Privacy- en informatiebeveiligingsbeleid

Document gegevens:	
01. Portaal: Cliëntenzorg	N.v.t.
02. Portaal: Medewerkers	N.v.t.
03. Portaal: Gebouwen	N.v.t.
04. Portaal Bedrijfsvoering	4.4 ICT
05. Soort document	Beleid
06. Aantal pagina's (incl. voorblad)	30
07. Status	Definitief
08. Versienummer	Nr: 2.0
09. Datum vaststelling document	Juli 2020
10. Datum evaluatie (uiterlijk vóór...)	Augustus 2023
11. Auteur(s)	Dhr. M. Brouwers, dhr. B. Fastré

Geraadpleegde inhoudsdeskundige:		
01. Naam: dhr. M. Brouwers	Functie: projectleider informatiemanagement	Paraaf:
02. Naam: dhr. B. Fastré	Functie: Functionaris Gegevensbescherming / juridisch adviseur	
03. Naam:	Functie: N.v.t.	N.v.t.

Vaststellen document:		
01. Autorisator (doc. verantwoordelijke)	Dhr. JP. Halmans directeur Finance & Control	Paraaf:
02. Raad van Bestuur	Raad van Bestuur	Paraaf:
03. Centrale Cliëntenraad: Ter informatie	Voorzitter Centrale Cliëntenraad	N.v.t.
04. OR: Instemming	Voorzitter Ondernemingsraad	Paraaf:
05. Manager Marketing, Communicatie en fondsenwerving	Mevr. M. Schmitz	Paraaf:

Inhoudsopgave

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')[1], 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 passend gegevensbeschermingsbeleid te hebben en uit te voeren.[2] Door middel van dit beleidsdocument neemt de Raad van Bestuur haar verantwoordelijkheid ten aanzien van de naleving van de AVG, het aantoonbaar waarborgen van de privacyrechten en het voorzien in passende technische- en organisatorische maatregelen voor de bescherming van (Persoons)gegevens binnen Sevagram. Het privacy- en informatiebeveiligingsbeleid beschrijft de wijze waarop Sevagram uitvoering geeft aan de naleving van de AVG, bescherming van Persoonsgegevens, gegevensbeveiliging evenals welke regels en principes hierbij in acht dienen te worden genomen. Gezien de raakvlakken tussen privacy en informatiebeveiliging zijn beide onderwerpen in dit beleidsdocument gecombineerd.

Op het gebied van informatiebeveiliging hanteert Sevagram de binnen de zorg geldende NEN 7510:2017-norm als uitgangspunt en stelt zij zich ook tot doel het beleid en de uitvoering ten aanzien van dit onderwerp in de nabije toekomst te certificeren. De NEN 7510:2017 vereist een informatiebeveiligingsbeleid (IB-beleid).

Voldoen aan de AVG en aan de NEN 7510:2017 vereist expertise, tijd en aandacht. Het privacy- en informatiebeveiligingsbeleid – en de naleving daarvan - wordt binnen Sevagram daarom ook periodiek geëvalueerd en zo nodig bijgesteld.

Leeswijzer
Lees het document aandachtig en overweeg alle uitgangspunten en regels die hierin beschreven staan. In hoofdstuk 2 worden het doel, de reikwijdte en de definities besproken. Aansluitend wordt in hoofdstuk 3 en hoofdstuk 4 het privacy-/gegevensbeschermingsbeleid in algemene zin respectievelijk het beleid in relatie tot Betrokkenen behandeld. In hoofdstuk 5 wordt vervolgens ingegaan op de Verwerking van Persoonsgegevens door Sevagram, waarbij de categorieën van Persoonsgegevens en de Verwerkingsdoeleinden zijn gespecificeerd. De aanpak is beschreven in hoofdstuk 6 en de verantwoordelijkheden in hoofdstuk 7. Het document sluit af met de kwaliteitsbewaking (hoofdstuk 8), waarin de borging, communicatie en naleving aan bod komen.

[1] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de Verwerking van PersoonsgegevenPersoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).
[2] Artikel 24 lid 2 AVG.

2 Inleiding

Dit beleid gaat over het beschermen van Persoonsgegevens in alle relevante processen van Sevagram. Onder Persoonsgegevens wordt verstaan: alle informatie over of herleidbaar tot een natuurlijk persoon (de Betrokkene). Voor de hand liggende Persoonsgegevens zijn bijvoorbeeld een naam, adres, BSN en een emailadres. Maar bijvoorbeeld kentekengegevens, IP-adressen, foto's, beeld- en (stem)geluidsmateriaal kunnen ook onder Persoonsgegevens worden geschaard. Voor Sevagram betreft dit gegevens van categorieën Betrokkenen zoals cliënten, medewerkers, vrijwilligers, maar ook bezoekers/leveranciers.

2.1 Toepassingsgebied

Dit beleid is van toepassing op de gehele Sevagram-organisatie. Van iedere medewerker (zowel in als buiten loondienst, dus ook onderaannemers en opdrachtnemers/ZZP'ers), vrijwilliger en stagiaire wordt geacht dat hij/zij hieraan voldoet.

2.2 Reikwijdte

Dit privacy- en informatiebeveiligingsbeleid is van toepassing op alle bedrijfsprocessen, informatiesystemen, netwerken, toepassingen, locaties en alle Verwerkingen van Persoonsgegevens van/door Stichting Sevagram Zorgcentra en de daaraan gerelateerde (groeps)entiteiten, waaronder ook Stichting Sevagram Verzorgd Wonen en Stichting Sevagram Verwenzorg.

De AVG is uitsluitend van toepassing op geheel of gedeeltelijke geautomatiseerde Verwerkingen van Persoonsgegevens alsmede op Persoonsgegevens die in een bestand zijn opgenomen of daartoe bestemd zijn.[3]

2.3 Doel

De doelstelling van dit beleid is vierledig:

1. het uitwerken van het toepasselijke beleidskader om huidige en toekomstige vormen van Verwerking van Persoonsgegevens binnen Sevagram te toetsen alsmede taken, bevoegdheden verantwoordelijkheden op het gebied van privacy- en informatiebeveiliging binnen de organisatie te beleggen;
2. het voorzien in een beleidskader voor het treffen, periodiek evalueren en bijstellen van passende technische- en organisatorische maatregelen om (Persoons)gegevens van (Betrokkenen van) Sevagram te beveiligen;
3. het waarborgen van de naleving van de AVG en gerelateerde sectorale privacywetgeving, alsmede;
4. alle Betrokkenen op transparante wijze inzicht bieden in de wijze waarop Sevagram met de Verwerking en beveiliging van Persoonsgegevens evenals met de uitoefening van privacyrechten onder de AVG omgaat.

Het is voor de Raad van Bestuur van essentieel belang dat de bescherming van Persoonsgegevens van cliënten, medewerkers en andere Betrokkenen en informatiebeveiliging is gewaarborgd.

2.4 Planetree

Het welzijn van cliënten staat bij Sevagram voorop en alles staat in het teken van uitstekende mensgerichte zorg. Deze aanpak is gebaseerd op de Planetree-visie en komt in de kern neer op een empathische benadering van onze cliënten, maar ook van de mensen

[3] Artikel 2 lid 1 AVG.

in hun directe omgeving zoals familie, mantelzorgers en vrienden. Goede samenwerking tussen alle belanghebbenden, meer onderling begrip en duidelijke kaders bevorderen betere zorg en helpen een veilige, helende omgeving te creëren die bijdraagt aan de kwaliteit van leven van cliënten. Een veilige omgeving impliceert ook dat Betrokkenen er kunnen van uitgaan dat hun privacy is gewaarborgd en hun Persoonsgegevens optimaal worden beschermd door Sevagram.

2.5 Definities

In dit beleidsstuk worden de navolgende begrippen (aangeduid met een hoofdletter) gehanteerd:

'Beschikbaarheid':
De mate waarin geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot Componenten.

'Betrokkene(n)':
de (levende) natuurlijke perso(o)n(en) waarop Persoonsgegevens betrekking hebben (artikel 4 lid 1 AVG). Bij Sevagram zijn de categorieën Betrokkenen: cliënten, medewerkers, vrijwilligers, stagiaires en leveranciers/bezoekers op wie de verwerkte Persoonsgegevens betrekking hebben.

'CISO':
Concern Information Security Officer; dit is de medewerker die binnen Sevagram verantwoordelijk is voor informatiebeveiliging.

'Component':
Alles wat voor Sevagram een waarde vertegenwoordigt, in de vorm van fysieke objecten of informatie; synoniem met bedrijfsmiddel en asset.

'EU/EEA':
Lidstaten die behoren tot de Europese Unie (EU) / Europese Economische Ruimte (EER: EU + Noorwegen, Zwitserland en Liechtenstein).

'Datalek':
Een Incident of inbreuk in verband met Persoonsgegevens zoals bedoeld in artikel 4 lid 12 AVG. Bij een Datalek kan het gaan om onbevoegde toegang tot of vernietiging, wijziging of vrijkomen van Persoonsgegevens bij een organisatie, ongeacht de intentie daartoe. Onder een Datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige Verwerking van gegevens.

'Derde(n)':
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 (artikel 4 lid 10 AVG).

'DPIA'
Een gegevensbeschermingseffectbeoordeling *('data protection impact assessment')* zoals bedoeld in artikel 35 AVG.

'Dreiging':
De kans dat een bepaald Incident zich voordoet.

‘Eigenaar’, ‘Eigendom’:
Als er wordt gesproken over Eigenaar of Eigendom van een Component, wordt hiermee bedoeld de verantwoordelijkheid voor de verwerking ervan.

‘Functionaris Gegevensbescherming’ (‘FG’):
De Functionaris Gegevensbescherming is een onafhankelijke adviseur en toezichthouder met betrekking tot de naleving van de AVG en nationaalrechtelijke privacyregelgeving. De FG behartigt de belangen van de Betrokkenen en is het eerste aanspreekpunt voor de Autoriteit Persoonsgegevens (AP), de toezichthoudende autoriteit binnen Nederland (artikel 39 AVG).

‘Incident’:
Een gebeurtenis met ongewenste gevolgen; bijvoorbeeld een beveiligingsincident.

‘Integriteit’:
De mate van correctheid en volledigheid van informatie en informatieverwerking.

‘KISS’:
Het interne kennis informatiesysteem van Sevagram, waarin alle procedures en beleidsstukken kunnen worden geraadpleegd waarnaar in dit document wordt verwezen.

‘Risico’:
De combinatie van Dreiging en kwetsbaarheid op een bepaalde Component.

‘Rest-risico’:
Het risiconiveau dat achterblijft na het nemen van maatregelen; de aanname hierbij is dat Risico’s, hoe klein ook, altijd blijven bestaan.

‘Persoonsgegeven(s)’:
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon: 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, identificatienummer, locatiegegevens, online identificator of een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (artikel 4 lid 1 AVG).

‘Sevagram’:
De Stichting Sevagram Zorgcentra en/of de daaraan gelieerde concernentiteiten, waaronder Stichting Sevagram Verzorgd Wonen en Stichting Sevagram Verwenzorg.

‘Vertrouwelijkheid’:
De mate waarin informatie moet worden beschermd tegen ongeautoriseerde openbaarmaking.

‘Verwerking’ of **‘Verwerken’:**
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 (artikel 4 lid 2 AVG).

‘Verwerker’:
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt (artikel 4 lid 8 AVG)

‘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 (artikel 4 lid 7 AVG).

3 Beleid

3.1 Algemeen beleidsuitgangspunt

Het algemeen beleidsuitgangspunt van Sevagram is dat Persoonsgegevens in overeenstemming met de toepasselijke wet- en regelgeving en op behoorlijke en zorgvuldige wijze moeten worden verwerkt.

Sevagram wil een omgeving bieden waarin de privacy van cliënten, medewerkers en andere belanghebbenden wordt geborgd en waarin duidelijk is wat de rechten en plichten zijn van alle partijen. Zowel voor cliënten als voor medewerkers betekent dit dat ze gerust kunnen zijn dat zorgvuldig en discreet met privacygevoelige informatie wordt omgegaan.

Concreet betekent dit dat te allen tijde de toegang tot privacygevoelige informatie is beperkt tot de vastgestelde verantwoordelijken, de cliënt zelf en waar benodigd ondersteunende diensten, zoals technisch beheer en applicatiebeheer.

Een veilige werkomgeving wordt bereikt door samenwerking. Iedereen is verantwoordelijk voor zijn eigen handelen en voor elkaar. Het is daarom van groot belang om elkaar te helpen en elkaar aan te spreken op onveilig gedrag.

3.2 Algemene beginselen en Verwerkingsgrondslagen onder de AVG

De AVG kent een aantal basisregels ('beginselen') die voor iedere Verwerking van Persoonsgegevens van toepassing zijn. Voor de correcte naleving van de AVG is het van belang dat alle medewerkers/vrijwilligers/stagiaires op de hoogte zijn van deze basisregels. Dit betreft:

1. *Rechtmatigheid, behoorlijkheid en transparantie*

   Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de Betrokkene rechtmatig, behoorlijk en transparant is.[4] 'Rechtmatig' wil zeggen dat er altijd een wettelijke grondslag dient te zijn om Persoonsgegevens te Verwerken zoals bedoeld in artikel 6 AVG.

   Op grond van artikel 6 lid 1 AVG is er sprake van zes (limitatieve) wettelijke Verwerkingsgrondslagen, te weten:
   (a) toestemming van Betrokkene, en noodzakelijkheid voor: (b) de uitvoering van een overeenkomst (bijvoorbeeld de zorgleverings-/behandelingsovereenkomst met cliënt), (c) het voldoen aan een wettelijke verplichting (bijvoorbeeld het bijhouden van een dossier op grond van Wet op de geneeskundige behandelovereenkomst), (d) de bescherming van een vitaal belang van Betrokkene (bijvoorbeeld een medische noodsituatie), (e) de vervulling van een algemeen belang of openbaar gezag, dan wel (f) de behartiging van een gerechtvaardigd belang van Sevagram (bijvoorbeeld communicatie, directe marketing of interne kwaliteitsverbetering).

   Ten aanzien van de dienstverlening van Sevagram kunnen, afhankelijk van de Verwerking, alle bovengenoemde grondslagen uit artikel 6 AVG (met uitzondering van de e-grond "algemeen belang of openbaar gezag") van toepassing zijn. De verschillende wettelijke grondslagen die Sevagram hanteert per Verwerking zijn raadpleegbaar in de Privacyverklaring (www.sevagram.nl/privacy).

[4] Artikel 5 lid 1 sub a AVG.

Indien er bijzondere Persoonsgegevens (zoals gezondheidsgegevens van cliënten) worden verwerkt, dient er eveneens een wettelijke uitzonderingrond van toepassing te zijn (op basis van artikel 9 AVG), zoals de uitdrukkelijke toestemming van de Betrokkene/cliënt of de noodzakelijkheid van de Verwerking ten behoeve van gezondheidszorg.[5] Voor wat betreft de Verwerking van gezondheidsgegevens van cliënten door Sevagram als zorgverlener is in de regel de laatstgenoemde uitzonderingsgrondslag van toepassing.

Indien de Verwerking plaats vindt op basis van toestemming van Betrokkene, dan dient deze schriftelijk te worden vastgelegd in een toestemmingsverklaring. Sevagram dient als Verwerkingsverantwoordelijke immers te kunnen aantonen dat rechtsgeldige toestemming is gegeven. Daarbij dient altijd sprake te zijn van geïnformeerde, specifieke, ondubbelzinnige, vrijelijk gegeven toestemming.[6] Ten aanzien van cliënten wordt bij de intake bij Sevagram het algemeen ECD toestemmingsformulier ingevuld en opgeslagen in het elektronisch cliëntendossier. Hierin wordt de vrijelijk gegeven, geïnformeerde toestemming van de cliënt (c.q. vertegenwoordiger) vastgelegd ten aanzien van alle Verwerkingen/aangelegenheden waarbij de cliënt een vrije keuze heeft. In gevallen waarin er geen effectieve keuzevrijheid is, kan toestemming niet als Verwerkingsgrondslag worden gehanteerd. Een gegeven toestemming kan te allen tijde eenvoudig worden ingetrokken. Hierover moet Betrokkene voorafgaand aan het geven van toestemming worden geïnformeerd. Intrekking van toestemming heeft evenwel geen terugwerkende kracht.

Indien een Verwerking rechtmatig is, dient deze tevens 'behoorlijk' te zijn. Dit houdt in dat een Verwerking netjes en verantwoord dient te geschieden.

Het 'transparantiebeginsel' houdt in dat een (zorg)instelling open en transparant moet zijn ten aanzien van de Persoonsgegevens die worden verwerkt en Betrokkenen hierover dienen te worden geïnformeerd.[7]

Sevagram geeft (onder andere) invulling aan de transparantieplicht door middel van het onderhavige privacybeleid[8] alsmede haar Privacyverklaring. Beide documenten zijn publiek toegankelijk en raadpleegbaar online op de website www.sevagram.nl/privacy. [9]

2. *Doelbinding*

Persoonsgegevens mogen enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en mogen vervolgens niet voor (daarmee onverenigbare doelen) verder worden verwerkt.[10]

De wijze waarop Sevagram concreet toepassing geeft aan het principe van doelbinding is uiteengezet in hoofdstuk 5 (onderdeel 5.2 t/m 5.3).

[5] Artikel 9 lid 2 sub a AVG respectievelijk artikel 9 lid 2 sub h AVG.
[6] Artikel 7 AVG.
[7] Artikel 12 en 13 AVG.
[8] Artikel 24 lid 2 AVG.
[9] Artikel 12 en 13 AVG.
[10] Artikel 5 lid 1 sub b AVG. Een doel is enkel 'gerechtvaardigd' indien dit doel kan worden gebaseerd op een wettelijke grondslag uit artikel 6 AVG.

3. *Minimale gegevensbescherming ('dataminimalisatie')*

Persoonsgegevens moeten toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.[11] Een (zorg)instelling mag niet meer Persoonsgegevens verwerken dan noodzakelijk is voor het beoogde doel ('dataminimalisatie'). De Verwerking moet daarnaast de subsidiariteits- en proportionaliteitstoets kunnen doorstaan. [12] Het Verwerken van te veel of onnodige (categorieën van) Persoonsgegevens door een organisatie is onrechtmatig.

Sevagram geeft toepassing aan het principe van dataminimalisatie door bij alle (nieuwe) Verwerkingen van Persoonsgegevens kritisch te evalueren of het beoogde doel ook kan worden bereikt met minder Persoonsgegevens en het proces hierop af te stemmen.

4. *Juistheid*

Persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd. Een (zorg)instelling moet alle redelijke maatregelen nemen om de juistheid van gegevens te controleren en om onjuiste gegevens te wissen of te rectificeren.[13]

Sevagram voert in het licht hiervan periodieke controles uit teneinde te verifiëren of de door haar verwerkte Persoonsgegevens correct zijn.

5. *Opslagbeperking*

Persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de Betrokkene niet langer te identificeren dan voor de Verwerkingsdoeleinden noodzakelijk is.[14] Indien Persoonsgegevens niet meer noodzakelijk zijn (of de wettelijke bewaartermijn is verstreken) dient vernietiging plaats te vinden.

Sevagram geeft toepassing aan het principe van opslagbeperking door een bewaartermijnenbeleid te voeren en te handhaven, waarbij Persoonsgegevens niet langer worden bewaard dan strikt noodzakelijk is voor het beoogde doel. Opslagbeperking in relatie tot het bewaartermijnenbeleid wordt nader behandeld in onderdeel 4.10.

6. *Integriteit, Beschikbaarheid en Vertrouwelijkheid ('BIV')*

Een (zorg)instelling dient passende beveiligingsmaatregelen te treffen teneinde Persoonsgegevens voldoende te beveiligen tegen ongeoorloofde of onrechtmatige Verwerking en tegen (on)opzettelijk(e) inzage, verlies, vernietiging of beschadiging.[15]

De wijze waarop de Integriteit, Beschikbaarheid en Vertrouwelijkheid van (persoons)gegevens wordt gewaarborgd binnen Sevagram, is nader uiteengezet in hoofdstuk 5 t/m 8.

[11] Artikel 5 lid 1 sub c AVG.
[12] Dit wil zeggen dat de inbreuk op de belangen van Betrokkenen niet onevenredig mag zijn in verhouding tot het te dienen doel van de Verwerking en dit doel in redelijkheid niet op een andere, voor de Betrokkene minder nadelige wijze kan worden bereikt.
[13] Artikel 5 lid 1 sub d AVG.
[14] Artikel 5 lid 1 sub e AVG.
[15] Artikel 5 lid 1 sub f AVG.

Alle (nieuwe) Verwerkingen van Persoonsgegevens binnen Sevagram dienen verenigbaar te zijn met bovengenoemde wettelijke criteria. De wijze waarop hieraan nadere invulling wordt gegeven door Sevagram wordt beschreven in de hierna volgende hoofdstukken.

3.3 Randvoorwaarden

- Sevagram voert een actief beleid om het beveiligingsbewustzijn van eenieder die werkzaamheden verricht in naam van Sevagram te stimuleren. Medewerkers worden onder meer door interactieve *wallpapers*, presentaties en nieuwsbrieven periodiek geïnformeerd over actuele onderwerpen op het gebied van privacy en informatiebeveiliging, zoals *phishing* en toegang tot cliëntinformatie.
- Sevagram hanteert een gedegen inwerkprogramma voor al haar medewerkers met aandacht voor de omgang met privacygevoelige informatie. Concreet dienen alle medewerkers van Sevagram bij indiensttreding een verplichte e-learningmodule “informatiebewust werken” over privacy- en informatiebeveiliging te doorlopen. De teammanager ziet erop toe dat dat alle medewerkers binnen zijn/haar team deze e-learning zo snel mogelijk na datum indiensttreding hebben afgerond.
- Sevagram hanteert een ‘*clean desk, clear screen*’ beleid. Accounts worden na verloop van een bepaalde periode automatisch geblokkeerd en medewerkers dienen bij het verlaten van hun werkplek hun account te vergrendelen. Dit wordt steekproefsgewijs gecontroleerd.
- Het raadplegen van cliëntgegevens of inloggen in de beveiligde omgeving van Sevagram van buitenaf kan enkel door middel van 2-factor-authentificatie.
- Sevagram hanteert een beleid inhoudende dat alle cliëntgegevens in de daarvoor bestemde cliëntinformatiesystemen, zoals het elektronisch patiëntdossier of medicatiedossier, worden verwerkt.
- Sevagram hanteert een beleid dat alle gegevens van medewerkers eveneens in specifieke beveiligde HR-informatiesystemen worden verwerkt.
- Uitganspunt is dan ook dat Persoonsgegevens van cliënten en medewerkers in beginsel niet worden opgeslagen in netwerkmappen (G:schijf), teneinde Datalekken te voorkomen.
- Er wordt geen vertrouwelijke informatie op verwijderbare media zoals USB-sticks opgeslagen. De opslag op externe gegevensdragers is om die reden ook technisch uitgeschakeld.
- De ICT-afdeling draagt zorg voor het ter beschikking stellen van de benodigde ICT-middelen en de beveiliging daarvan.

3.5 Doelstellingen

Belangrijk voor Sevagram is dat privacy en informatiebeveiliging de primaire (zorg)processen en organisatiedoelstellingen ondersteunt. Hierbij staan de cliënt en de medewerker steeds centraal.
De uitkomst hiervan is:

- het voldoen aan randvoorwaardelijke eisen van privacy en informatiebeveiliging. Verlies van Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie vergroot de kans op Incidenten en Datalekken;
- vertrouwen bieden in een zorgvuldige omgang met privacygevoelige informatie;
- het voldoen aan relevante wet- en regelgeving;
- het beschermen en versterken van de reputatie op het gebied van privacy en informatiebeveiliging;
- het voldoen aan interne kwaliteitseisen;
- het stimuleren van een verantwoordelijke en transparante organisatiecultuur waarin Incidenten en Datalekken tijdig ontdekt, gemeld en afgehandeld worden;

- het zorgdragen dat tekortkomingen afgehandeld worden;
- de privacy van de informatie van cliënten waarborgen;
- het zorg dragen voor bescherming van de informatie en haar onderliggende systemen tegen (cyber)criminaliteit;
- het zorg dragen dat kwetsbaarheden worden geïdentificeerd en worden weggenomen;
- het zorg dragen dat informatiesystemen te allen tijde up-to-date zijn;
- het zorg dragen voor de Beschikbaarheid van de informatiesystemen;
- het de privacy van de personeelsinformatie waarborgen;
- het zorg dragen dat de medewerkers adequaat zijn getraind om de aan haar toegewezen privacy-taken en -verantwoordelijkheden te kunnen voldoen en veilig kunnen werken;
- het zorgdragen dat medewerkers geschikt zijn voor de functie die ze (zullen gaan) vervullen.

De Raad van Bestuur draagt het beleid actief uit en verwacht van alle medewerkers dat zij dat ook doen en iedereen zijn verantwoordelijkheid daarin neemt.

4 Beleidskaders richting de Betrokkenen

4.1 Vertrouwen en veiligheid

Vertrouwen is de basis om met medewerkers, relaties en partners samen te werken. Dit vertrouwen vraagt om openheid van Sevagram over de gegevens die Sevagram van de medewerkers en relaties vraagt. Maar ook om de veiligheid van diezelfde gegevens bij Sevagram als werkgever of aanbieder van producten en diensten. Sevagram gaat daarbij zorgvuldig om met gegevens en zorgt voor een passend niveau van beveiliging en zorgt er voor dat elke Verwerking van gegevens voldoen aan de toepasselijk wet- en regelgeving.

4.2 Informatiebeveiliging in relatie tot privacy

Informatie, informatiesystemen, toepassingen en netwerken dienen in voldoende mate beschikbaar te zijn, dienen volledige en juiste informatie te bevatten en dienen uitsluitend toegankelijk voor rechtmatige gebruikers te zijn. De informatie, informatiesystemen, toepassingen en netwerken moeten in staat zijn bedreigingen voor hun Beschikbaarheid, Integriteit en Vertrouwelijkheid te weerstaan en moeten zich bij het optreden van Incidenten en calamiteiten kunnen herstellen.

Om hieraan te kunnen voldoen zal Sevagram het volgende doen:

- alle Componenten op het gebied van hardware, software en informatie die onder het beheer vallen, beschermen. Dit wordt bereikt door het implementeren en beheren van een uitgebalanceerd pakket technische- en organisatorische beveiligingsmaatregelen.
- in verhouding tot de risico's voor de diverse Componenten effectieve en efficiënte beveiliging bieden.
- het beleid op een consistente, tijdige, effectieve en efficiënte manier implementeren en beheren.
- voor alle bedrijfskritische informatiesystemen, toepassingen en netwerken een systeembeveiligingsbeleid opstellen. Hierin komen aan bod:
  - de autorisaties voor het gebruik van het systeem;
  - een beschrijving van beveiligingsmaatregelen die van toepassing zijn op het systeem;
  - de verantwoordelijkheden en bevoegdheden voor het systeem;
  - een continuïteitsplan voor het systeem.
- zich inspannen om de medewerkers (de gebruikers van informatiesystemen, toepassingen en netwerken) uitleg te geven over beveiliging en hun verantwoordelijkheden en om het noodzakelijke beveiligingsbewustzijn onder de medewerkers te creëren. Medewerkers moeten hiertoe o.a. via het Leerportaal een verplichte interactieve informatiemodule doorlopen. Tevens zullen zij bij implementatie van nieuwe systemen (met Persoonsgegevens) getraind worden in eigenlijk gebruik (*Privacy by Design*). Voor dagelijkse ondersteuning en vragen kunnen zij zich wenden tot de Functionaris Gegevensbescherming of de PrivacyDesk (in TOP-desk).
- Aan alle medewerkers duidelijk maken dat onverantwoorde en/of ongepaste daden tot disciplinaire maatregelen kunnen leiden, zoals ook beschreven in de gedragscode voor medewerkers, te vinden in KISS in het document met naam 'RICH-Gedragscode (Versie 1)'.

Waar van toepassing zal Sevagram zich houden aan:

- De Nederlandse en Europese wet- regelgeving;
- De gedrags- en beroepsregels van de beroepsorganisaties van de medewerkers;
- De gedrags- en fatsoensnormen van het maatschappelijk verkeer.

4.3 Gegevens en privacy

Dit beleid is van toepassing op alle (Persoons)gegevens van cliënten, medewerkers en relaties die Sevagram verzamelt en verwerkt. Sevagram is de Verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens zoals beschreven in dit beleid.

4.3.1 Doeleinden jegens Betrokkenen

Sevagram hecht veel waarde aan de bescherming van uw privacy. Betrokkenen kunnen erop vertrouwen dat Sevagram:

- werkt naar de letter en geest van de privacywet- en regelgeving;
- gegevens veilig en zorgvuldig verwerkt;
- gegevens niet doorgeeft of verkoopt aan derden voor commerciële of charitatieve doeleinden;
- uw rechten respecteert;
- alleen samenwerkt met partijen die dezelfde uitgangspunten hanteren;
- vragen over privacy transparant en eerlijk zal beantwoorden.

4.4 Geheimhouding

Medewerkers, vrijwilligers en stagiaires van Sevagram hebben de plicht tot geheimhouding van alle vertrouwelijke informatie, bedrijfsgegevens, Persoonsgegevens of informatie van cliënten, waarvan zij uit hoofde van hun functie kennis hebben gekregen en waarvan zij weten of redelijkerwijs moeten weten tot geheimhouding daarvan gehouden te zijn.

Alle medewerkers in loondienst van Sevagram zijn op basis van hun arbeidsovereenkomst (contractueel) gehouden tot geheimhouding. BIG-geregistreerde medewerkers zijn daarnaast ook gehouden aan een wettelijke geheimhoudingsplicht op grond van (artikel 88) van de Wet op de beroepen in de individuele gezondheidszorg ('Wet BIG').

Ten aanzien van vrijwilligers en stagiaires wordt de Vertrouwelijkheid/geheimhouding eveneens contractueel door Sevagram geborgd. Externe medewerkers - zoals onderaannemers, ZZP'ers, vrijwilligers en stagiaires - dienen voor de aanvang van hun werkzaamheden een geheimhoudingsverklaring te tekenen.

Bij de inschakeling van leveranciers / onderaannemers of de samenwerking met ketenpartners (bijvoorbeeld externe zorgverleners zoals apotheken) worden contractuele afspraken gemaakt over geheimhouding en de naleving van de AVG. Een en ander vindt ook uitdrukking in de gedragscode voor externe partijen (KISS RICH-Gedragscode voor externe partijen).

4.5 Integriteitsscreening / VOG

Sevagram verwerkt als zorginstelling ook bijzondere Persoonsgegevens (gezondheidsgegevens) van een kwetsbare doelgroep (ouderen). Om reden stelt Sevagram hoge eisen aan de Integriteit van haar medewerkers en vindt er ook een Integriteitsscreening plaats.

Alle medewerkers, en vrijwilligers dienen voor indiensttreding een geldige en originele Verklaring Omtrent Gedrag ('VOG') voor te kunnen leggen.[16] De VOG-verplichting is opgenomen als ontbindende voorwaarde in de standaard arbeidsovereenkomst en vrijwilligersovereenkomst van Sevagram. Het integrale VOG-Beleid van Sevagram is

[16] Voor medewerkers die woonachtig zijn in andere landen geldt het equivalent van de Nederlandse VOG in dat betreffende land. Voor medewerkers die wonen in België is dat het "Uittreksel uit het Strafregister" respectievelijk voor medewerkers die wonen in Duitsland de 'Führungszeugnis'.

opgenomen in het beleidsstuk "BELEI-Verklaring omtrent gedrag" in KISS. In sommige gevallen kan, afhankelijk van de werkzaamheden, ook een VOG-verplichting van toepassing zijn ten aanzien van stagiaires.

Bij de aanwerving van nieuw zorgpersoneel heeft Sevagram als zorginstelling voorts een wettelijke 'vergewisplicht' op grond van de Wkkgz. Dit houdt in dat Sevagram voorafgaand aan de indiensttreding van een zorgmedewerker onderzoek doet naar het arbeidsverleden van de sollicitant en beoordeelt of deze geschikt is om zorg te verlenen. Indien een aankomende medewerker / sollicitant weigert hieraan medewerking te verlenen, vormt dit in beginsel voor Sevagram een beletsel voor indiensttreding.

4.6 Inzage in (cliënt)gegevens (autorisatie) / toegang tot elektronische cliëntendossiers

Het algemene beleidsuitgangspunt van Sevagram is dat medewerkers enkel toegang mogen c.q. kunnen hebben tot informatie/(Persoons)gegevens die noodzakelijk zijn voor de uitvoering van de aan hen opgedragen werkzaamheden *(*het zogenaamde *"need to know"*-principe).

Gebruikte ICT-systemen / applicaties worden om die reden binnen Sevagram dusdanig ingericht dat het *"need to know"*-principe reeds zo veel mogelijk technisch wordt afgedwongen.

Sevagram hanteert een autorisatiematrix waarin is vastgelegd welke medewerkers (welke functies) toegang hebben tot welke applicaties en (Persoons)gegevens (functieautorisatie en typeautorisatie).

Wat betreft toegang van medewerkers tot (Persoons)gegevens van cliënten in gedigitaliseerde dossiers (elektronische cliëntendossiers), hanteert Sevagram het wettelijk uitgangspunt dat inzage alleen is toegestaan indien en voor zover (cumulatief):

1. een medewerker rechtstreeks betrokken is bij de behandeling van c.q. zorgverlening aan de cliënt (en/of bij de beheersmatige/administratieve afwikkeling van die behandeling/zorgverlening), én;

2. de toegang beperkt blijft tot gegevens die noodzakelijk zijn voor de uitvoering van de taken van die medewerker.[17]

Om dit te kunnen waarborgen treft Sevagram passende technische en organisatorische maatregelen op het gebied van toegangsverlening aan medewerkers tot gegevens in gedigitaliseerde cliëntendossiers, waarbij als 'passend' eveneens de maatregelen uit de NEN 7510 (en NEN7513) als maatstaf gelden. Concreet voert Sevagram daartoe het volgende beleid:

- medewerkers ontvangen een (voorafgaande) training met betrekking tot applicaties (elektronisch cliëntendossier) waarin cliëntgegevens worden verwerkt;
- de autorisatie van een (zorg)medewerker tot een applicatie / elektronisch cliëntendossier wordt enkel op verzoek van diens leidinggevende (team manager) verstrekt;
- medewerkers worden uitsluitend geautoriseerd voor de elektronische dossiers van (groepen van) cliënten waarmee zij rechtstreeks een zorg- of behandelrelatie hebben. Daarbij is er sprake van een autorisatie op het niveau van de (groep) cliënten waarmee er een zorg/behandelrelatie is (doorgaans op locatiebasis)

[17] Artikel 7:457 lid 1 en lid 2 BW (WGBO) jo. artikel 32 AVG.

evenals een functieautorisatie (inhoudende dat medewerkers enkel toegang hebben tot de voor hun werkzaamheden relevante Persoonsgegevens);
- er is een 'noodknopprocedure' die toegang geeft tot (bepaalde) niet-geautoriseerde gegevens om de veiligheid van de zorg/behandeling van cliënten te kunnen waarborgen. Medewerkers dienen daarbij altijd een reden op te geven voor het gebruik van de 'noodknop', op basis waarvan de rechtmatigheid van de inzage (achteraf) kan worden gecontroleerd';
- er vindt *logging* plaats op acties van medewerkers in elektronische patiëntendossiers;
- logbestanden worden periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik (zoals onbevoegde inzage) van Persoonsgegevens en waar nodig wordt actie ondernomen;
- Gezien het belang van Vertrouwelijkheid, Integriteit en het (medische) beroepsgeheim tilt Sevagram zwaar aan onbevoegde/onrechtmatige inzage in elektronische cliëntendossiers. Onbevoegde inzage in (of onrechtmatig gebruik van) gegevens in elektronische cliëntendossiers kwalificeert volgens de vaste jurisprudentie als ernstig verwijtbaar handelen en kan daarom een grondslag vormen voor een ontslag (op staande voet) en/of tuchtrechtelijke sancties (in geval van BIG-geregistreerde medewerkers).[18] Afhankelijk van de omstandigheden van het geval kan in dergelijk geval door Sevagram aan een in overtreding zijnde medewerker een sanctie opgelegd worden variërend van een officiële waarschuwing tot ontslag op staande voet.

4.7 Verwerkers

Sevagram schakelt bij de uitvoering van haar bedrijfsprocessen / dienstverlening ook derden in. Voor zover deze derden bij het uitvoeren van de betreffende diensten en bedrijfsactiviteiten Persoonsgegevens Verwerken, doen zij dit in hoedanigheid van Verwerker voor Sevagram. Persoonsgegevens mogen in dat geval enkel op instructie van Sevagram, voor doeleinden van Sevagram (en niet voor andere/onverenigbare doeleinden) door de Verwerker worden verwerkt. Hierover maakt Sevagram contractuele afspraken met alle Verwerkers in de vorm van zogenaamde 'Verwerkersovereenkomsten'. Daarin worden onder andere afspraken vastgelegd over geheimhouding en over de minimale technische- en organisatorische maatregelen die een Verwerker moet treffen.

Sevagram werkt uitsluitend samen met Verwerkers die de AVG naleven en passende technische- en organisatorische maatregelen treffen om een adequaat informatiebeveiligingsniveau te kunnen waarborgen. Opslag van Persoonsgegevens (server/cloudopslag) door Verwerkers (of subverwerkers) – met name gezondheidsgegevens van cliënten - dient in de regel plaats te vinden binnen de EU/EEA. Opslag op servers buiten de EU/EEA is uitsluitend toegestaan in geval van voorafgaande schriftelijke toestemming van Sevagram. Hetzelfde geldt voor andere vormen van doorgifte van persoonsgegevens naar landen buiten de EU/EEA of aan internationale organisaties. Laatstbedoelde toestemming zal door Sevagram enkel worden verleend indien er sprake is van een geldig doorgiftemechanisme zoals bedoeld in hoofdstuk 5 AVG én indien er in betreffende land *de* facto sprake is van een adequaat beschermingsniveau.

4.8 Doorgifte van Persoonsgegevens aan Derden

Indien daartoe een wettelijke grondslag bestaat - zoals een wettelijke verplichting, een overeenkomst of toestemming van Betrokkene[19] - kunnen Persoonsgegevens door Sevagram

[18] Zie o.a: Gerechtshof Amsterdam, 6 februari 2018, ECLI:NL:GHAMS:2018:409.
[19] Artikel 6 lid 1 AVG.

worden doorgegeven aan de volgende categorieën Derden:

- het zorgkantoor;
- het Centrum voor Indicatiestelling Zorg ('CIZ');
- zorgverzekeraars;
- gemeenten;
- de belastingdienst;
- bedrijfsartsen/arbodienst;
- apotheken;
- ziekenhuizen;
- huisartsen;
- tandartsen;
- overige medische specialisten/externe behandelaren/zorginstellingen;
- leveranciers/onderaannemers;
- opleidingsinstituten.

Digitale verzending van Persoonsgegevens aan Derden vanuit Sevagram dient altijd plaats te vinden via beveiligde e-mail.

Persoonsgegevens zullen door Sevagram (behoudens uitdrukkelijke toestemming van Betrokkene) nooit worden 'verkocht' of doorgegeven aan Derden voor louter commerciële of charitatieve doeleinden.

4.9 Beveiliging van gegevens

Sevagram treft passende – op het risico afgestemde – technische en organisatorische maatregelen om (Persoons)gegevens voldoende te beveiligen tegen inbreuken op de Beschikbaarheid, Integriteit en Vertrouwelijkheid, teneinde Incidenten/Datalekken te voorkomen. Sevagram beveiligt haar systemen en applicaties volgens de geldende standaarden voor informatiebeveiliging. Getroffen beveiligingsmaatregelen worden periodiek geëvalueerd en zo nodig bijgesteld, onder andere aan de hand van interne en externe beveiligingsaudits.

4.10 Opslagbeperking en bewaartermijnen

Uitgangspunt binnen Sevagram is dat Persoonsgegevens worden bewaard voor zo lang dat noodzakelijk is voor het beoogde doel. In gevallen waarin een wettelijke bewaartermijn van toepassing is, geldt deze wettelijke termijn als (uiterlijke) bewaartermijn. In gevallen waarin geen wettelijke bewaartermijn geldt, hanteert Sevagram een intern vastgestelde bewaartermijn.

Sevagram beschikt over een beleidsdocument "overzicht bewaartermijnen" (zie: KISS), waarin de wettelijke c.q. binnen de organisatie intern gehanteerd bewaartermijn per categorie document/(Persoons)gegevens is vastgesteld. Dit overzicht wordt periodiek geactualiseerd. De meest voorkomende (wettelijke) bewaartermijnen binnen Sevagram zijn als volgt:

- (Persoons)gegevens uit het medisch/zorgdossier van de cliënt worden op grond van de WGBO bewaard gedurende 20 jaar[20] na afsluiting van de behandeling/zorg;
- financiële gegevens worden bewaard gedurende de fiscale bewaartermijn van 7 jaar;

[20] Voor dossiers die zijn afgesloten op uiterlijk 31 december 2019, geldt nog de oude WGBO-bewaartermijn van 15 jaar.

- camerabeelden (beveiligingscamera's) worden bewaard gedurende 4 weken na vervaardiging van de beelden;
- loonbelastingverklaringen en kopieën van identiteitsbewijzen (medewerkers/bezoldigde stagiaires) bewaart Sevagram gedurende 5 jaar na het einde van de arbeidsovereenkomst/stageovereenkomst;
- gegevens van sollicitanten (CV, sollicitatiebrief, referenties, correspondentie) bewaart Sevagram tot 4 weken na afloop van de sollicitatieprocedure. Met toestemming van de sollicitant kunnen de gegevens tot een jaar bewaard worden na afronding van de sollicitatieprocedure.

Na het verstrijken van de bewaartermijn worden de betreffende (Persoons)gegevens in beginsel onherroepelijk verwijderd. In sommige gevallen kan Sevagram evenwel een gerechtvaardigd belang[21] hebben om bepaalde (Persoons)gegevens langer te bewaren, bijvoorbeeld om verweer te kunnen voeren in een gerechtelijke procedure. In dat geval worden deze gegevens bewaard voor zolang noodzakelijk is voor de behartiging van dit gerechtvaardigd belang.

4.11 Melding, registratie en afhandeling van Incidenten / Datalekken

Incidenten of Datalekken dienen onverwijld (direct na ontdekking) te worden gemeld bij de Privacydesk van Sevagram via het formulier "Melding Datalek" in Topdesk of door verzending van dit formulier per e-mail aan: Privacydesk@sevagram.nl.

Incidenten kunnen worden gemeld door een Betrokkene, een Verwerker of een Derde.

Van alle Datalekken die een waarschijnlijk risico inhouden voor de rechten en vrijheden van de Betrokken natuurlijke personen, zal door Sevagram op grond van artikel 33 AVG een melding worden gemaakt bij de Autoriteit Persoonsgegevens.

Van ieder Incident / Datalek, de afhandeling daarvan inclusief de eventueel te nemen (mitigerende) maatregelen en analyse ten aanzien van de wettelijke AVG-meldingsplicht (Datalekken) wordt een nauwgezette registratie bijgehouden ('datalekkenregister'). Sevagram hecht er belang aan dat de organisatie leert van gemaakte fouten en dat herhaling van Datalekken / Incidenten zo veel mogelijk wordt voorkomen. Om die reden wordt ieder Datalek geanalyseerd en worden er op basis daarvan zo mogelijk interne verbetermaatregelen ontwikkeld en uitgevoerd.

De volledige procedure ten aanzien van de melding, registratie en afhandeling van Incidenten / Datalekken is raadpleegbaar in het document "PROC Meldplicht Datalekken" in KISS.

4.12 Rechten van Betrokkenen

Betrokkenen hebben een aantal rechten met betrekking tot hun Persoonsgegevens. Sevagram stelt alles in het werk zodat Betrokkene(n) hun rechten onder de AVG eenvoudig en effectief kunnen uitoefenen.

Betrokkenen hebben op grond van de AVG:
- recht op (transparante) informatie met betrekking tot de verwerking van persoonsgegevens;
- recht op inzage in - en afschrift van - de door Sevagram van Betrokkene(n) verwerkte Persoonsgegevens, zoals vastgelegd in KISS in de procedures 'RICH-Inzagerecht voor cliënten (Versie 1)' en 'RICH-Inzagerecht voor medewerkers (Versie 1)'. Het eerste

[21] In de zin van artikel 6 lid 1 sub f AVG.

(digitale) afschrift wordt door Sevagram kosteloos verstrekt. Teneinde eenvoudige inzage door cliënten / vertegenwoordigers (curator, mentor en desgewenst contactpersoon / familie) in het elektronisch cliëntendossier maximaal te faciliteren, biedt Sevagram kosteloze digitale inzage door middel van het cliëntportaal "Mijn Sevagram". Het aanvraagformulier voor toegang tot het cliëntportaal kan via een zorgmedewerker worden verkregen;
- recht op rectificatie van persoonsgegevens;
- recht om vergeten te worden ('gegevenswissing' of 'vergetelheid');
- recht van bezwaar;
- recht van beperking van Verwerking;
- recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming/profilering;
- recht om elektronisch verwerkte Persoonsgegevens over te dragen ('dataportabiliteit').

Bovengenoemde AVG-rechten zijn niet absoluut. Sevagram beoordeelt per verzoek of aan de wettelijke voorwaarden voor toewijzing wordt voldaan. Voor toewijzing van het verzoek is noodzakelijk dat de verzoekende Betrokkene zich voorafgaand (in persoon) legitimeert.

Sevagram verstrekt geen gegevens telefonisch of via e-mail zonder zeker te stellen dat Betrokken in voldoende mate kan worden geïdentificeerd.

Een verzoek van een Betrokkene tot uitoefening van bovengenoemde AVG-rechten kan worden gericht aan de Privacydesk:
- Per e-mail: Privacydesk@sevagram.nl;
- Telefonisch via:
  - 088-9912208 voor medewerkers (bereikbaar op maandag t/m donderdag tijdens kantooruren);
  - 0900-7774777 voor andere Betrokkenen;
- In geval van medewerkers, een TOPdesk melding registreren (op naam van de PrivacyDesk);
- Inzageverzoeken van cliënten in het eigen (elektronische) cliëntdossier / cliëntportaal kunnen ook eenvoudig rechtstreeks worden aangevraagd bij de zorg/team manager van de locatie.

Binnen een maand na ontvangst van het verzoek zal Betrokkene worden geïnformeerd over het gevolg dat door Sevagram aan het verzoek wordt gegeven. Deze termijn kan door Sevagram zo nodig 2 keer met telkens een maand worden verlengd. Bij verlenging van deze termijn zal Sevagram Betrokken altijd binnen een maand na ontvangst van het verzoek in kennis stellen.[22]

Klachten met betrekking tot de verwerking van persoonsgegevens door Sevagram of ten aanzien van de uitvoering van bovengenoemde AVG-rechten kunnen door Betrokkene(n) (vertrouwelijk) worden ingediend bij de Functionaris Gegevensbescherming van Sevagram:

- Telefonisch: (045) 560 28 05;
- E-mail: FG@sevagram.nl.

[22] Artikel 12 lid 3 AVG.

5 Verwerking van Persoonsgegevens door Sevagram

In dit hoofdstuk wordt per categorie Betrokkenen – te weten: cliënten, medewerkers/stagiaires/vrijwilligers – uiteengezet welke categorieën Persoonsgegevens door Sevagram worden verwerkt voor welke doeleinden.

5.1 Categorieën Persoonsgegevens die door Sevagram worden verwerkt

Hieronder wordt per categorie Betrokkenen benoemd welke Persoonsgegevens door Sevagram worden verwerkt.

5.1.1 Verwerkte Persoonsgegevens van cliënten

Sevagram verwerkt de navolgende categorieën Persoonsgegevens van cliënten:

- NAW gegevens (voornaam, achternaam en adresgegevens);
- contactgegevens (telefoonnummer en e-mailadres);
- contactgegevens (NAW, e-mailadres en telefoonnummer) van de 1e contactpersoon en (indien van toepassing) de wettelijke vertegenwoordiger/mentor/bewindvoerder;
- BSN-nummer;
- geslacht;
- geboortedatum;
- nationaliteit;
- burgerlijke staat;
- documentnummer identiteitsbewijs (er wordt geen kopie/scan gemaakt/bewaard);
- rekeningnummer;
- gezondheidsgegevens / medische gegevens;
- verzekeringsgegevens;
- foto (enkel voor in het elektronisch cliëntendossier t.b.v. identificatiedoeleinden)
- eventuele camerabeelden (enkel ten behoeve van beveiligingsdoeleinden en/of zorgverlening/zorgtechnologie, indien en voor zover van toepassing);

Persoonsgegevens van cliënten worden in de regel rechtstreeks door Sevagram bij betreffende cliënten opgevraagd. Indien een cliënt wordt doorgestuurd naar Sevagram vanuit een externe zorgverlener (bijvoorbeeld het ziekenhuis of een andere zorginstelling) vindt er doorgaans (met toestemming van de cliënt) een dossieroverdracht plaats, waarbij de noodzakelijke Persoonsgegevens worden uitgewisseld.

5.1.2 Verwerkte Persoonsgegevens van medewerkers en stagiaires

Sevagram verwerkt de volgende Persoonsgegevens van haar medewerkers en stagiaires:

- NAW-gegevens (voornaam, achternaam en adresgegevens)
- BSN-nummer;
- geslacht;
- geboortedatum;
- geboorteplaats/land;
- nationaliteit;
- e-mailadres(sen);
- telefoonnummer(s);
- bankrekeningnummer;
- kopie identiteitsbewijs;
- verklaring omtrent gedrag ('VOG');
- burgerlijke staat;
- eventuele partnergegevens, indien er een partnerpensioen is (werknemers);

- eventuele gegevens van kinderen, indien er een wezenpensioen is (werknemers);
- inkomensgegevens (zoals salarisstrookjes en jaaropgaves) en eventuele uitkeringsgegevens (werknemers);
- opleidingsgegevens;
- gegevens in het kader van functioneren en beoordeling;
- eventuele gegevens met betrekking tot een mogelijke aanvraag voor zwangerschapsverlof, ouderschapsverlof of onbetaald verlof (werknemers);
- verzuimfrequentie;
- (profiel)foto (enkel ten behoeve van identificatiedoeleinden / medewerkerspas);
- eventuele camerabeelden (enkel ten behoeve van beveiligingsdoeleinden of zorgverlening/zorgtechnologie);
- eventuele kentekens (uitsluitend parkings P1, P2 en P3 Henri Dunantstraat 3 Heerlen).

5.1.3 Verwerkte Persoonsgegevens van vrijwilligers

Van vrijwilligers verwerkt Sevagram de volgende Persoonsgegevens:

- voor- en achternaam;
- adresgegevens;
- geslacht;
- geboortedatum;
- geboorteplaats/land;
- nationaliteit;
- e-mailadres(sen);
- telefoonnummer(s);
- bankrekeningnummer (enkel bij Verwerking onkostendeclaraties);
- verklaring omtrent gedrag ('VOG');
- gegevens over functioneren;
- burgerlijke staat / eventuele partnernaam (enkel t.b.v. aanspreking);
- eventuele (profiel)foto (enkel ten behoeve van identificatiedoeleinden / vrijwilligerspas);
- eventuele camerabeelden (enkel ten behoeve van beveiligingsdoeleinden);
- eventuele kentekens (uitsluitend parkings P1, P2 en P3 Henri Dunantstraat 3 Heerlen).

Persoonsgegevens van medewerkers, stagiaires en vrijwilligers worden in de regel rechtstreeks bij deze Betrokkenen opgevraagd.

Sevagram verwerkt in beginsel geen gezondheidsgegevens of gegevens van strafrechtelijke aard (met uitzondering van de VOG) met betrekking tot medewerkers, stagiaires of vrijwilligers.

5.2 Doeleinden waarvoor Sevagram Persoonsgegevens verwerkt

Hieronder wordt per categorie Betrokkenen benoemd voor welke doeleinden Persoonsgegevens worden verwerkt:

5.2.1 Doeleinden Verwerking Persoonsgegevens cliënten

Persoonsgegevens van cliënten worden door Sevagram verwerkt voor de volgende doeleinden:

- het uitvoeren van de tussen de cliënt en Sevagram gesloten zorg- of behandelingsovereenkomst inclusief bijbehorende zorg/behandelplan;

- bedrijfsvoering en administratieve afwikkeling van de behandeling/zorg die Sevagram biedt, door middel van onder andere intern systeembeheer, het aanvragen van een indicatie bij het Centrum voor Indicatiestelling Zorg ('CIZ'), het declareren van zorg bij het zorgkantoor (CZ), de gemeente of de ziektekostenverzekeraar;
- het voldoen aan wettelijke verplichtingen die op Sevagram (als zorginstelling) rusten op grond van onder andere (niet limitatief):
    - de Wet op de geneeskundige behandelovereenkomst ('WGBO'): bijvoorbeeld de verplichting tot het bijhouden van een patiëntendossier gedurende de wettelijke termijn;
    - de Wet kwaliteit, klachten en geschillen zorg ('Wkkgz'): bijvoorbeeld behandeling van Incidenten en klachten, kwaliteitsbewaking- en verbetering;
    - de Wet langdurige zorg ('Wlz'), Zorgverzekeringswet ('Zvw'), Wet maatschappelijke ondersteuning ('WMO'): bijvoorbeeld de uitwisseling van Persoonsgegevens met het CIZ, zorgverzekeraars en gemeentes;
    - de Wet aanvullende bepalingen Verwerking Persoonsgegevens in de zorg ('Wabvpz'), bijvoorbeeld: identificatieplicht en gebruik van het BSN-nummer in de zorg;
    - de Wet zorg en dwang ('Wzd'): bijvoorbeeld vastlegging stappenplan bij de toepassing van onvrijwillige zorg.
- het bieden van meer bewegingsvrijheid en levenscomfort voor cliënten door de inzet van zorgtechnologie/domotica (met toestemming van de cliënt/vertegenwoordiger);
- het kunnen contacteren van de cliënt (en diens contactpersoon en/of vertegenwoordiger) en de beantwoording van vragen;
- de behartiging van gerechtvaardigde belangen van Sevagram, zoals:
    - communicatie en marketing: het informeren van cliënten over de dienstverlening van Sevagram, bijvoorbeeld door nieuwsbrieven evenals het aanbieden van eventuele aanvullende diensten en producten;
    - (niet wettelijk verplichte) interne audits, interne kwaliteitsverbetering, opleidingsdoeleinden en cliënttevredenheidsonderzoek;
    - raadpleging van het cliëntdossier door bepaalde functionarissen voor de afwikkeling van klachten/Incidenten/calamiteiten;
    - diefstalpreventie en de beveiliging van gebouwen, terreinen en eigendommen door middel van cameratoezicht;
    - fraudepreventie / rechtmatigheidscontroles, zoals bijvoorbeeld controle op logging van informatiesystemen zoals het elektronisch cliëntendossier.
- wetenschappelijk onderzoek in het kader van gezondheidszorg / algemeen belang (met toestemming van de cliënt / vertegenwoordiger). Toestemming is niet vereist indien aan bepaalde wettelijke voorwaarden wordt voldaan of indien uitsluitend niet herleidbare (geanonimiseerde) gegevens worden gebruikt.

Cliëntgegevens worden door Sevagram voornamelijk verwerkt in daartoe ingerichte beveiligde applicaties zoals applicaties voor het bijhouden van een elektronisch cliëntendossier.

5.2.2 Doeleinden Verwerking Persoonsgegevens medewerkers, stagiaires en vrijwilligers

Persoonsgegevens van medewerkers, stagiaires en vrijwilligers worden door Sevagram voor de volgende doeleinden verwerkt:

- het uitvoeren van de arbeidsovereenkomst, vrijwilligersovereenkomst of stageovereenkomst in de brede zin van het woord:

    - het regelen van indiensttreding, het opstellen van een overeenkomst en de communicatie daaromtrent;
    - het kunnen uitvoeren van de overeengekomen afspraken, bijvoorbeeld de betaling van het overeengekomen salaris / (stage)vergoeding dan wel de aanmelding van een werknemer bij het pensioenfonds of de arbeidsongeschiktheidsverzekeraar (indien van toepassing).
- de uitvoering van de dienstverlening van Sevagram in een multidisciplinaire setting:
    - de vermelding van zakelijke contactgegevens van medewerkers in interne contactenlijsten/telefoonboek;
    - het mogelijk maken van beeldbellen bij interne- externe videoconferenties;
- het voeren van administratie en het voldoen aan wettelijke verplichtingen die op Sevagram (als werkgever) rusten:
    - het bijhouden van een personeelsdossier voor werknemers met daarin verslagen van beoordelings- en functioneringsgesprekken, verzuimfrequentie, eventuele waarschuwingen/klachten, kopie identiteitskaart, BSN-nummer en eventuele persoonlijke aantekeningen van de leidinggevende. Voor vrijwilligers wordt er een beperkter vrijwilligersdossier bijgehouden;
    - het bijhouden van een kopie identiteitsbewijs op grond van de Wet op de Loonbelasting (uitsluitend medewerkers en bezoldigde stagiaires)
    - het vaststellen en (laten) uitbetalen van een onkostenvergoeding of een reiskostenvergoeding voor woon/werkverkeer;
    - het berekenen, vastleggen en betalen/afdragen van belastingen en premies op grond van de wet;
    - het regelen van eventuele aanspraken op uitkeringen via overheidsinstanties zoals het UWV;
    - het organiseren van de verkiezing van de leden van een ondernemingsraad op grond van de Wet op de Ondernemingsraden('WOR'), en;
    - de uitvoering of toepassing van overige wettelijke verplichtingen van Sevagram.
- overige doeleinden en de behartiging van gerechtvaardigde belangen van Sevagram:
    - identificatie en het verlenen van toegang tot gebouwen en terreinen van Sevagram (door middel van medewerkerspas met foto, druppel met personeelsnummer);
    - diefstalpreventie en het beveiligen van terreinen, gebouwen en eigendommen (camerabewaking);
    - de uitvoering van de attentieregeling (speciale gebeurtenissen) voor medewerkers en vrijwilligers;
    - interne- en/of externe communicatie- en marketingdoeleinden (bv. de interne nieuwsbrieven en magazines);
    - interne opleidingsdoeleinden (bv. instructie- of opleidingsfilmpjes).

Persoonsgegevens van medewerkers, stagiaires en vrijwilligers worden verwerkt in specifieke applicaties / ICT systemen ten behoeve van personeelsadministratie, verzuimregistratie, ICT-systemen en de salarisadministratie.

5.3 Overige Verwerkingen / doeleinden / doelbinding

Sevagram verwerkt de verzamelde Persoonsgegevens uitsluitend voor bovenstaande - of daarmee verenigbare - doeleinden. Daarmee geeft Sevagram toepassing aan het principe van 'doelbinding' onder de AVG.[23] Er vindt geen automatische besluitvorming of 'profilering' plaats op basis van Persoonsgegevens.

[23] Artikel 5 lid 1 sub b AVG.

Als Sevagram voornemens is Persoonsgegevens voor andere doeleinden te Verwerken dan hierboven vernoemd, zal Sevagram daarvoor in beginsel - behoudens wettelijke uitzonderingen - de uitdrukkelijke voorafgaande toestemming van Betrokkene vragen.

Ten aanzien van camerabewaking (cameratoezicht) geldt het camerareglement van Sevagram (raadpleegbaar via www.sevagram.nl/privacy).

6 Aanpak van Privacy

6.1 Risicomanagement

6.1.1 Risicobewustzijn

Risicobewustzijn van alle medewerkers is de sleutel voor een effectief beleid. Risicobewustzijn wordt volledig ondersteund door de Raad van Bestuur en zal worden gestimuleerd door middel van training en publicaties. Het risicobewustzijn wordt ook ondersteund door het opstellen en naleven van reglementen en zal indien nodig ook aandacht krijgen in functiebeschrijvingen en arbeidscontracten of inhuurovereenkomsten.

6.1.2 Risico- identificatie

Via een vastgestelde methodiek worden mogelijke Dreigingen ten aanzien van privacy-risico's geïdentificeerd en geïndexeerd. Dit gebeurt minimaal tweejaarlijks voor de hele organisatie en indien nodig geacht eerder middels het uitvoeren van DPIA's. Het management zal de hieruit voortkomende resultaten beoordelen en 'zo kosteneffectief mogelijk' maatregelen implementeren ter vermindering van het risico tot een acceptabel niveau.

6.2 Beperkte toegang

Toegang tot informatie en IT-faciliteiten zal op basis van *'need to know'* worden beperkt, zodat gebruikers toegang krijgen tot datgene wat noodzakelijk is voor het uitvoeren van de functie. Dit is één van de essentiële principes van veilig informatiebeheer. Toegang tot informatiesystemen wordt geïnitieerd door de leidinggevende van de medewerker op basis van toegekende autorisaties en de medewerkersrol. Na het accorderen door de informatie- of informatiesysteem-Eigenaar zullen de autorisaties worden toegekend.

6.3 Informatie Eigendom

ICT-middelen die aan medewerkers beschikbaar worden gesteld, dienen voor zakelijke doeleinden te worden toegepast. Opgeslagen en verwerkte informatie van of voor Sevagram op systemen van de organisatie blijft te allen tijde Eigendom van Sevagram. De internationale en lokale privacywetgeving zal worden gehandhaafd wanneer een beroep op Eigendomsrechten wordt gedaan.

7 Verantwoordelijkheden

7.1 Management verantwoording

De Raad van Bestuur is verantwoordelijk voor de borging en beheer van dit beleid en zal via delegatie naar medewerkers de taken en verantwoordelijkheden beleggen voor de implementatie en beheer van maatregelen voortkomend uit dit beleid.

Beheersing van kwaliteit, informatiebeveiliging en privacy wordt bereikt door een stelsel van organisatorische en technische maatregelen. Deze maatregelen bestaat onder meer uit strategisch beleid, richtlijnen, procedures, gedragscodes, werkinstructies, een organisatie en controles. Medewerkers dienen bewust te worden gemaakt van het belang van deze maatregelen en daar waar nodig geïnstrueerd te worden.

Hierbij stelt Sevagram zich ten doel die maatregelen te treffen die noodzakelijk en in economische zin rendabel zijn om de veiligheid van de informatie en het personeel te waarborgen, aan de relevante wet- en regelgeving te voldoen, de continuïteit van de bedrijfsvoering te waarborgen en om de reputatie te beschermen.

7.2 Functionaris Gegevensbescherming ('FG')

Sevagram heeft een Functionaris voor de Gegevensbescherming benoemd (FG). De FG is een onafhankelijke toezichthouder en adviseur met betrekking tot de naleving van de AVG. Deze behartigt de belangen van de Betrokkenen en is eerste aanspreekpunt voor de nationale toezichthoudende autoriteit, de Autoriteit Persoonsgegevens (AP). Hierdoor werkt de FG vanuit een ander gezichtspunt dan de andere medewerkers. Om het belang van de Betrokkenen te kunnen behartigen, moet de FG zo vroeg mogelijk bij veranderingen die een impact hebben op de Verwerking van Persoonsgegevens worden betrokken.

Alle (nieuwe) of beoogde Verwerkingen (waaronder ook doorgiftes van) Persoonsgegevens dienen bij de Functionaris Gegevensbescherming te worden gemeld. Deze worden gedocumenteerd in het verwerkingsregister van Sevagram (zie ook: onderdeel 7.4.1 en 7.4.3 hierna). Medewerkers hebben een actieve plicht om de FG hierbij tijdig te betrekken.

De FG adviseert vanuit een onafhankelijke positie en heeft een link naar de organisatie, het bestuur en de toezichthouder. De FG vervult een strategische rol voor privacy en – tezamen met de CISO - een operationele rol in het kader van meldingen en de afhandeling van Datalekken richting de AP.

7.3 CISO

De CISO is binnen Sevagram verantwoordelijk voor informatiebeveiliging en het treffen, evalueren alsmede bijstellen van passende technische- en organisatorische maatregelen (NEN7510) om (Persoons)gegevens voldoende te beveiligingen voor inbreuken op de Beschikbaarheid, Integriteit en Vertrouwelijkheid. Daartoe beheert de CISO het informatiebeveilingsmanagementsysteem (ISMS) van Sevagram.

De CISO is betrokken bij afhandeling van Incidenten en Datalekken, de uitvoering van DPIA's en werkt daartoe nauw samen met de Functionaris Gegevensbescherming.

7.2 Medewerkersverantwoording

Alle medewerkers hebben de verantwoording tot naleving van dit beleid en opvolging van de maatregelen welke voortvloeien uit dit beleid. Identificatie van Incidenten of niet naleving t.a.v. dit beleid dienen gemeld te worden aan de leidinggevende of aan de FG.

7.3 Beoordeling en corrigerende maatregelen

Sevagram zal de maatregelen die uit dit beleid voortkomen periodiek controleren door middel van controles en eventueel interne en externe audits t.a.v. (kosten)effectiviteit. Jaarlijks zal de Raad van Bestuur effectiviteit van dit beleid beoordelen op basis van verzamelde gegevens en informatie.

Input voor deze beoordeling is o.a.:

- Registratie van Incidenten en non-compliance issues;
- Registratie van controle, interne en externe audits;
- Klanttevredenheidsonderzoeken;
- Leveranciersbeoordelingen;
- Risicoanalyse output;
- Medewerkerscompetenties;
- Bewustwording en training;
- Wet- & regelgeving;
- DPIA's.

Op basis van de (tussentijdse) beoordelingen zullen waar mogelijk corrigerende en of preventieve maatregelen worden doorgevoerd. Corrigerende en preventieve maatregelen kunnen ook voortkomen uit overleggen en bijbehorende rapportages en worden zodanig vorm gegeven, dat de kans op herhaling geminimaliseerd wordt.

7.4 Documentatie

7.4.1 Verwerkingsregister

Sevagram is als onderdeel van haar verantwoordingsplicht op grond van de AVG verplicht om een register van verwerkingsactiviteiten – ook genoemd: een 'verwerkersregister' - bij te houden.[24] Dit is een (digitaal) register waarin alle verwerkingen van persoonsgegevens worden geregistreerd. Bij Sevagram wordt het verwerkingsregister gezamenlijk beheerd door de CISO en de FG.

Alle nieuwe verwerkingen van persoonsgegevens binnen Sevagram (bijvoorbeeld een nieuwe applicatie waarin persoonsgegevens worden verwerkt, een nieuwe voorgenomen verzameling van persoonsgegevens of doorgifte van persoonsgegevens aan een derde) moeten voorafgaand bij de FG/CISO worden gemeld ten behoeve van het verwerkingsregister. Dit kan via het e-mailadres: Privacydesk@sevagram.nl.

Alle medewerkers hebben een eigen verantwoordelijkheid om (nieuwe of veranderde) verwerkingen van persoonsgegevens tijdig te melden bij de Privacydesk. De FG toetst daarbij of de beoogde nieuwe verwerking voldoet aan de AVG. Daarnaast toetst de CISO of de Verwerking verenigbaar is met de informatiebeveiligingsstandaarden die binnen Sevagram gelden. Dit geldt niet slechts voor nieuwe verwerkingen, maar ook voor veranderingen in bestaande verwerkingen (bijvoorbeeld: indien beoogd wordt om bestaande persoonsgegevens te gebruiken voor een ander doel).

[24] Artikel 30 AVG.

7.4.2 Classificatie van gegevens

Voor een effectieve bescherming van de privacy is vereist dat de waarde van de informatie voor de onderneming bekend is. Het betreft hierbij classificatie van privacygevoelige informatie in termen van vereiste Vertrouwelijkheid, Integriteit en Beschikbaarheid aan de hand van de navolgende vertrekpunten:

- Informeert het management en medewerkers over wat moet worden beschermd en hoe informatiemiddelen op een standaard manier kunnen worden beschermd;
- Toont de waarde van middelen aan medewerkers, zodat het bewustzijn van beveiliging binnen hun dagelijkse werkzaamheden wordt gestimuleerd;
- Stelt Sevagram in staat te voldoen aan eventuele wettelijke en contractuele verplichtingen;
- De Eigenaar van de informatie blijft verantwoordelijk voor het up-to-date houden van de identificatie van informatiemiddelen en de toegekende waarde van elk van de geïdentificeerde middelen.

7.4.3 Privacy by Design & Privacy by Default

De AVG vereist dat reeds bij het ontwerp van (nieuwe) producten/diensten rekening wordt gehouden met de bescherming van Persoonsgegevens (*'privacy by design'* oftewel: *'gegevensbescherming door ontwerp')* en dat in relatie tot Betrokkenen privacy ook als 'standaardinstelling' moet zijn doorgevoerd *('privacy by default'* of *'gegevensbescherming door standaardinstellingen).*[25]

- *Privacy by Design:* het doel van gegevensbescherming door ontwerp is dat door het meenemen van preventieve in plaats van reactieve maatregelen in de ontwikkelingsfase, het risico op Incidenten / Datalekken aanzienlijk kan worden beperkt. Voorkomen is immers beter dan genezen.
- *Privacy by Default:* gegevensbescherming door standaardinstellingen impliceert dat producten en diensten standaard dusdanig moeten worden ingesteld dat de hoogste mate van privacy voor Betrokkenen wordt gegarandeerd.

Sevagram geeft aan deze principes concreet de navolgende uitwerking:

- *Privacy by Design:* bij alle (nieuwe) Verwerkingen, projecten en/of applicaties die een (beoogde) Verwerking van Persoonsgegevens impliceren, dient reeds in het beginstadium (tijdig) advies te worden ingewonnen bij de Functionaris Gegevensbescherming (privacy) en de CISO (informatiebeveiliging). Deze verplichting rust op alle medewerkers die intern Eigenaar zijn van een (beoogde) Verwerking, project of systeem. Dit is noodzakelijk zodat de FG tijdig kan adviseren over de vraag of al dan niet een voorafgaande DPIA dient te worden uitgevoerd. De tijdige uitvoering van een DPIA is de primaire verplichting van de interne Eigenaar van de beoogde Verwerking, het project of systeem tezamen met de CISO. De FG heeft hierin enkel een adviserende en toezichthoudende rol. De adviezen van de FG en CISO dienen zo veel mogelijk te worden meegenomen in de implementatietraject.
- Bij de diensten en producten die Sevagram aanbiedt aan Betrokkenen moet de privacy van betrokkenen als standaardinstelling worden gewaarborgd. Sevagram streeft ernaar haar applicaties en informatievoorziening standaard in richten op de meest privacy vriendelijke wijze en houdt hiermee ook rekening bij de selectie van (nieuwe) leveranciers / Verwerkers. Concreet houdt dit bijvoorbeeld in dat indien 'toestemming' wordt gevraagd, er altijd sprake zal zijn van een actieve handeling (*'opt-in'* in plaats van *'opt-out'*), dat applicaties standaard zo weinig mogelijk Persoonsgegevens dienen te verwerken (bv. geen onnodige locatiegegevens), en dat Betrokkenen altijd een geïnformeerde keuze kunnen maken op basis van heldere en transparante informatie.

[25] Artikel 25 AVG.

8 Kwaliteitsbewaking

8.1 Communicatie

In de communicatie van dit beleid staat de bewustwording van de eigen medewerkers (inclusief ingehuurde derden) en de naleving van de regels en richtlijnen centraal. Om dit te bewerkstelligen zullen er gedragsregels opgesteld en worden gecommuniceerd zodat medewerkers weten wat er van hen wordt verwacht, welke risico's er zijn en welke rechten en plichten medewerkers hebben. Veranderingen en aanpassingen in het managementsysteem worden door het Directieteam beoordeeld en intern gecommuniceerd, indien nodig ook naar relevante externe partijen.

Het Directieteam bepaalt:
- wat wordt gecommuniceerd;
- wanneer wordt gecommuniceerd;
- met wie wordt gecommuniceerd;
- wie de communicatie uitvoert en;
- welke processen door de communicatie worden beïnvloed.

8.2 Borging

Borging vindt plaats door middel van vastlegging van de overeengekomen werkwijze in procesbeschrijvingen, richtlijnen, een gedragscode, procedures, werkinstructies en informatiesystemen. Deze dienen voor alle medewerkers toegankelijk te zijn en zullen via intranet of KISS worden verspreid, zodat in het geval van Incidenten en calamiteiten deze snel en eenduidig toegankelijk zijn.

8.3 Geldigheid en evaluatie

De Raad van Bestuur is Eigenaar van dit beleidsdocument. Dit beleid is drie jaar geldig en wordt minimaal een keer per jaar geëvalueerd met het oog op:
- de toereikendheid en de tactische en operationele uitvoering ervan;
- de stand van de techniek (beveiliging en bedreiging);
- voortschrijdend inzicht;
- veranderende wet- en regelgeving of organisatie.

Op grond van de jaarlijkse beoordeling, veranderende wet- en regelgeving of door andere omstandigheden, kan dit beleid tussentijds worden bijgesteld.

8.4 Naleving

Naleving van het beleid wordt gecontroleerd. Niet naleving van of niet voldoen aan het beleid kan disciplinaire maatregelen tot gevolg hebben conform de geldende wetgeving/jurisprudentie en het interne beleid van Sevagram.