, medewerkers en andere betrokkenen in de wijze waarop wordt omgegaan met persoonsgegevens en privacy.
- Careyn werkt mee aan technologische ontwikkelingen, innovatie en globalisering op het gebied van gegevensbescherming.
- Careyn hanteert duidelijke richtlijnen hoe zij omgaat met de verwerking van en het toezicht op persoonsgegevens.
- Maatregelen en procedures om privacy te waarborgen gaan voor op individuele wensen, plannen en handelswijzen van medewerkers om over gegevens te beschikken.
- Careyn handelt klachten van cliënten, werknemers en andere betrokkenen over privacyaspecten af op een toegankelijke, laagdrempelige en begrijpelijke wijze.
- Careyn besteedt bij indiensttreding, doorstroming en uitdiensttreding van medewerkers nadrukkelijk aandacht aan het toekennen en verwijderen van rechten op de verschillende systemen van Careyn.
- Naleving van de privacywetgeving is de verantwoordelijkheid van iedereen. Van managers, behandelaars, verpleegkundigen, verzorgenden, overige medewerkers en ingeschakelde derden wordt verwacht dat zij actief bijdragen aan bevorderen van een veilige verwerking van persoonsgegevens. Hiertoe heeft Careyn een e-learning programma ontwikkeld voor medewerkers op Intranet.

3.2 Beginselen

Iedere verwerking van persoonsgegevens moet voldoen aan de in deze paragraaf te benoemen beginselen. Deze verwerkingsbeginselen vormen het normatieve kader van het Gegevensbeschermingsbeleid. Zij worden nader geconcretiseerd in de rechten die betrokkenen hebben ten aanzien van de verwerking van hun persoonsgegevens en in de verplichtingen die Careyn heeft om deze gegevensverwerkingen zorgvuldig en naar behoren uit te voeren, zodat zij kan voldoen aan de Verordening.

3.1.1 Rechtmatigheid, behoorlijkheid en transparantie

Careyn zorgt dat haar procedures voor het verwerken van gegevens conform de wet worden uitgevoerd en dat niets wordt verborgen van betrokkenen. Uitgangspunt is dat persoonsgegevens alleen worden verwerkt voor gerechtvaardigde doeleinden. Careyn maakt duidelijk dat een verwerking noodzakelijk is met het oog op het bereiken van specifiek in de Verordening genoemde doelen, dan wel door middel van verkregen toestemming. Deze duidelijkheid wordt onder meer door Careyn verschaft middels het op haar website gepubliceerde Privacy Statement.

3.1.2 Doelbinding

Careyn zorgt dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen wordt verzameld en verwerkt. Persoonsgegevens worden zodra dit doel is bereikt niet verder verwerkt. Wanneer gegevens later voor een ander doel worden gebruikt, is dit doel verenigbaar met het oorspronkelijke verzameldoel.

3.1.3 Dataminimalisatie

Careyn gebruikt bij het verzamelen en verwerken van persoonsgegevens niet meer gegevens dan nodig is om het doel waarvoor ze gebruikt zullen worden te bereiken. Voor zover mogelijk zal Careyn minder of geen persoonsgegevens verwerken.

3.1.4 Juistheid

Careyn ziet toe dat de persoonsgegevens juist en actueel zijn. Om dit te bewerkstelligen neemt Careyn alle redelijke maatregelen om ervoor te zorgen dat gegevens die dit niet (meer) zijn worden gerectificeerd, dan wel worden gewist.

3.1.5 Opslagbeperking

Careyn verwijdert persoonsgegevens in identificeerbare vorm zodra deze niet langer nodig zijn voor het oorspronkelijke doel waarvoor ze zijn verzameld.

3.1.6 Integriteit en vertrouwelijkheid

Careyn behandelt persoonsgegevens vertrouwelijk. Persoonsgegevens worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Persoonsgegevens worden alleen verwerkt door personen die daartoe zijn geautoriseerd en slechts binnen het doel waarvoor deze zijn verwerkt. Toegang tot informatie, informatiesystemen en het bedrijfsnetwerk wordt bepaald op basis van “need to know”. Clientinformatie is in principe alleen toegankelijk wanneer hieraan een behandel- of zorgrelatie ten grondslag ligt.

Daarnaast zijn organisatorische en technische maatregelen getroffen, die waarborgen dat persoonsgegevens passend worden beveiligd en beschermd tegen ongeoorloofde en onrechtmatige verwerking, opzettelijk verlies, vernietiging of beschadiging. Meer informatie hieromtrent is vastgelegd in paragraaf 8.2.

4. Borging in de organisatie

4.1 Rollen en bevoegdheden, taken en verantwoordelijkheden

Verwerkingsverantwoordelijke (Raad van Bestuur)	**Rol/bevoegdheid:** • Eindverantwoordelijke voor de rechtmatige en zorgvuldige omgang met persoonsgegevens. • Functionele aansturing van de Functionaris Gegevensbescherming voor de realisatie van gegevensbescherming binnen Careyn en het creëren van randvoorwaarden voor de implementatie, uitvoering en borging van het Gegevensbeschermingsbeleid. • Fungeert als escalatie-orgaan voor de Functionaris Gegevensbescherming. • Stimulerend en sturend in de naleving van het Gegevensbeschermingsbeleid door directeuren, managers, medewerkers en overig personeel. **Taken:** • Beoordeling en vaststelling van het Gegevensbeschermingsbeleid. • Regulier overleg (elk half jaar) met Functionaris Gegevensbescherming over voortgang, ontwikkelingen en risico's in de plan-do-check-act cyclus van het informatieveiligheidsbeleid en het informatieverwerkingsbeleid. **Verantwoordelijkheden:** • Eindverantwoordelijk voor vaststellen van Gegevensbeschermingsbeleid. • Eindverantwoordelijk voor uitvoering en naleving van Gegevensbeschermingsbeleid. • Verantwoordelijk voor het vaststellen van het doel en de middelen voor de verwerking van de persoonsgegevens. • Verantwoordelijk voor nemen van passende en effectieve maatregelen zodat verwerkingen conform de Verordening plaatsvinden. • Verantwoordelijk voor uitvoering van een Gegevensbeschermingseffectbeoordeling. • Verantwoordelijk voor het bijhouden van een Register van de verwerkingsactiviteiten die plaatsvinden. • Verantwoordelijk voor aanstellen van Privacy Officer en Security Officer.
Functionaris gegevens-	**Rol/bevoegdheid** • Betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

bescherming	• Rol van ‘bemiddelaar’. • Adviseert en begeleidt Careyn ten aanzien van de informatieveiligheid en privacy. • Faciliterend naar de Privacy Officer in het creëren van randvoorwaarden voor de implementatie, uitvoering en borging van het Gegevensbeschermingsbeleid. • Faciliterend naar de Security Officer in het creëren van randvoorwaarden voor de implementatie, uitvoering en borging van het Gegevensbeschermingsbeleid. • Functionele aansturing van de Privacy Officer voor de realisatie van gegevensbescherming binnen Careyn. • Functionele aansturing van de Security Officer voor de realisatie van gegevensbeveiliging binnen Careyn • Fungeert als escalatie-orgaan voor de Privacy Officer en de Security Officer • Bedenken, ontwikkelen en implementeren van nieuwe maatregelen in overleg met Privacy Officer en Security Officer. **Taken:** • Controle houden op de naleving van de algemene verordening gegevensbescherming. • Informatie verzamelen om verwerkingsactiviteiten te identificeren. • Toezien op de naleving van verwerkingsactiviteiten. • Toezien op de naleving van het gegevensbeschermingsbeleid met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel. • (Gevraagd en ongevraagd) adviseren van de verwerkingsverantwoordelijke bij de uitvoering van een gegevensbeschermingseffectbeoordeling. • Extern fungeren als aanspreekpunt op het gebied van gegevensbeveiliging. • Samenwerken met de Autoriteit Persoonsgegevens en handelen als contactpunt voor de toegang tot alle documenten en informatie over de uitvoering van de taken. • Opmaken van inventarissen en het bijhouden van een register van de verwerkingsactiviteiten op basis van informatie die hem wordt verleend door de diverse afdelingen binnen Careyn die voor de verwerking van persoonsgegevens instaan. • Regulier overleg (elk half jaar) met Privacy Officer en Security Officer over voortgang, ontwikkelingen en risico’s in de plan-do-check-act cyclus van het informatieveiligheidsbeleid en het informatieverwerkingsbeleid. • Overleg met Privacy Officer bij constatering van incidenten in relatie tot gegevensverwerking.

	• Overleg met Security Officer bij constatering van incidenten in relatie tot gegevensbeveiliging. **Verantwoordelijkheden:** • Aansturen van medewerkers in de naleving van informatieveiligheidsbeleid en informatieverwerkingsbeleid. • Verantwoordelijk voor het stimuleren van een risicogebaseerde aanpak. • Signaleren van tekortkomingen in de naleving van de AVG, initiatief nemen om gedragsverandering bij medewerkers te stimuleren in afstemming met betreffende leidinggevende. • Signaleren van tekortkomingen in de naleving van het Gegevensbeschermingsbeleid, rapporteren aan de Verwerkingsverantwoordelijke en adviseren over verbeteringen. • Kennis nemen en uitdragen van het stelsel van maatregelen welke van kracht zijn binnen Careyn voor informatieveiligheid en informatieverwerking.
Security Officer (SO)	**Rol/bevoegdheid:** • Hiërarchisch werkzaam en rapporterend aan de directeur bedrijfsvoering. • Werkt nauw samen met de Privacy Officer. • Werkt nauw samen met afdeling Kwaliteit, Informatie management, ICT voor ICT beveiliging en Control. • Werkt nauw samen met afdeling Marketing & Communicatie voor bewustwording en activeren van gedrag van medewerkers in relatie tot informatieverwerking. • Werkt nauw samen met afdeling HR voor in-door-uitstroom proces van medewerkers. • Werkt nauw samen met afdeling Juridische Zaken voor controle en afstemming wet- en regelgeving. • Adviseert en begeleidt Careyn ten aanzien van de informatieveiligheid. **Taken:** • Uitvoeren van (minimaal) jaarlijkse (interne) audit en rapportage verwerken in Plan voor Informatieverwerking. • Ontwikkelen strategisch beleid op het gebied van informatiebeveiliging. • Opstellen en actualiseren van Maatregelen, Instructies en Afspraken voor de implementatie van Informatiebeveiligingsbeleid. • Toezien op het actueel blijven van het verwerkingsregister. • Bedenken, ontwikkelen en implementeren van nieuwe maatregelen in overleg met de verwerkingsverantwoordelijke om gewenste niveau van

	informatieverwerking te bereiken. • Rapporteren van overtredingen, c.q. datalekken. • Rapporteren van overtredingen op het Informatieveiligheidsbeleid aan verwerkingsverantwoordelijke om gewenste niveau van informatieveiligheid te bereiken. • Een adviserende rol richting de Privacy Officer met betrekking tot sancties die opgelegd worden aan de betrokken medewerker bij overtredingen. • Rapporteren aan RvB over overtredingen, waartoe Careyn bij wet- en regelgeving verplicht is. • Regulier overleg (elk half jaar) met portefeuillehouder Raad van Bestuur over voortgang, ontwikkelingen en risico's in de plan-do-check-act cyclus van het informatieverwerkingsbeleid. • Regulier overleg met de Privacy Officer en de Functionaris Gegevensbescherming • Overleg met portefeuillehouder Raad van Bestuur bij constatering van incidenten in relatie tot informatieverwerking. **Verantwoordelijkheden:** • Aansturing van Managers en medewerkers in de naleving van informatieverwerkingsbeleid. • Kennis nemen van de juiste wet- en regelgeving die van toepassing is op Careyn. • Signaleren en rapporteren van mogelijke risico's van informatieverwerking.
Privacy Officer (PO)	**Rol/bevoegdheden:** • Hiërarchisch werkzaam en rapporterend aan de Functionaris Gegevensbescherming (FG) en de Verwerkingsverantwoordelijke. • Werkt nauw samen met de Security Officer. • Werkt nauw samen met afdeling Privacy. • Werkt nauw samen met afdeling HR voor in-door-uitstroom proces van medewerkers. • Werkt nauw samen met de afdeling Kwaliteit, Informatie management, ICT en Control. • Werkt nauw samen met afdeling Marketing & Communicatie voor bewustwording en activering van gedrag van medewerkers in relatie tot gegevensbescherming. • Werkt nauw samen met afdeling Juridische Zaken voor controle en afstemming wet- en regelgeving. • Adviseert en begeleidt Careyn t.a.v. de informatieverwerking en Privacy. **Taken:**

- Analyseren en controleren van naleving van de Algemene Verordening Gegevensbescherming (AVG)
- Opstellen en actualiseren van Gegevensbeschermingsbeleid.
- Opstellen en actualiseren Verwerkersovereenkomsten.
- Inrichten en toezien op actueel blijven van Verwerkingsregister.
- Opstellen, implementeren en actualiseren Procedure datalekken.
- Opstellen, implementeren en actualiseren Procedure rechten betrokkenen.
- Uitvoeren van Gegevensbeschermingseffectbeoordeling (DPIA).
- Uitvoeren van (minimaal) jaarlijkse (interne) audit en rapportage verwerken.
- Opstellen en actualiseren van Maatregelen, Instructies en Afspraken voor de implementatie van Gegevensbeschermingsbeleid.
- Bedenken, ontwikkelen en implementeren van nieuwe maatregelen in overleg met Managers om gewenste niveau van gegevensbescherming te bereiken.
- Rapporteren van overtredingen op het gegevensbeschermingsbeleid aan betreffende Manager, Concernmanager ICT en portefeuillehouder Raad van Bestuur.
- Sancties opleggen bij overtredingen, in overleg met direct leidinggevende van betrokken medewerker.
- In samenspraak met Verwerkingsverantwoordelijke bepalen of er een melding gedaan moet worden aan autoriteiten dan wel betrokkene (in het geval van Meldplicht datalekken).
- Melding aan autoriteit persoonsgegevens uitvoeren in geval van een Datalek.
- Rapporteren maandelijks over de status van Privacy aan Functionaris Gegevensbescherming (FG) die vervolgens rapporteert aan de Verwerkingsverantwoordelijke van Careyn.
- Regulier overleg (elk half jaar) met Verwerkingsverantwoordelijke over voortgang, ontwikkelingen en risico's in het Beleid.
- Overleg met Functionaris Gegevensbescherming bij constatering van incidenten in relatie tot informatieveiligheid.
- Regulier overleg met Security Officer en Functionaris Gegevensbescherming.

Verantwoordelijkheden:

- Aansturing van managers en medewerkers in de naleving van Gegevensbeschermingsbeleid.
- Toezien op aantoonbare naleving van de in artikel 5 van de Verordening genoemde eisen.
- Signaleren mogelijke risico's bij privacy-incidenten.
- Bewaken balans tussen belang van privacy en uitvoerbaarheid van maatregelen binnen de organisatie.

	• Toezien op de omgang met persoonsgegevens binnen organisatie en controleren of organisatie voldoet aan de Verordening. • Trainen van personeel en bijstaan bij vragen over privacy en persoonsgegevens.

5. Persoonsgegevensverwerkingen binnen Careyn

5.1 Omschrijving (categorieën persoonsgegevens)

Binnen Careyn zijn er vijf verwerkingsactiviteiten te onderscheiden:

- Verwerking van gewone persoonsgegevens van cliënten;
- Verwerking van bijzondere persoonsgegevens van cliënten;
- Verwerking van gewone persoonsgegevens van medewerkers;
- Verwerking van bijzondere persoonsgegevens van medewerkers;

5.1.1 Verwerking van gewone persoonsgegevens van cliënten

Careyn verzamelt de volgende gewone persoonsgegevens van cliënten:

- Voor- en achternaam
- Geslacht
- Adres (straat en huisnummer, postcode en woonplaats)
- Telefoonnummer
- E-mailadres
- Geboortedatum
- Identificerende gegevens (patiëntennummer e.d.)
- Financiële gegevens (DBC, Facturatie, Verzekeringsgegevens)
- Burgerservicenummer (BSN)

5.1.2 Verwerking van bijzondere persoonsgegevens van cliënten

Careyn vraagt naast gewone persoonsgegevens ook om gegevens over de gezondheid en het medicijngebruik van cliënten. Careyn verzamelt de volgende bijzondere persoonsgegevens van cliënten:

- Genetische gegevens
- Gegevens betreffende de gezondheid
- Filosofische of religieuze overtuigingen

5.1.3 Verwerking van gewone persoonsgegevens van medewerkers (waaronder benodigde persoonsgegevens van vrijwilligers)

Careyn verzamelt de volgende gewone persoonsgegevens van medewerkers:

- Voor- en achternaam
- Geslacht
- Adres
- Telefoonnummer
- E-mail
- Geboortedatum
- Identificerende gegevens (abonneenummer, lidmaatschapsnummer e.d.)
- Financiële gegevens (salaris, leningen, verzekeringsgegevens, kadaster)
- Opleiding en vorming
- Verklaring Omtrent Gedrag (VOG)

- Burgerservicenummer (BSN)

5.1.4 Verwerking van bijzondere persoonsgegevens van medewerkers

Careyn verzamelt de volgende bijzondere persoonsgegevens van medewerkers:

- Gegevens betreffende de gezondheid van medewerkers waarmee Careyn rekening dient te houden.

5.2 Doel en juridische grondslag

5.2.1 Verwerking van gewone persoonsgegevens van cliënten

Doeleinde:

- De verwerking van gewone persoonsgegevens heeft als doel instandhouding en ondersteuning van een adequate behandeling en zorgverlening aan cliënten en bewoners, waardoor een goede kwaliteit van zorg zoveel mogelijk wordt gewaarborgd.

Juridische grondslag:

- De verwerking van gewone persoonsgegevens heeft als juridische grondslag “noodzakelijk voor de uitvoering van de overeenkomst” of “noodzakelijk voor het nakomen van een wettelijke verplichting”.
- De verwerking van nationale identificatienummers, zoals het BSN, is alleen toegestaan indien dit gebeurt voor de uitvoering van de wet of voor doeleinden bij wet bepaald. Careyn is hiertoe verplicht op basis van de Wet gebruik burgerservicenummer in de zorg (Wbsn-z).

5.2.2 Verwerking van bijzondere persoonsgegevens van cliënten

Doeleinde:

- De verwerking van bijzondere persoonsgegevens heeft als doel instandhouding en ondersteuning van een adequate behandeling en zorgverlening aan cliënten en bewoners, waardoor een goede kwaliteit van zorg zoveel mogelijk wordt gewaarborgd.

Juridische grondslag:

- De verwerking van bijzondere persoonsgegevens heeft als juridische grondslag “noodzakelijk voor de uitvoering van de overeenkomst” of “noodzakelijk voor het nakomen van een wettelijke verplichting”.

5.2.3 Verwerking van gewone persoonsgegevens van (toekomstige) medewerkers

Doeleinde:

- De verwerking van gewone persoonsgegevens heeft als doel doelmatige bedrijfsvoering.

Juridische grondslag:

- De verwerking van gewone persoonsgegevens heeft als juridische grondslag “noodzakelijk voor de uitvoering van de overeenkomst”, “noodzakelijk voor het nakomen van een wettelijke verplichting”, “noodzakelijk voor de behartiging van een gerechtvaardigd belang” of “met toestemming van de betrokken persoon”.
- De verwerking van nationale identificatienummers, zoals het BSN, is alleen toegestaan indien dit gebeurt voor de uitvoering van de wet of voor doeleinden bij wet bepaald. Careyn is hiertoe verplicht op basis van de Wet op de loonbelasting.

5.2.4 Verwerking van bijzondere persoonsgegevens van (toekomstige) medewerkers

Doeleinde:

- De verwerking van bijzondere persoonsgegevens heeft als doel het verwerken van indiensttredingen, personeelsmutaties, uitdiensttredingen, de registratie van personeelszaken en het uitvoeren van de verzuimbegeleiding en re-integratie.

Juridische grondslag:

- De verwerking van bijzondere persoonsgegevens heeft als juridische grondslag “noodzakelijk voor de uitvoering van de overeenkomst” en “noodzakelijk voor het nakomen van een wettelijke verplichting.

5.3 Bewaartermijnen

Persoonsgegevens worden niet langer dan noodzakelijk voor het doel waarvoor zij zijn verwerkt bewaard. Zorggegevens worden na afloop van de zorgverlening verplicht 15 jaar bewaard.

6.Rechten van de betrokkene

6.1 Recht op informatie en communicatie

Careyn voldoet aan de informatieplicht die zij krachtens de Verordening heeft door de betrokkene actief op de hoogte te stellen van het feit dat zijn persoonsgegevens worden verwerkt en met welk doel. Careyn informeert de betrokkene over de risico's van gegevensverwerking, de geldende regels, de waarborgen, en de wijze waarop rechten met betrekking tot de verwerking van gegevens kunnen worden uitgeoefend.

Careyn communiceert met de betrokkene over zijn rechten in duidelijke en eenvoudige taal. Informatie wordt aangeboden in toegankelijke, beknopte, transparante en begrijpelijke vorm. De informatie wordt middels het privacy statement kosteloos aan de betrokkene verstrekt.

Careyn verschaft opgevraagde informatie niet indien:

- De betrokkene de betreffende informatie reeds heeft, bijvoorbeeld doordat het reeds aan betrokkene is verstrekt.
- De informatieverstrekking aan de betrokkene onmogelijk blijkt of een onevenredige inspanning vergt.
- De verkrijging of verstrekking van de persoonsgegevens uitdrukkelijk bij wet wordt uitgesloten en in die wet de gerechtvaardigde belangen van de betrokkene zijn gewaarborgd.
- De persoonsgegevens vertrouwelijk dienen te blijven in verband met het beroepsgeheim.

6.2 Recht op inzage

De betrokkene heeft het recht om de persoonsgegevens die Careyn van hem verwerkt in te zien.
Careyn verplicht zich bij inzageverzoeken om de betrokkene van het volgende op de hoogte te stellen:

- Waarom bepaalde gegevens worden verwerkt (de verwerkingsdoeleinden);
- Welke soorten gegevens worden verzameld;
- De (categorieën van) ontvangers van de persoonsgegevens;
- Welke privacy rechten betrokkenen hebben;
- Het recht om klacht in te dienen bij de Autoriteit Persoonsgegevens;
- Het recht op rectificatie, wissen, beperking en bezwaar hebben.

Genoemde informatie wordt middels een kopie verstrekt. Wanneer het recht op inzage door een betrokkene redelijkerwijs wordt ingeroepen wordt deze kopie kosteloos verstrekt. Voor bijkomende kopieën kan Careyn op basis van administratieve kosten wel een vergoeding vragen.
Indien de betrokkene een verzoek elektronisch indient en niet om een andere regeling verzoekt, verstrekt Careyn de informatie in een gangbare elektronische vorm.

6.3 Recht op rectificatie en aanvulling

Careyn draagt zorg dat gegevens die door haar worden verwerkt accuraat zijn en blijven. De betrokkene heeft, indien sprake is van onjuistheden in de gegevensverwerking, het recht om incorrecte gegevens te rectificeren en waar nodig aan te vullen.
Indien de betrokkene gebruik wenst te maken van zijn recht op rectificatie, faciliteert Careyn de betrokkene hierin.

Careyn stelt de betrokkene wiens persoonsgegevens zijn gerectificeerd, hiervan op de hoogte tenzij dit onmogelijk blijk dan wel onevenredige inspanningen vergt.

6.4 Recht op gegevenswissing en vergetelheid

Careyn zal in bepaalde gevallen op verzoek van de betrokkene persoonsgegevens wissen. Careyn is verplicht persoonsgegevens van betrokkene zonder onredelijke vertraging te wissen, onder andere indien:

- De persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- De betrokkene zijn toestemming intrekt en er geen andere rechtsgrond voor de verwerking bestaat;
- De betrokkene gegrond bezwaar heeft gemaakt tegen de verwerking en geen dwingende gerechtvaardigde gronden voor de verwerking prevaleren;
- De persoonsgegevens onrechtmatig zijn verwerkt.

De betrokkene heeft bij Careyn de mogelijkheid om zijn recht van vergetelheid uit te oefenen, dat wil zeggen; het recht om vergeten te worden. De betrokkene heeft het recht op verwijdering van alle informatie, die direct of indirect naar hem herleidbaar is.

Careyn neemt alle beschikbare technische maatregelen om persoonsgegevens die openbaar zijn gemaakt te wissen, tenzij dit op grond van de Verordening wegens bijvoorbeeld een wettelijke bewaartermijn niet is toegestaan.

6.5 Recht op beperking

De betrokkene kan onder bepaalde omstandigheden zijn recht op beperking uitoefenen teneinde het gebruik van de verwerkte persoonsgegevens te beperken. Indien wordt voldaan aan de volgende criteria:

- De juistheid van de persoonsgegevens wordt betwist;
- De verwerking is onrechtmatig;
- Careyn heeft de persoonsgegevens zelf niet meer nodig voor de betreffende verwerkingsdoeleinden, maar de betrokkene zelf wel;
- De betrokkene maakt bezwaar tegen de verwerking op basis van de rechtsgrond gerechtvaardigd belang, in afwachting van de vraag of de gerechtvaardigde belangen van Careyn zwaarder wegen dan die van betrokkenen.

Wanneer de verwerking van gegevens wordt beperkt zal Careyn de persoonsgegevens alleen kunnen verwerken indien:

- De betrokkene toestemming heeft gegeven;
- Sprake is van gewichtige redenen van algemeen belang, zoals bijvoorbeeld ter bescherming van de rechten van andere personen;
- In het kader van een rechtsvordering.

Careyn stelt partijen met wie de persoonsgegevens zijn gedeeld op de hoogte van de wijzigingen. Dit blijft slechts achterwege wanneer dit onmogelijk blijkt of een onevenredige inspanning vergt.

Wanneer een beperking wordt opgeheven zal Careyn de betrokkene hiervan op de hoogte brengen.

6.6 Recht op overdraagbaarheid van gegevens (dataportabiliteit)

Careyn zal de betrokkene, indien deze dit recht wenst uit te oefenen, de persoonsgegevens verstrekken in gestructureerde, gangbare en digitale vorm. Hiermee verkrijgt betrokkene de mogelijkheid tot overdracht van zijn persoonsgegevens aan een nieuwe verwerkingsverantwoordelijke.

Dit recht kan alleen worden uitgeoefend indien:
- De verwerking berust op ondubbelzinnige dan wel uitdrukkelijke toestemming van de betrokkene;
- De verwerking noodzakelijk is voor de uitoefening van de overeenkomst.

6.7 Bezwaar

Careyn zal verwerking van persoonsgegevens staken indien de betrokkene gebruik maakt van zijn recht op bezwaar tegen gegevensverwerking op basis van de grondslag gerechtvaardigd belang, behoudens gevallen waarin de belangen voor Careyn om de persoonsgegevens te verwerken zwaarder wegen dan de belangen van de betrokkene om de gegevensverwerking te staken.

7.Verplichtingen uit de Verordening

7.1 Verantwoordingsplicht

Careyn moet volgens de Verordening kunnen aantonen dat zij voldoet aan de eisen die de wet stelt aan gegevensbescherming. Dit wordt “accountability” of “verantwoordingsplicht”[2] genoemd. Om te kunnen voldoen aan de eis van “accountability” is het noodzakelijk om de kwaliteit van gegevensbescherming te optimaliseren en te borgen. Daarvoor heeft Careyn gegevensbescherming opgenomen in haar Beleid Informatieveiligheid (de zogenaamde “Plan Do Check Act-cyclus”). Het is noodzakelijk dat er continu aandacht is voor gegevensbescherming. Door consistente en regelmatige beoordeling van de kwaliteit van de gegevensbescherming voldoet Careyn aantoonbaar aan de eisen die door de Verordening aan gegevensbescherming worden gesteld.

In de volgende paragrafen wordt geeft Careyn aan hoe zij haar verantwoordingsplicht vervult.

7.2 Verwerkersovereenkomst

7.2.1 Careyn als verwerkingsverantwoordelijke

Wanneer Careyn als verwerkingsverantwoordelijke een verwerker inschakelt voor haar gegevensverwerkingen, sluit zij met deze een schriftelijke, waaronder elektronische, overeenkomst. Met een verwerkersovereenkomst sluit Careyn uit dat de andere partij de persoonsgegevens voor eigen doelen mag verwerken. Alleen verwerkers die afdoende garanties bieden ten aanzien van de bescherming van persoonsgegevens worden ingehuurd.

In de verwerkersovereenkomst legt Careyn onder meer de volgende onderwerpen vast:

- Een algemene beschrijving van het onderwerp, de duur, de aard en het doel van de verwerking, het soort persoonsgegevens, de categorieën van betrokkenen en de rechten en verplichtingen die Careyn heeft als verwerkingsverantwoordelijke;
- De verwerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken. Dit betekent dat de verwerking in principe uitsluitend plaatsvindt op basis van de schriftelijke instructies van Careyn;
- De geheimhoudingsplicht: personen in dienst van of werkzaam voor de verwerker hebben een geheimhoudingsplicht;
- De verwerker treft passende technische en organisatorische maatregelen om de verwerking te beveiligen;
- De verwerker schakelt geen subverwerker(s) in zonder de voorafgaande schriftelijke toestemming van Careyn;
- De verwerker helpt Careyn bij het voldoen aan haar plichten als de betrokkene zijn privacyrechten wenst uit te oefenen;

[2] Art. 5 lid 2 AVG

- De verwerker helpt Careyn ook andere verplichtingen na te komen, zoals het melden van datalekken en het uitvoeren van een Gegevensbeschermingseffectbeoordeling (DPIA);
- Na afloop van de verwerkingsdiensten verwijdert de verwerker de gegevens en kopieën, behoudens het geval dat de verwerker wettelijk verplicht is de gegevens te bewaren.

7.2.2 Careyn als verwerker

Wanneer Careyn als verwerker in opdracht van opdrachtgevers gegevensverwerkingen verricht, is de opdrachtgever verantwoordelijk voor het afsluiten van de verwerkersovereenkomst. Careyn is op grond van deze overeenkomst verplicht de daarin opgenomen verplichtingen na te komen.

7.3 Register van verwerkingsactiviteiten

Om aantoonbaar te maken dat Careyn voldoet aan haar verantwoordingplicht, houdt zij een register bij van de verwerkingsactiviteiten waarvoor zij verwerkingsverantwoordelijke is.

Dit register bevat minimaal de volgende gegevens:

- De naam en contactgegevens van de verwerkingsverantwoordelijke alsmede van de Functionaris Gegevensbescherming;
- De verwerkingsdoeleinden;
- Een beschrijving van de categorieën van betrokkenen (bijv. cliënten of werknemers) en van de categorieën persoonsgegevens;
- Een beschrijving van de categorieën van ontvangers van de persoonsgegevens aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- Indien van toepassing: een beschrijving van eventuele doorgifte van persoonsgegevens aan een derde land of internationale organisatie en eventueel documenten met betrekking tot passende waarborgen;
- Indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van persoonsgegevens moeten worden gewist;
- Indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Careyn geeft uitvoering aan deze verplichting door een verwerkingsregister bij te houden in een Excelsheet.

7.4 Gegevensbeschermingseffectbeoordeling

Een Gegevensbeschermingseffectbeoordeling, in de praktijk ook wel Privacy Impact Assessment (PIA) of Data Protection Impact Assessment (DPIA) genoemd, is een beoordeling van de effecten van een voorgenomen verwerkingsactiviteit op de bescherming van persoonsgegevens en de rechten en vrijheden van de betrokkene. Het is een instrument om van voorgenomen regelgeving of projecten waarbij persoonsgegevens worden verwerkt de effecten voor de betrokkene op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen. Op

basis hiervan treft Careyn maatregelen om deze effecten voor de betrokkene te voorkomen of te verkleinen. Hiermee voldoet Careyn aan de op haar rustende verantwoordingsplicht.

Er hoeft geen PIA uitgevoerd te worden wanneer de gegevensverwerking:

- Waarschijnlijk geen hoog privacy risico oplevert;
- Sterk lijkt op een andere gegevensverwerking waarvoor al een DPIA is uitgevoerd;
- Wordt geregeld door een andere Europese of nationale wet en er bij de totstandkoming van deze wet al een PIA is uitgevoerd. Behoudens gevallen waarin de privacy toezichthouder oordeelt dat er toch een PIA nodig is;
- Op een lijst staat van de verwerkingen waarvoor een PIA niet verplicht is. De Verordening geeft de privacy toezichthouder de mogelijkheid een dergelijke lijst op te stellen, maar dit is niet verplicht.

Indien Careyn gebruik maakt van een van bovenstaande uitzonderingen onderbouwt zij tegelijkertijd waarom zij zich niet genoodzaakt voelt een PIA uit te voeren.

7.4.1 Analyse van risico's

Careyn voert voorafgaand aan een verwerking van persoonsgegevens een Gegevensbeschermingseffectbeoordeling uit indien een voorgenomen verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Careyn bepaalt dit zelf door de risico's te analyseren. Careyn begint niet met de verwerking van gegevens voordat een benodigde PIA is uitgevoerd.

Er is sprake van een hoog risico wanneer een voorgenomen verwerking aan twee of meer van de onderstaande negen criteria voldoet:

1. Evaluatie van personen of scoretoekenning;
2. Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg;
3. Stelselmatige monitoring;
4. Gevoelige gegevens of gegevens van zeer persoonlijke aard;
5. Op grote schaal verwerkte gegevens;
6. Matching of samenvoeging van datasets;
7. Gegevens met betrekking tot kwetsbare betrokkenen;
8. Innovatieve toepassing van nieuwe technologische of organisatorische oplossing;
9. Blokkering van een recht, dienst of contract.

7.4.2 Inhoudelijk

De PIA bevat in ieder geval:

- Een beschrijving van de beoogde verwerking en de verwerkingsdoeleinden;
- Een beoordeling van de noodzakelijkheid en evenredigheid van de verwerking met betrekking tot de verwerkingsdoeleinden;
- Een beoordeling van de risico's voor de betrokkene;
- De beoogde maatregelen in de zin van waarborgen, veiligheidsmaatregelen en mechanismen om die risico's weg te nemen of te beperken.

De resultaten van de PIA neemt Careyn mee bij de opstelling van maatregelen die Careyn gaat treffen om de belangen van de betrokkene te beschermen en om aan te tonen dat zij de Verordening bij haar verwerkingsactiviteit naleeft.

Careyn evalueert regelmatig de resultaten van de PIA met het oog op veranderde omstandigheden, met name wanneer de verwerkingsactiviteit anders wordt ingericht, bijvoorbeeld door het gebruik van andere of nieuwere technologieën.

8.Beveiliging van persoonsgegevens

8.1: Beveiligingsincidenten / Meldplicht datalekken

Wanneer beveiligingsmaatregelen niet afdoende zijn gebleken en persoonsgegevens (mogelijk) zijn gelekt of verloren zijn gegaan, kan er sprake zijn van een datalek.
Een datalek is een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

De Europese privacy-toezichthouders hebben richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens de Verordening gepubliceerd.
Er worden drie categorieën datalekken gehanteerd:

1. Inbreuk op de vertrouwelijkheid: indien er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot persoonsgegevens;
2. Inbreuk op de integriteit: indien er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens;
3. Inbreuk op de beschikbaarheid: indien er sprake is van een onbevoegd of onopzettelijk verlies van toegang tot, of vernietiging van persoonsgegevens;

Binnen Careyn is een procesbeschrijving betreffende het melden van beveiligingsincidenten en een richtsnoer inzake de meldplicht datalekken opgesteld.
In het kort is de procedure als volgt:

- De medewerker meldt een (mogelijke) datalek in Topdesk.
- De Security Officer pakt de melding op en doet in samenwerking met de Privacy Officer nader onderzoek naar het incident, waarbij de Functionaris Gegevensbescherming en de bestuurssecretaris van de ontwikkelingen op de hoogte worden gehouden.
- Indien het een datalek betreft wordt er een melding gemaakt bij de Autoriteit Persoonsgegevens
- Indien er een risico voor de betrokkene te verwachten is wordt een brief verstuurd naar de betrokkene.

8.1.1 Melden bij de toezichthouder

Careyn meldt de datalek uiterlijk binnen 72 uur bij de Autoriteit Persoonsgegevens, tenzij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van betrokkenen. Indien dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd.

Bij de melding aan de Autoriteit Persoonsgegevens omschrijft en deelt Careyn in ieder geval het volgende:

- De aard van het datalek
- Indien van toepassing en waar mogelijk de categorieën van betrokkenen en het aantal betrokkenen.
- De naam en contactgegevens van de Functionaris Gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen.

- De waarschijnlijke gevolgen van het datalek.
- De maatregelen die Careyn heeft genomen of voorgesteld om het datalek aan te pakken.

8.1.2 Melden bij de betrokkene

Careyn meldt het datalek onverwijld aan de betrokkene, indien een hoog risico voor de rechten en vrijheden is ontstaan. Careyn meldt dit aan de betrokkene in eenvoudige en duidelijke taal.

De mededeling zal achterwege blijven indien:

- Careyn passende technische en organisatorische beschermingsmaatregelen genomen heeft en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk i.v.m. persoonsgegevens betrekking heeft, met name welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden;
  Een voorbeeld hiervan is wanneer de betreffende gegevens goed zijn versleuteld of vervangen door een hashwaarde.

  Deze uitzondering geldt alleen mits er aan 3 limitatieve voorwaarden is voldaan:
  1. De gegevens zijn nog volledig intact;
  2. Careyn heeft nog steeds de volledige controle over de gegevens;
  3. De sleutel voor encryptie of hashing die is gebruik bij de inbreuk heeft geen gevaar gelopen en met de beschikbare technologie onvindbaar.

- Careyn achteraf maatregelen heeft genomen om ervoor te zorgen dat het risico voor rechten en vrijheden van de betrokkene zich waarschijnlijk niet meer zal voordoen.

- De mededeling onevenredige inspanningen zou vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij de betrokkene even doeltreffend wordt geïnformeerd.

Bij de melding aan de betrokkene omschrijft en deelt Careyn in ieder geval het volgende:

- De aard van het datalek;
- De naam en contactgegevens van de Functionaris Gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- De waarschijnlijke gevolgen van het datalek;
- De maatregelen die Careyn heeft genomen of voorgesteld om het datalek aan te pakken.

8.2 Privacy by Design and Default

Careyn houdt rekening met de stand van de techniek, de kosten en de aard, de omvang, de context en het doel van de verwerking, alsook met de risico's voor de rechten en vrijheden van de betrokkenen die met de specifieke verwerking zijn verbonden.
De Verordening hanteert het beginsel van *Privacy by Design* en *Privacy by Default*, ook wel Privacy door ontwerp en door standaard-instellingen genoemd. Dit verplicht Careyn ertoe om bij het ontwikkelen van een nieuw beleid of het ontwerp van nieuwe systemen waarbinnen persoonsgegevens worden verwerkt telkens privacy en gegevensbescherming

mee te nemen. Careyn tracht de inbreuk op de persoonlijke levenssfeer die zij maakt bij de verwerking van persoonsgegevens zo veel mogelijk te minimaliseren.

Om aan deze verplichting te voldoen treft Careyn privacy verhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Bij de bepaling welke technische en organisatorische maatregelen kunnen worden toegepast houdt Careyn rekening met een aantal elementen:

- De stand van de techniek;
- De uitvoeringskosten;
- De aard, omvang, context en het doel van de verwerking;
- De risico's voor de betrokkene.

Careyn hanteert onder andere de volgende maatregelen:

- Cryptografische maatregelen voor het waarborgen van vertrouwelijkheid (pseudonominseren en versleutelen van gevoelige informatie, het gebruiken van een beveiligd mailsysteem).
- Cryptografische maatregelen voor het waarborgen van integriteit en authenticiteit (digitale handtekening).
- Cryptografische maatregelen voor het waarborgen van onweerlegbaarheid (bewijs dat een gebeurtenis wel of niet heeft plaatsgevonden).
- Maatregelen die toezien op de fysieke beveiliging en de beveiliging van de omgeving (toegang tot locaties/ruimten wordt gegeven op basis van functie en noodzakelijke toegang).
- Maatregelen die toezien op de toegangsbeveiliging (registratie van gebruikers, beheer van gebruikerswachtwoorden).
- Maatregelen die het vermogen omvatten om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen.

Daarnaast wordt het principe van dataminimalisering gehanteerd. Alleen die gegevens die noodzakelijk zijn voor het doel van de verwerking worden verwerkt waardoor Careyn een zorgvuldige en verantwoorde omgang met (persoons)gegevens technisch kan afdwingen.

8.2.1 Informatieveiligheidsbeleid

Careyn heef het beleid voor informatieveiligheid vastgelegd in het 'Beleid Informatieveiligheid' en het 'Handboek Informatieveiligheid'. Hierin worden maatregelen beschreven welke de beschikbaarheid, integriteit en vertrouwelijkheid van informatie waarborgen. Naar aanleiding van risicoanalyses worden maatregelen opgenomen in het informatiebeveiligingsproces.
In deze documenten wordt gedetailleerder ingegaan op de soorten (cryptografische) maatregelen die Careyn treft teneinde informatieveiligheid te borgen.

8.3: Bewaren en vernietigen van persoonsgegevens

Careyn bewaart persoonsgegevens die door haar worden verwerkt niet langer dan wettelijk noodzakelijk is. De bewaringstermijn hangt af van het doel waarvoor de persoonsgegevens worden verzameld en verwerkt.