Privacybeleid

Document gegevens:	
01. Portaal: Cliëntenzorg	N.v.t.
02. Portaal: Medewerkers	N.v.t.
03. Portaal: Gebouwen	N.v.t.
04. Portaal Bedrijfsvoering	N.v.t.
05. Soort document	Beleid
06. Aantal pagina's (incl. voorblad)	1
07. Status	Definitief
08. Versienummer	Nr: 2.0
09. Datum vaststelling document	Maand 2020
10. Datum evaluatie (uiterlijk vóór...)	Maand 2020
11. Auteur(s)	Michiel Beijer – Privacy Officer

Geraadpleegde inhoudsdeskundige:		
01. Naam: Jeroen Benning	Functie: CISO	Paraaf:
02. Naam: Veerle Diederen	Functie: FG	Paraaf:
03. Naam:	Functie: Maak een keuze	Paraaf:

Vaststellen document:		
01. Autorisator (doc. verantwoordelijke)	Jean-Pierre Halmans, directeur F&C	Paraaf:
02. Raad van Bestuur	Raad van Bestuur	Paraaf:
03. Centrale Cliëntenraad: Maak een keuze	Voorzitter Centrale Cliëntenraad	Paraaf:
04. OR: Maak een keuze	Voorzitter Ondernemingsraad	Paraaf:

Inhoud

1. Voorwoord

Bij de uitvoering van het zorgproces en de overige vormen van dienstverlening van Sevagram is het noodzakelijk dat persoonsgegevens worden verwerkt. Dit dient op een zorgvuldige en rechtmatige wijze plaats te vinden. Mede vanuit haar mensgerichte Planetree-visie hecht Sevagram veel waarde aan privacy en de bescherming van persoonsgegevens van haar cliënten, medewerkers, vrijwilligers en alle overige betrokkenen. Alle betrokkenen kunnen en mogen erop vertrouwen dat hun persoonsgegevens door Sevagram zorgvuldig en met inachtneming van de toepasselijke wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG), worden verwerkt.

De AVG bevat regels met betrekking tot de bescherming van natuurlijke personen op het gebied van persoonsgegevens en het vrije verkeer daarvan. Op grond van de AVG dient Sevagram een Privacybeleid te hebben en uit te voeren. Door middel van dit beleidsdocument neemt de Raad van Bestuur haar verantwoordelijkheid ten aanzien van de naleving van de AVG en het aantoonbaar waarborgen van de privacyrechten van betrokkenen binnen Sevagram. Het Privacybeleid beschrijft de wijze waarop Sevagram uitvoering geeft aan de naleving van de AVG en welke regels en principes hierbij in acht dienen te worden genomen. Het Privacybeleid en het informatiebeveiligingsbeleid (IB-beleid) zijn de twee pijlers als het gaat om privacy en gegevensbescherming, waaronder een aantal uitvoerende beleidstukken en procedures onder hangen. Een aantal van deze procedures staan specifiek genoemd bij één of meerdere van de beschreven onderwerpen. Voor de overige procedures wordt verwezen naar bijlage 1.

Ondanks dat het Privacy- en IB-beleid veel raakvlakken hebben is ervoor gekozen om deze twee beleid stukken apart van elkaar op te zetten. Het Privacybeleid komt namelijk met name voort vanuit de AVG en het IB-beleid is vooral gericht op de opvolging van de NEN-7510:2017 richtlijn, welke ook vereist dat Sevagram een IB-beleid heeft en uitvoert. Tevens heeft Sevagram uitgesproken om in de toekomst te willen certificeren voor deze NEN-7510:2017. Voldoen aan zowel de AVG en de NEN-7510:2017 vereist expertise en aandacht. Dit zal dan ook terugkomen in het Privacybeleid.

Leeswijzer:
Lees dit document aandachtig en overweeg alle besluiten die hierin beschreven staan. In de eerste hoofdstukken wordt beschreven voor wie dit beleid van toepassing is en wordt kort stilgestaan bij de wettelijke kaders vanuit de AVG. Vervolgens zal vanaf hoofdstuk 7 achtereenvolgens gesproken worden over de verschillende rollen en verantwoordelijkheden, en op welke manier Sevagram invulling wilt geven aan de verplichtingen vanuit de AVG rondom Privacy. Tot slot zal er ook nog aandacht besteed worden aan het delen van gegevens met derden en mogelijke risico's die er zijn als het gaat om de privacy van betrokkenen.

2. Bereik

Het bereik van dit beleid is het door de verwerkingsverantwoordelijke opstellen en onderhouden van het Privacybeleid van Stichting Sevagram Zorgcentra (‘Sevagram’).

3. Verantwoordelijkheden

Het voor Sevagram opstellen en onderhouden van een beleidsverklaring betreffende de bescherming van persoonsgegevens is de verantwoordelijkheid van de portefeuillehouder privacy / Privacy Officer.

4. Procedure

Dit beleid is opgesteld door de privacy officer en bevat de volgende elementen:

- Toepasselijkheid AVG
- Verantwoordelijkheden en rollen AVG
- Grondbeginselen van bescherming persoonsgegevens
- Rechten van betrokkenen
- Toestemming
- Veiligheid van persoonsgegevens
- Verstrekking van persoonsgegevens aan derden
- Bewaring en verwijdering van persoonsgegevens
- Doorgifte van persoonsgegevens
- Risico’s

Het concept-Privacybeleid is ter advies voorgelegd aan de functionaris van gegevensbescherming en vervolgens aan de Stuurgroep Privacy. De privacy officer heeft vervolgens de verkregen adviezen verwerkt om de concept-beleidsverklaring ter accordering voor te leggen aan de Raad van Bestuur.

5. Inleiding

De Algemene Verordening Gegevensbescherming van 2016 vervangt de EU-Richtlijn Gegevensbescherming 95/46/EC uit 1995 en komt tevens in de plaats van alle op basis daarvan door individuele lidstaten ontwikkelde wetgeving. Doel van de AVG is tweeledig: beschermen van de “rechten en vrijheden” van natuurlijke personen (levende individuen) en zeker stellen dat persoonsgegevens uitsluitend worden verwerkt met medeweten en, voor zover mogelijk, met toestemming van de betrokkenen.

5.1 Door Sevagram gehanteerde definities (afgeleid van de AVG)

Materieel toepassingsgebied (artikel 2): De AVG is van toepassing op de geheel of gedeeltelijk geautomatiseerde (d.w.z. computergestuurde) verwerking, alsmede op de verwerking, anders dan met geautomatiseerde middelen, van persoonsgegevens (in de vorm van persoonsgegevens op papier) die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Territoriaal toepassingsgebied (artikel 3): De AVG is van toepassing op alle in de EU gevestigde verwerkingsverantwoordelijken die persoonsgegevens verwerken in de context van de activiteiten van hun organisatie, alsmede op verwerkingsverantwoordelijken buiten de EU die persoonsgegevens verwerken om goederen of diensten aan te bieden aan of het gedrag te volgen van betrokkenen die zich in de EU bevinden.

Vestigingen (artikel 4): De hoofdvestiging van een verwerkingsverantwoordelijke in de EU is de plaats waar de belangrijkste beslissingen over doelstellingen van en middelen voor de verwerking van persoonsgegevens worden genomen, m.a.w. de plaats van zijn centrale administratie in de EU. Buiten de EU gevestigde verwerkingsverantwoordelijken of verwerkers moeten een vertegenwoordiger in de EU aanwijzen die gemachtigd is op te treden namens de verwerkingsverantwoordelijke of verwerker en het contact verzorgt met de toezichthoudende autoriteit en de betrokkenen in alle kwesties die verband houden met de verwerking van persoonsgegevens.

Persoonsgegevens (artikel 4): 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 van persoonsgegevens (artikel 9): Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van 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.

Verwerkingsverantwoordelijke (artikel 4): De 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.

Betrokkene (artikel 4): Elke levende persoon die het onderwerp is van persoonsgegevens die in het bezit zijn van een organisatie.

Verwerking (artikel 4): 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.

Profilering (artikel 4): Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Inbreuk in verband met persoonsgegevens (artikel 4): 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.

Toestemming van de betrokkene (artikel 4): Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem of haar betreffende verwerking van persoonsgegevens aanvaardt.

Derde (artikel 4): 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.

Bestand (artikel 4): Elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.

6. Beleidsverklaring

6.1 De Raad van Bestuur en het directieteam van Sevagram, statutair gevestigd te Heerlen, hebben de overtuigde intentie zich volledig te houden aan alle relevante EU- en nationale wetgeving met betrekking tot de bescherming van persoonsgegevens en de bescherming van de rechten en vrijheden van personen van wie Sevagram persoonsgegevens verzamelt en verwerkt.

6.2 Dit beleid en andere relevante beleidsstukken zoals het informatiebeveiligingsbeleid beschrijven de betekenis van compliance met de Algemene Verordening Gegevensbescherming (AVG) alsmede relevante delen van de NEN-7510:2017 en de daarmee verbonden processen en procedures.

6.3 De AVG en dit beleid zijn van toepassing op alle bij Sevagram in gebruik zijnde functies voor verwerking van persoonsgegevens, met inbegrip van verwerkingsfuncties die worden gebruikt voor verwerking van persoonsgegevens van klanten, medewerkers, leveranciers en partners en alle andere persoonsgegevens die, afkomstig uit welke bron dan ook, door Sevagram worden verwerkt.

6.4 Sevagram heeft doelstellingen voor bescherming van persoonsgegevens opgesteld en vastgelegd in haar Privacy- en Informatiebeveiligingsbeleid.

6.5 De privacy officer is verantwoordelijk voor jaarlijkse controle van het register van verwerkingen in het licht van mogelijke veranderingen in de activiteiten van Sevagram en mogelijke extra vereisten zoals gebleken uit gegevensbeschermingseffectbeoordelingen (DPIA's - Data Protection Impact Assessments). Genoemd register dient beschikbaar te worden gesteld op verzoek van de toezichthoudende autoriteit.

6.6 Dit beleid is van toepassing op alle medewerkers en belanghebbende partijen, zoals externe leveranciers van Sevagram. Inbreuken op de AVG zullen worden behandeld volgens het disciplinaire beleid van Sevagram en kunnen tevens als wetsdelict worden beoordeeld, in welk geval de kwestie zo snel mogelijk aan de bevoegde autoriteiten zal worden gemeld.

6.7 Van partners van en externe partijen werkend met of voor Sevagram met toegang of mogelijke toegang tot persoonsgegevens, wordt verwacht dat zij kennis hebben genomen van dit beleid, dit beleid begrijpen en zich aan dit beleid zullen houden. Geen enkele externe partij heeft het recht van toegang tot persoonsgegevens in het bezit van Sevagram zonder voorafgaande afsluiting van een gegevensvertrouwelijkheidsovereenkomst, die aan de externe partij dezelfde zwaarwegende verplichtingen oplegt als waaraan Sevagram zelf gehouden is en die Sevagram het recht geeft conformering aan deze overeenkomst te controleren.

7. Verantwoordelijkheden en rollen onder de AVG

7.1 Sevagram is onder de AVG een verwerkingsverantwoordelijke.

7.2 Het hoogste management van Sevagram en alle personeelsleden in management- of leidinggevende rollen binnen de organisatie zijn verantwoordelijk voor de ontwikkeling, invoering en stimulering van goede praktijken op het gebied van de bescherming van persoonsgegevens binnen Sevagram; de exacte verantwoordelijkheden worden gespecificeerd in individuele functieomschrijvingen.

7.3 De Privacy Officer rapporteert aan het directieteam en de Raad van Bestuur van Sevagram inzake de bescherming van persoonsgegevens binnen Sevagram en de status van compliance met en praktische toepassing van wetgeving op het gebied van bescherming van persoonsgegevens. De Functionaris voor Gegevensbescherming heeft een, onafhankelijke, controlerende functie als het gaat om deze compliance en praktische toepassing van de wetgeving.

7.4 De Privacy Officer beschikt over de juiste kwalificaties en passende ervaring, is aangesteld met de bedoeling dat hij of zij de verantwoordelijkheid op zich neemt voor monitoring van en advisering met betrekking tot conformering, binnen Sevagram en op dagelijkse basis, aan dit beleid en, in het bijzonder, voor monitoring en advisering van managers en leidinggevenden inzake AVG-compliance bij Sevagram, binnen hun respectievelijke verantwoordelijkheidsterreinen.

7.5 De Privacy Officer heeft specifieke verantwoordelijkheden met betrekking tot relevante procedures en is het eerste aanspreekpunt voor medewerkers die uitleg nodig hebben over welk aspect dan ook van gegevensbescherming-compliance.

7.6 Naleven van wetgeving op het gebied van bescherming van persoonsgegevens is de verantwoordelijkheid van alle medewerkers van Sevagram die persoonsgegevens verwerken.

7.7 Sevagram is in haar rol als verwerkingsverantwoordelijke verplicht om vereisten op het gebied van training en bewustwording in relatie tot de rollen van medewerkers betrokken bij de verwerking van persoonsgegevens te specificeren. Deze vereisten zijn opgenomen in de “Procedure Training en bewustwording”.

7.8 Het is de verantwoordelijkheid van medewerkers en vrijwilligers van Sevagram om ervoor te zorgen dat persoonsgegevens over hen en door hen verstrekt aan Sevagram correct en actueel zijn.

8. Principes van bescherming van persoonsgegevens

Alle vormen van verwerking van persoonsgegevens moeten worden uitgevoerd in overeenstemming met de grondbeginselen zoals omschreven in artikel 5 van de AVG. Beleid en procedures met betrekking tot de bescherming van persoonsgegevens binnen Sevagram zijn opgesteld om compliance met deze grondbeginselen te waarborgen.

8.1 Verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn

Sevagram onderhoudt een “Procedure Opstellen en bekendmaken privacyverklaringen”.

De specifieke informatie die in dit kader door Sevagram aan de betrokkenen wordt verstrekt, moet minimaal het volgende omvatten:

- Identiteit en contactgegevens van de verwerkingsverantwoordelijke en, voor zover van toepassing, diens vertegenwoordiger;
- Contactgegevens van de Functionaris Gegevensbescherming;
- Doelstellingen van de verwerking waarvoor de persoonsgegevens zijn bedoeld en de wettelijke grondslag voor de verwerking;
- De bewaartermijn van de persoonsgegevens;
- Het recht van de betrokkene op inzage, rectificatie en verwijdering van zijn of haar persoonsgegevens en het recht om bezwaar te maken tegen de verwerking, en de voorwaarden (of het ontbreken van voorwaarden) voor de uitoefening van deze rechten, bijvoorbeeld in verband met mogelijke effecten op de rechtmatigheid van eerdere verwerking;
- De ontvangers of categorieën van ontvangers van de persoonsgegevens, waar van toepassing;
- Dat de verwerkingsverantwoordelijke, waar van toepassing, het voornemen heeft tot doorgifte van de persoonsgegevens aan een ontvanger in een derde land en het niveau van bescherming dat voor de persoonsgegevens wordt geboden;
- Alle andere informatie die nodig is om zeker te stellen dat sprake is van verwerking die voldoet aan de beginselen van rechtmatigheid, behoorlijkheid en transparantie.

8.2 Persoonsgegevens mogen alleen worden verzameld voor specifieke, expliciete en gerechtvaardigde doeleinden

Gegevens die zijn verkregen voor uitdrukkelijk omschreven doeleinden mogen niet worden gebruikt voor een doel dat afwijkt van de doeleinden als omschreven in het register van verwerkingen van Sevagram.

8.3 Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de voorgenomen verwerking

- De Privacy officer en Functionaris voor Gegevensbescherming zorgen er door monitoring en advisering voor dat Sevagram geen informatie verzamelt die niet strikt noodzakelijk is voor de gestelde doeleinden.
- Alle vormen van gegevensverzameling (elektronisch of op papier), met inbegrip van gegevensverzamelingsvereisten in nieuwe informatiesystemen, moeten vergezeld gaan van een koppeling naar één (of meer) privacyverklaring(en).
- De functionaris gegevensbescherming zorgt voor monitoring van en advisering inzake methoden van gegevensverzameling om zeker te stellen dat de verzamelde persoonsgegevens toereikend en ter zake dienend blijven en niet excessief zijn.

8.4 Om ervoor te zorgen dat persoonsgegevens accuraat en actueel zijn, moeten alle redelijke maatregelen worden genomen om persoonsgegevens die onjuist zijn onverwijld te wissen of te rectificeren

- Persoonsgegevens die bij Sevagram zijn opgeslagen, moeten regelmatig worden gecontroleerd en waar nodig geactualiseerd. Persoonsgegevens waarvan niet in redelijkheid kan worden aangenomen dat ze correct zijn, moeten ook niet worden bewaard.
- De Privacy officer zorgt er door monitoring en advisering voor dat alle medewerkers training ontvangen over het belang van het verzamelen van accurate persoonsgegevens en het op peil houden van die accuratesse.
- Het is ook de verantwoordelijkheid van de betrokkene om ervoor te zorgen dat de persoonsgegevens in bezit van Sevagram accuraat en actueel zijn. Dat is de reden waarom betrokkenen bij het invullen van registratie- of aanvraagformulieren tevens, door middel van een standaard opgenomen tekst, verklaren de in het formulier verstrekte persoonsgegevens correct zijn op het tijdstip van indienen.
- Medewerkers zijn gehouden Sevagram te verwittigen van wijzigingen in hun omstandigheden, zodat hun persoonsgegevens overeenkomstig kunnen worden aangepast. Het is de verantwoordelijkheid van Sevagram om ervoor te zorgen dat alle berichtgeving met betrekking tot wijziging van omstandigheden wordt gedocumenteerd en dat er actie op wordt ondernomen.
- De CISO en Privacy officer zorgen er door monitoring en advisering voor dat passend beleid en passende procedures geïmplementeerd zijn om persoonsgegevens accuraat en actueel te houden, rekening houdend met de hoeveelheid verzamelde gegevens, de snelheid waarmee veranderingen kunnen optreden en andere relevante factoren.
- Minimaal op jaarlijkse basis bekijkt de Privacy officer de einddatums voor bewaring van alle door Sevagram verwerkte persoonsgegevens aan de hand van het register van verwerkingen, ter identificatie van persoonsgegevens die niet langer nodig zijn in de context van het geregistreerde doel. Deze persoonsgegevens worden vervolgens op een veilige manier verwijderd/vernietigd conform de “Procedure Veilige Verwijdering van Opslagmedia”.
- De Privacy officer ziet erop toe dat wordt gereageerd op door betrokkenen ingediende verzoeken tot rectificatie, en wel binnen één maand. Die termijn kan indien nodig en gelet op de complexiteit van het verzoek, met nog eens twee maanden worden verlengd. Als Sevagram besluit geen gevolg te geven aan een verzoek, deelt de Privacy officer de betrokkene mee waarom het verzoek zonder gevolg is gebleven, en informeert hij hem/haar over de mogelijkheid om een klacht in te dienen bij een toezichthoudende autoriteit en beroep bij de rechter in te stellen.

- In het geval dat derden mogelijk onjuiste of achterhaalde persoonsgegevens hebben ontvangen, zorgt de Privacy officer ervoor dat die derden van de problemen op de hoogte worden gesteld en worden geïnstrueerd de persoonsgegevens niet te gebruiken als basis voor besluitvorming ten aanzien van de betrokkenen. Waar nodig zorgt de Privacy officer er ook voor dat correcties worden doorgegeven aan de betreffende derden.

8.5 Persoonsgegevens moeten worden bewaard in een vorm die identificatie van de betrokkenen niet langer mogelijk maakt dan noodzakelijk is voor de doeleinden van verwerking van de gegevens

- Als persoonsgegevens langer worden bewaard dan tot aan de einddatum van verwerking, worden ze geminimaliseerd, versleuteld of gepseudonimiseerd ter bescherming van de betrokkene(n).
- Persoonsgegevens worden bewaard in overeenstemming met de “Procedure Bewaartermijnen” en worden bij verstrijken van de bewaartermijn op een veilige manier vernietigd, zoals beschreven in deze procedure.
- Wanneer persoonsgegevens langer worden bewaard dan de bewaartermijnen die zijn vastgelegd in de “Procedure Bewaartermijnen”, ziet de Privacy officer erop toe dat rechtvaardiging voor die verlengde periode duidelijk is omschreven en in overeenstemming is met wettelijke eisen ten aanzien van bescherming van persoonsgegevens.

8.6 De verwerkingsverantwoordelijke moet in staat zijn compliance aan te tonen met de andere principes van de AVG (accountability)

Bij wijze van aanvulling op de eisen ten aanzien van transparantie, staan in de AVG ook bepalingen die stimuleren tot accountability en zorgvuldige bedrijfsvoering. Het accountability-principe in artikel 5, lid 2 stelt dat de verwerkingsverantwoordelijke niet alleen moet voldoen aan de in de AVG genoemde principes van verantwoorde gegevensverwerking, maar tevens in staat moet zijn naleving aan te tonen. Sevagram zal naleving van deze principes aantonen door implementatie van beleid voor bescherming van persoonsgegevens, door zich te houden aan vastgelegde gedragsregels, door het nemen van technische en organisatorische maatregelen en door adoptie van technieken als data protection by design, door het uitvoeren van gegevensbeschermingseffectbeoordelingen (DPIA’s), door het onderhouden van procedures voor melding van datalekken en reactie op incidenten.

9. Rechten van de betrokkenen

Als het gaat om de persoonsgegevens die over hen worden verzameld en vastgelegd en over de verwerking van die gegevens, hebben betrokkenen de volgende rechten:

- Inzage van zijn of haar persoonsgegevens om te controleren wat voor persoonsgegevens zijn verzameld en aan wie ze beschikbaar zijn gesteld.
- Bezwaar te maken tegen verwerking die tot schade, materieel dan wel immaterieel, kan leiden.
- Bezwaar te maken tegen verwerking ten behoeve van direct marketing.
- Geïnformeerd te worden over de mechanismen van geautomatiseerd proces van besluitvorming dat verstrekkende gevolgen voor de betrokkene kan hebben.
- Niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit waaraan voor hem of haar verstrekkende gevolgen verbonden zijn.
- Compensatie te eisen voor geleden schade als gevolg van een overtreding van de AVG.
- Actie te ondernemen om te zorgen dat onjuiste persoonsgegevens worden gerectificeerd, geblokkeerd, gewist (met inbegrip van het recht op vergetelheid) of vernietigd.

- De toezichthoudende autoriteit te verzoeken na te gaan of er sprake is van een overtreding van de AVG.
- De hem of haar betreffende persoonsgegevens te verkrijgen in een gestructureerd, gangbaar en machineleesbaar formaat en die aan een andere verwerkingsverantwoordelijke door te laten zenden.
- Niet te worden onderworpen aan geautomatiseerde besluitvorming zonder daar toestemming voor te hebben gegeven.

Sevagram zorgt ervoor dat betrokkenen de volgende rechten kunnen uitoefenen:

- Betrokkenen hebben het recht te vragen om inzage in hun persoonsgegevens en het recht een verzoek, klacht of bezwaar in te dienen bij Sevagram zoals beschreven in de procedures voor medewerkers, cliënten en overige betrokkenen. Deze procedures beschrijven ook hoe Sevagram ervoor zal zorgen dat haar reactie op een verzoek voldoet aan de vereisten van de AVG.

10. Toestemming

Sevagram begrijpt 'toestemming' in de betekenis van expliciet en vrijwillig verleend, als een specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene of diens vertegenwoordiger door middel van een verklaring of een ondubbelzinnige actieve handeling aangeeft in te stemmen met verwerking van hem of haar betreffende persoonsgegevens. De betrokkene of diens vertegenwoordiger kan die toestemming op elk gewenst moment intrekken.

Sevagram verstaat onder 'toestemming' ook dat de betrokkene of diens vertegenwoordiger volledig is geïnformeerd over de voorgenomen verwerking en zich daarmee akkoord heeft verklaard, in het volle bezit van zijn of haar verstandelijke vermogens en zonder dat er druk op hem of haar is uitgeoefend. Onder druk of dwang verkregen toestemming of toestemming die is verleend op basis van misleidende informatie, wordt niet beschouwd als een wettelijke grondslag voor verwerking.

Sevagram moet in staat zijn aan te tonen dat toestemming is verkregen voor een verwerking van persoonsgegevens. Afhankelijk van de te verkrijgen toestemming wordt hierbij gebruik gemaakt van een te ondertekenen formulier of een prominent aanwezige privacyverklaring op de website die bezoekers moeten accepteren alvorens ze persoonsgegevens kunnen doorgeven.

Voor bijzondere persoonsgegevens moet expliciete, schriftelijke toestemming zijn verkregen tenzij er sprake is van een alternatieve wettelijke grondslag voor verwerking. Als er sprake is van een alternatieve wettelijke grondslag voor verwerking van bijzondere persoonsgegevens is deze terug te vinden in het register van verwerkingen.

11. Gegevensveiligheid

Alle medewerkers van Sevagram hebben de taak ervoor te zorgen dat de persoonsgegevens die in het bezit zijn van Sevagram en waarvoor zij verantwoordelijk zijn, veilig worden bewaard en onder geen enkele voorwaarde worden verstrekt aan derden, tenzij die derde uitdrukkelijk door Sevagram is geautoriseerd voor ontvangst van de betreffende informatie en daartoe een vertrouwelijkheidsovereenkomst is aangegaan.

Alle persoonsgegevens dienen uitsluitend toegankelijk te zijn voor personen die ermee moeten werken en toegang mag alleen worden verleend volgens de “Procedure Toegangscontrole”.
Alle persoonsgegevens moeten worden behandeld met inachtneming van de hoogste veiligheidseisen en moeten als volgt worden bewaard:

- in een afsluitbare ruimte met voorzieningen voor toegangscontrole; en/of
- in een afgesloten lade of archiefkast; en/of
- in het geval van digitale gegevens, wachtwoordbeveiliging in overeenstemming met de geldende bedrijfsregels; en/of
- opgeslagen op (uitneembare) computermedia, versleuteld in overeenstemming met de “Procedure Veilige verwijdering van opslagmedia”.

Er dient op te worden gelet dat beeldschermen en terminals alleen zichtbaar zijn voor geautoriseerd personeel van Sevagram. Alle medewerkers zijn verplicht een individuele Gebruikersovereenkomst aan te gaan voordat hen toegang wordt verleend tot bedrijfsinformatie van welke aard dan ook. In die overeenkomst worden o.a. zaken geregeld als automatische schermuitschakeling en screen time-outs.
Gegevens op papier mogen niet worden achtergelaten op plaatsen waar ze kunnen worden gezien door ongeautoriseerd personeel en mogen niet worden meegenomen uit de bedrijfsgebouwen zonder uitdrukkelijke toestemming. Zodra zulke papieren persoonsgegevens niet langer nodig zijn voor dagelijkse klantenondersteuning, dienen ze uit hun beveiligd archief te worden verwijderd in overeenstemming met de “Procedure Veilige verwijdering van opslagmedia”.

Persoonsgegevens mogen alleen worden gewist of verwijderd in overeenstemming met de “Procedure Bewaartermijnen”. Papieren persoonsgegevens waarvoor het einde van de bewaartermijn is bereikt, worden versnipperd en afgevoerd als ‘vertrouwelijk afval’. Vaste schijven van overbodig geworden computers worden verwijderd en onmiddellijk vernietigd volgens de voorschriften van de “Procedure Veilige verwijdering van opslagmedia”. Pas daarna is afvoer mogelijk. ‘Off-site’ verwerking van persoonsgegevens verhoogt het gevaar van verlies, diefstal of beschadiging van gegevens. Voor off-site gegevensverwerking is dan ook specifieke autorisatie vereist.

12. Verstrekking van persoonsgegevens aan derden

Sevagram moet ervoor zorgen dat persoonsgegevens niet worden verstrekt aan ongeautoriseerde derden. Daaronder vallen ook familieleden en vrienden van medewerkers, overheidsinstanties en in bepaalde omstandigheden, de politie. Alle medewerkers dienen voorzichtigheid te betrachten wanneer hen wordt gevraagd persoonsgegevens te verstrekken aan enige andere partij dan de betrokkene zelf. In voorkomende gevallen dient altijd de vraag te worden gesteld of verstrekking van de persoonsgegevens relevant en noodzakelijk is voor de bedrijfsvoering van Sevagram.

Onder de AVG is verstrekking van persoonsgegevens aan derden in sommige gevallen toegestaan zonder toestemming van de betrokkene, namelijk als er een van de volgende doelen mee gediend wordt:

- waarborging van nationale veiligheid;
- voorkoming van of onderzoek naar strafbare feiten, met inbegrip van aanhouding en vervolging van de daders;
- belastingtechnisch onderzoek of heffing van belasting;
- onderzoek naar schendingen van beroepscode (bijv. met betrekking tot gezondheid, veiligheid en welzijn op het werk);
- voorkoming van ernstige schade voor een derde; en

- bescherming van de vitale belangen van een persoon.

Verzoeken tot verstrekking van persoonsgegevens om een van deze redenen moeten vergezeld gaan van een deugdelijke onderbouwing en voor feitelijke verstrekking is altijd specifieke autorisatie nodig van de Privacy officer.

13. Bewaring en verwijdering van gegevens

Sevagram bewaart persoonsgegevens, in een vorm die identificatie van de betrokkenen mogelijk maakt, niet langer dan nodig is met het oog op het doel of de doeleinden waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

Sevagram kan persoonsgegevens langer bewaren als die persoonsgegevens dan uitsluitend worden verwerkt met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. In dat geval zullen passende technische en organisatorische maatregelen worden genomen om rechten en vrijheden van de betrokkenen te waarborgen. De bewaartermijn voor elke categorie persoonsgegevens wordt vastgelegd in de “Procedure Bewaartermijnen”, samen met de criteria voor bepaling van die periode, waarbij ook wettelijke verplichtingen een rol kunnen spelen. De actuele bewaartermijnen zijn ten alle tijden terug te vinden in het register van verwerkingen.

De procedures van Sevagram ten aanzien van bewaring en verwijdering van persoonsgegevens zijn in alle gevallen van toepassing. Persoonsgegevens moeten op een veilige manier worden verwijderd, in overeenstemming met artikel 5 lid 1 sub f AVG – dusdanig dat veiligheid gewaarborgd is, ter bescherming van de “rechten en vrijheden” van de betrokkenen. Verwijdering van persoonsgegevens gebeurt altijd volgens de “Procedure Veilige verwijdering van opslagmedia”.

14. Doorgifte van gegevens

Doorgifte van persoonsgegevens vanuit de Europese Economische Ruimte (EER) naar niet-EER landen (in de AVG ‘derde landen’ genoemd) is verboden tenzij het derde land in kwestie passende waarborgen biedt voor een adequaat “beschermingsniveau voor de grondrechten van de betrokkenen”.

Doorgifte van persoonsgegevens naar landen buiten de EER is verboden tenzij een of meer van de in de AVG gespecificeerde waarborgen of uitzonderingen van toepassing zijn:

<u>Een adequaatheidsbesluit</u>
De Europese Commissie kan derde landen, een gebied en/of specifieke sectoren in derde landen beoordelen en voert zulke beoordelingen ook in de praktijk uit, om vast te stellen of er sprake is van een adequaat beschermingsniveau voor de rechten en vrijheden van natuurlijke personen. Waar dat geval is, is geen autorisatie vereist.
Landen die behoren tot de Europese Economische Ruimte (EER) maar geen lidstaat zijn van de EU, worden geaccepteerd als voldoend aan de voorwaarden voor een adequaatheidsbesluit.
In het Publicatieblad van de Europese Unie worden lijsten gepubliceerd van landen die op dat moment voldoen aan de adequaatheidsvereisten van de Commissie.

<u>Bindende bedrijfsvoorschriften</u>

Sevagram kan een beroep doen op goedgekeurde bindende bedrijfsvoorschriften voor doorgifte van persoonsgegevens naar landen buiten de EU. De voorschriften waar **Sevagram** zich op wil beroepen, moeten dan ter goedkeuring worden voorgelegd aan de relevante toezichthoudende autoriteit.

Modelcontractclausules
Sevagram kan een beroep doen op goedgekeurde modelcontractclausules voor doorgifte van persoonsgegevens naar landen buiten de EER. Als **Sevagram** zich beroept op door de relevante toezichthoudende autoriteit goedgekeurde modelcontractclausules, wordt automatisch uitgegaan van adequaatheid.

Uitzonderingen
Bij ontstentenis van een adequaatheidsbesluit, lidmaatschap van Privacy Shield, bindende bedrijfsvoorschriften en/of modelcontractclausules, is doorgifte van persoonsgegevens naar een derde land of internationale organisatie alleen toegestaan op een van de volgende voorwaarden:

- De betrokkene heeft uitdrukkelijk met de voorgestelde doorgifte ingestemd, na te zijn ingelicht over de risico's die dergelijke doorgiften voor hem kunnen inhouden bij ontstentenis van een adequaatheidsbesluit en van passende waarborgen;
- De doorgifte is noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkene en de verwerkingsverantwoordelijke of voor de uitvoering van op verzoek van de betrokkene genomen precontractuele maatregelen;
- De doorgifte is noodzakelijk voor de sluiting of de uitvoering van een in het belang van de betrokkene tussen de verwerkingsverantwoordelijke en een andere natuurlijke persoon of rechtspersoon gesloten overeenkomst;
- De doorgifte is noodzakelijk wegens gewichtige redenen van algemeen belang;
- De doorgifte is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering; en/of
- De doorgifte is noodzakelijk voor de bescherming van de vitale belangen van de betrokkene of van andere personen, indien de betrokkene lichamelijk of juridisch niet in staat is zijn toestemming te geven.

15. Risico's

Sevagram is zich bewust van de risico's die zijn verbonden aan verwerking van bepaalde typen persoonsgegevens.

Sevagram evalueert het niveau van risico voor betrokkenen dat is verbonden met de verwerking van hun persoonsgegevens. Voor verwerkingen met verhoogd risico worden door Sevagram een gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment, DPIA) uitgevoerd, zoals dat ook gebeurt voor verwerkingen met verhoogd risico die ten behoeve van Sevagram worden uitgevoerd door andere organisaties. Waar deze evaluatieprocessen wijzen op het bestaan van concrete risico's, zal Sevagram er alles aan doen om die risico's te beheersen en de kans op afwijking van dit beleid te reduceren.

Waar een bepaald type verwerking, met name wanneer daarbij nieuwe technologieën worden gebruikt en gelet op aard, reikwijdte, context en doeleinden waarschijnlijk grote risico's voor de rechten en vrijheden van natuurlijke personen met zich meebrengt, zal Sevagram voorafgaand aan feitelijke verwerking een DPIA uitvoeren om de effecten van de voorgenomen verwerking op de bescherming van

persoonsgegevens vast te stellen. Eén DPIA kan daarbij gelden voor een set van gelijksoortige verwerkingen met vergelijkbaar hoog risico.

Waar uit de resultaten van een DPIA duidelijk wordt dat Sevagram op het punt staat een verwerking van persoonsgegevens te starten die ernstige lichamelijke, materiële en/of immateriële schade zou kunnen veroorzaken voor de betrokkenen, moet de beslissing over wel of niet doorgaan van deze verwerking door Sevagram via een escalatieproces worden voorgelegd aan de functionaris voor gegevensbescherming. Als er sprake is van ernstige zorgen, in termen van de ernst van de mogelijke lichamelijke, materiële of immateriële schade of in termen van het aantal betrokkenen, zal de Privacy officer de kwestie via een volgende stap in het escalatieproces voorleggen aan de toezichthoudende autoriteit. Alle passende mechanismen zullen worden geselecteerd en toegepast om het met verwerking van afzonderlijke persoonsgegevens verbonden risico terug te brengen tot een aanvaardbaar niveau, onder verwijzing naar de door Sevagram gedocumenteerde criteria voor risico-acceptatie en de vereisten van de AVG.

Documenteigenaar en Goedkeuring

Het is de verantwoordelijkheid van de Privacy officer, eigenaar van dit document, om ervoor te zorgen dat deze procedure periodiek wordt getoetst in overeenstemming met de voor het AVG-project geldende toetsingsvereisten.

Een actuele versie van dit document is beschikbaar voor alle medewerkers via KISS en wordt gepubliceerd op het intranet.

Bijlage 1: Relevante procedures en beleidstukken inzake Privacy

Naast de genoemde procedures en beleidstukken in het Privacybeleid zijn er nog een aantal andere relevante stukken inzake privacy:

- Procedure behoud van kwaliteit van persoonsgegevens.
- Procedure geautomatiseerde individuele besluitvorming waaronder profilering.
- Procedure gebruik van persoonsgegevens in de onderzoekspraktijk.
- Continuïteitsplan
- Procedure secundair gebruik van persoonsgegevens.
- Procedure training en bewustwording.
- Procedure verwerking van bijzondere persoonsgegevens.
- Procedure beoordeling en rapportage datalekken.
- Camerareglement

Naast deze relevante stukken zijn er ook nog een aantal verplicht op te stellen werkprocessen voor het privacy team. Deze worden enkel opgenomen in de Privacy Manager t.b.v. bewijsvoering en enkel geconsulteerd door de Privacy officer, CISO of functionaris gegevensbescherming indien nodig. Denk hierbij bijvoorbeeld aan een format voor het uitvoeren van een DPIA.