Register van verwerkingen

Versie 24-07-2018. Dit register is in ontwikkeling.

1. Algemene informatie

De Gemiva-SVG Groep verwerkt als zorgaanbieder, werkgever en maatschappelijke organisatie persoonsgegevens. Daarbij zijn we gebonden aan de Algemene Verordening Gegevensbescherming (AVG) en aan (onder meer) zorgspecifieke regelgeving.

De AVG schrijft voor dat organisaties die persoonsgegevens verwerken (verzamelen, opslaan, bewerken, verspreiden, verwijderen, etc.) een register van verwerkingen bijhouden. Die verplichting geldt ook voor ons. In dat register moeten we onze verwerkingen beschrijven. De Autoriteit Persoonsgegevens (AP) kan zich dan een beeld vormen van de soorten persoonsgegevens die wij verwerken, de doelen die we daarmee dienen en de gebruikers van deze gegevens. Wij zijn niet verplicht om ook anderen – bijvoorbeeld personen waarvan wij gegevens verwerken – inzage in het register te geven. De AVG bevat geen format voor de vormgeving van het register. Wij hebben gekozen voor een verhalende vorm.

Dit document is ons register. We beginnen met het vermelden van algemene gegevens, die voor al onze verwerkingen gelden. Daarna gaan we per afzonderlijke verwerking in op de doelen, de categorieën van personen van wie we gegevens verwerken, een beschrijving van het type persoonsgegevens in de verwerking, de toepasselijke bewaartermijnen (voor zover mogelijk) en de categorieën van ‘ontvangers’ (degenen die de persoonsgegevens kunnen inzien en eventueel bewerken).

Meer weten over ons privacybeleid? Bekijk ons privacystatement, ons privacykader en daarin opgenomen procedure voor het uitoefenen van AVG-rechten – zoals het recht op inzage of correctie. Ook deze documenten vind je op onze website via www.gemiva-svg.nl/privacy.

Algemene gegevens met betrekking tot onze verwerkingen

De Stichting Gemiva-SVG Groep is bij de Kamer van Koophandel geregistreerd onder nummer 41174469. Het postadres van de Gemiva-SVG Groep is Postbus 604, 2800 AP Gouda. Ons algemene telefoonnummer is 0182 57 58 00. Wil je ons mailen over privacyzaken, stuur dan een bericht naar secretariaat@gemiva-svg.nl.

De Gemiva-SVG Groep levert medewerkers aan samenwerkingsverbanden die een eigenstandige verwerkingsverantwoordelijkheid hebben. Het gaat dan om samenwerkingsverbanden op basis van opdrachten die door gemeenten in het kader van de Jeugdwet of de Wet op de maatschappelijke ondersteuning 2015 zijn verstrekt. Deze samenwerkingsverbanden zijn:

- Tom in de buurt, Alphen aan den Rijn (Wmo)
- Go! voor jeugd, Alphen aan den Rijn (Jeugdzorg)
- Gijs , Rotterdam (Jeugdzorg)

- Coöperatie Voortouw , Gouda (Sociale Teams 0-100)
- Coöperatie JGT Holland-Rijnland, Leiden (Jeugd- en gezinsteams)

Wij delen geen persoonsgegevens met organisaties in het buitenland.

Functionaris voor de gegevensbescherming

Vanwege onze omvang en de omstandigheid dat wij ook gegevens over de gezondheid en begeleiding van cliënten verstrekken, zijn wij verplicht om een functionaris voor de gegevensbescherming (fg) aan te stellen. Die houdt intern toezicht op de toepassing van de AVG en de uitvoering van ons privacybeleid. Deze functie wordt nu vervuld door Dirk van der Star. Hij is per post bereikbaar: functionaris gegevensbescherming Gemiva-SVG Groep, Postbus 604, 2800 AP Gouda, per mail op fg@gemiva-svg.nl en telefonisch op 0182 57 58 21.

Technische en organisatorische maatregelen

Terecht verwacht de AVG van ons dat wij redelijke maatregelen nemen om de persoonsgegevens waarover wij (komen te) beschikken te beschermen. We noemen hier de belangrijkste:

- We besteden de nodige aandacht aan voorlichting en bewustwording van onze medewerkers. Ons uitgangspunt is ‘Wat u niet wilt dat u geschiedt, doe dat ook een ander niet (aan)’.
- Op het gebied van technische maatregelen beschikken we over een ‘firewall’ en ‘redundante uitvoering’. Dat moet toegang door hackers en ongewenst verlies van data tegengaan. We maken dagelijks (automatisch) back ups van onze bestanden.
- Voor de toegang tot applicaties hebben we autorisatiematrixen opgesteld, die aangeven welke medewerkers (functionarissen) tot op welk niveau toegang tot gegevens hebben en deze kunnen inzien of muteren.
- We beschikken nog niet over Single Sign On, maar wel over een strikt wachtwoordbeleid, dat dwingt tot het ingeven van relatief sterke wachtwoorden die – afhankelijk van de applicatie – periodiek moeten worden gewijzigd.
- We loggen de toegang tot databases die persoonsgegevens bevatten, onder meer om te kunnen toetsen of er geen ongewenst of onnodig gebruik van toegangsrechten wordt gemaakt.
- Wermoeden we een datalek, dan treedt een procedure in werking waarbij de fg, het hoofd van de afdeling Netwerkbeheer en een lid van de Raad van Bestuur onderzoek doen of laten doen. Zij regisseren dat proces en bepalen of er daadwerkelijk sprake is van een datalek. Zo ja, dan melden zij dit volgens voorschrift bij de AP. Zij treffen maatregelen ter voorkoming van (extra) schade. Als dat redelijkerwijs mogelijk is zorgen zij er ook voor dat degenen wier persoonsgegevens via het datalek in onbevoegde handen (kunnen) zijn geraakt daarover worden geïnformeerd.

2. Verwerking cliëntgegevens

Via diverse gekoppelde applicaties (met name Plancare, Plancare Web) verwerken we gegevens van cliënten. Het doel daarvan is het bieden van adequate begeleiding, verantwoording aan

externe toezichthouders (Inspectie Gezondheidszorg en Jeugd), financiële verantwoording (aan gemeenten en zorgkantoren die de ondersteuning van cliënten bekostigen), en interne communicatie bij de begeleiding van cliënten tussen betrokken medewerkers. We verwerken deze persoonsgegevens – waaronder ook gezondheidsgegevens op basis van de met cliënten gesloten (zorg)overeenkomsten en toepasselijke wetgeving (Wlz, Jeugdwet, Wet op de maatschappelijke ondersteuning, Wet bijzondere opnemingen in psychiatrische ziekenhuizen, Wet op de geneeskundige behandelingsovereenkomst).

Potentiële cliënten, vertegenwoordigers

Vanwege de procedures rond indicatiestelling en zorgtoewijzing leggen we ook persoonsgegevens vast over (ons toegewezen of zich bij ons gemeld hebbende) potentiele cliënten. We beschouwen dat als vastleggen in het kader van de precontractuele fase.
In onze cliëntenregistratie zijn ook gegevens van (wettelijke) vertegenwoordigers van cliënten opgenomen. Naast hun 'status' ten opzichte van de cliënt gaat het dan om contact- en NAW-gegevens. Daarbij baseren we ons op de gesloten overeenkomst – indien de vertegenwoordiger die namens de cliënt aangaat – of op het gerechtvaardigde belang van de cliënt.

Toegang tot cliëntgegevens

We verstrekken gegevens – c.q. kennen rechten toe inzake het verwerken van gegevens – aan onze medewerkers die betrokken zijn bij en verantwoordelijk voor de ondersteuning, besluitvorming en behandeling van cliënten, de registratie en verantwoording daarvan of het interne toezicht op de kwaliteit ervan. Daarbij maken we een afweging tussen 'need to know' en de waarschijnlijkheid dat een medewerker tijdens zijn werk – teneinde kwalitatief goede ondersteuning te kunnen bieden – persoonsgegevens moet kunnen raadplegen. De begeleiders van een locatie hebben dus uitsluitend toegang tot de persoonsgegevens van cliënten die van 'hun' locatie gebruik maken. De behandelaars (artsen, gedragsdeskundigen) die locatie-overstijgend werken, kunnen gegevens van alle cliënten waarvoor zij potentieel ingezet worden inzien. Ook zij dienen daarbij de gedragsregel 'need to know' te respecteren. Per applicatie is in een autorisatiematrix vastgelegd wie (c.q. welke categorieën van medewerkers) welke rechten met betrekking tot de toegang en het gebruik van die applicatie heeft.

Vrijheidsbeperking, vermoedens van misbruik en klachtbehandeling

In het kader van deze verwerking van cliëntgegevens registreren en verwerken we ook gegevens rond de toepassing van vrijheidsbeperkende maatregelen, incidenten, vermoedens van misbruik of mishandeling en klachten. Waar het gaat om de twee laatstgenoemde registraties is de toegang beperkt tot slechts enkele functionarissen (klachtenfunctionaris, consultatieteam misbruik en mishandeling, Raad van Bestuur).
Het betreft hier overigens geen 'grootschalige' verwerkingen. Over klachten rapporteren we geanonimiseerd aan onze Centrale Medezeggenschaps Raad.

Bijzondere zorg buiten de locatie

Als cliënten bijzondere medische zorg nodig hebben (bijvoorbeeld omdat zij op willekeurige momenten toevallen kunnen krijgen of er sprake is van bijzondere allergieën) dan hebben onze

begeleiders bij uitstapjes buiten de locatie in een aantal situaties medische informatie over deze cliënten bij zich. Dat is dan nodig om hun veiligheid en gezondheidssituatie in geval van medische calamiteiten of ongelukken te kunnen borgen. We realiseren ons dat het risico op verlies van of ongeautoriseerde toegang tot deze informatie in dergelijke omstandigheden toeneemt, maar we menen dat het potentieel voorkomen of verminderen van gezondheidsschade voor de cliënt daartegen opweegt.

Uitwisseling van cliëntgegevens met derden

Op basis van relevante wetgeving delen wij persoonsgegevens van cliënten met financiers zoals zorgkantoren en gemeenten. Het gaat dan bijvoorbeeld om het versturen van digitale declaratieberichten, waaruit de financier moet kunnen opmaken dat de gedeclareerde zorg (in uren, dagdelen, minuten of andere 'inspanningseenheden' inderdaad aan een concrete burger met een passende indicatie is te relateren. Wettelijk zijn we ook verplicht dergelijke informatie door te leveren aan het Centraal Administratiekantoor, dat de zogenaamde eigen bijdrageregelingen voor de zorgsector uitvoert. Als we door het zorgkantoor (voorschrift zorgtoewijzing) of de gemeente zijn aangewezen als 'dossierhouder' voor de (nog niet geplaatste c.q. nog niet – volledig - ondersteunde) cliënt delen we die informatie – met toestemming van de cliënt – ook met andere aanbieders als voor de cliënt dringend een plek c.q. aanvullende ondersteuning moet worden geregeld.
Als de Wlz-cliënt aangeeft dat hij zijn indicatie wil vertalen in zorglevering door meerdere zorgaanbieders, wisselen wij met die zorgaanbieders de gegevens uit die nodig zijn om te kunnen vaststellen dat die zorglevering binnen de grenzen van de afgegeven indicatie en de bijbehorende bekostigingsvoorschriften blijft.

Digitaal cliëntportaal

Cliënten en door hen (of hun wettelijke vertegenwoordigers) aangewezen derden (maximaal 5 personen per cliënt) kunnen via het digitaal portaal MijnDossier! met een inlognaam en een zelfgekozen wachtwoord online inzage krijgen in delen van hun eigen dossier: de (persoonlijke) agenda, het ondersteuningsplan en de dagrapportage. Via MijnDossier! kunnen zij ook communiceren met hun persoonlijk begeleider. Zij zijn zelf verantwoordelijk voor het beheer van het door hen ingestelde wachtwoord. De cliënt of vertegenwoordiger kan de 'aanwijzing' van een derde ook intrekken. Daarvoor geldt dezelfde procedure als voor 'aanwijzen'.

Bewaartermijnen

(Medische) behandelgegevens dienen wij op grond van wetgeving 15 jaar te bewaren. Omdat ook de levensgeschiedenis van de cliënt relevant is voor de begeleiding, ondersteuning en behandeling die wij bieden, bewaren wij die gegevens tot 15 jaar na de 'uitstroom' (als gevolg van overlijden, vertrek naar een andere zorgaanbieder of anderszins) van de cliënt uit onze organisatie. Gegevens van burgers die bij ons op een wachtlijst staan en te kennen hebben gegeven geen zorg van ons te zullen afnemen, bewaren we maximaal een jaar na deze kennisgeving in het actieve dossier. Dat is ook nodig omdat zorgkantoren daar op basis van hun wettelijke taken tijdens hun zogenaamde materiële controle naar kunnen informeren. Vanwege technische beperkingen in de applicatie kunnen we deze gegevens echter (nog) niet 'deleten'. We zetten ze daarom na ommekomst van

de genoemde termijn in een aparte map, die slechts door een zeer beperkt aantal medewerkers geopend kan worden.

Voor de inhoud van de cliëntendossiers zijn de betrokken behandelaren, de persoonlijk begeleider en de locatiemanager van de locatie waar de cliënt diensten afneemt verantwoordelijk. Het sluiten en vernietigen van het dossier na ommekomst van de toepasselijke bewaartermijn is ingebouwd in Plancare (dossiers die gesloten zijn in 2003 worden in 2018 gedelete).

Nachttoezicht cliënten

Voor een groot aantal cliënten is nachttoezicht georganiseerd via uitluisteren of videotoegang. Dat is dan altijd in het ondersteuningsplan van de cliënt vastgelegd. De medewerkers die belast zijn met het nachttoezicht beschikken daarbij (uiteraard) over toegang tot de digitale dossiers van deze cliënten, zodat zij hun observaties ten behoeve van een geode risico-inschatting en eventueel vereiste acties kunnen koppelen aan de over de cliënt beschikbare informatie (bijvoorbeeld rapportages en medicatiegebruik).

Bewonersfinanciën en wasverzorging

Aan een aantal cliënten verlenen we op basis van een overeenkomst administratieve diensten. Cliënten kunnen met ons ook een overeenkomst sluiten rond wasverzorging. Met het oog op deze dienstverlening registreren wij betaalgegevens en financiële verplichtingen. Alleen de betrokken locatiemanagers, persoonlijk begeleiders en administratieve medewerkers en hun managers hebben inzicht in deze (persoons)gegevens. We bewaren de betrokken gegevens tot maximaal een jaar nadat de dienstverlening is beëindigd. De afdeling bewonersgelden is daarvoor verantwoordelijk.

3. Verwerking medewerkersgegevens

Via diverse gekoppelde applicaties (met name SDB) verwerken we gegevens van medewerkers die op arbeidsovereenkomst bij ons werkzaam zijn. Dat doen we om onze verplichtingen als ‘goed werkgever’ na te komen. Op die basis betalen we salarissen, leggen we opleidingsactiviteiten vast, registreren we bekwaamheden en de uitkomsten van ontwikkelgesprekken, vullen we personeelsdossiers (ook handig als je een medewerker na 40 jaar trouwe dienst op een jubileumtoespraak wilt vergasten!), betalen we reiskostenvergoedingen en andere gedeclareerde onkosten uit en bieden we verzuim- en loopbaanbegeleiding. De grondslag is dus de gesloten arbeidsovereenkomst in combinatie met wettelijke verplichtingen.

Gezondheidsgegevens, BSN, VOG, verzuimgegevens

Van medewerkers leggen we geen gezondheidsgegevens vast (dat doet onze bedrijfsarts, maar die is daarvoor eigenstandig verwerkingsverantwoordelijk) maar wel het BSN-nummer en de aanwezigheid van een VOG. We verstrekken deze gegevens – voor zover relevant – aan de betrokken leidinggevenden in de lijn, aan medewerkers personeel en organisatie en aan onze externe salarisverwerker SDB. We delen die gegevens voor zover relevant ook met de organisatie

die ons ondersteunt bij het dragen van de verplichtingen die uit ons eigen risicodragerschap in het kader van sociale wetgeving (Wia, Ziektewet) voortvloeien.

Subsidies inzake arbeidsmarkt, scholing etc.

Als dat noodzakelijk is ter verkrijging van arbeidsmarkt- en andere subsidies voor opleiding en scholing delen we relevante gegevens ook met de subsidiërende instellingen en het intermediaire bureau dat we daarbij inschakelen. Met dit bureau hebben we een verwerkersovereenkomst afgesloten. Hetzelfde geldt voor het bureau dat namens ons medewerkerstevredenheidsonderzoek uitvoert en instrumentarium voor zogenaamde teamreflecties verzamelt, bewerkt en teruglevert.

Bewaartermijnen

Als de medewerker uit dienst gaat, verwijderen we de gegevens 7 jaar na datum uitdiensttreding. We sluiten daarmee aan op de voorschriften die inde Wet op de Rijksbelastingen zijn opgenomen. De afdeling Personeel & Organisatie is verantwoordelijk voor het hanteren van de bewaartermijnen en het aansluiten vernietigen c.q. anonimiseren van de betrokken persoonsgegevens. De verantwoordelijkheid voor het beheren en opschonen c.q. vernietigen van gegevens rond de door medewerkers gevolgde opleidingen en scholingen – via de applicatie LeerLink – ligt bij de afdeling Leren en Ontwikkelen. Deze gegevens verwijderen we – ook met het oog op eventuele terugbetalingsverplichtingen op basis van de cao - uiterlijk twee jaar na de uitdiensttreding van de medewerker.

Vrijwilligers en stagiaires

Een bijzondere categorie medewerkers wordt gevormd door vrijwilligers. Met hen sluiten we een vrijwilligersovereenkomst. We registreren contractgegevens, bankrekeningnummers (om onkosten en vergoedingen te kunnen betalen) en de aanwezigheid van een VOG. Mutatis mutandis geldt hetzelfde voor de stagiaires die bij ons in het kader van hun opleiding stage lopen. Ook hier vormt de gesloten overeenkomst de grondslag voor de verwerking. Een jaar nadat de vrijwilligersovereenkomst is geëindigd, verwijderen we de betrokken gegevens. We beschikken overigens niet over een centraal register van vrijwilligers.

Sollicitanten

Gegevens van sollicitanten – indien we daarmee geen arbeidsovereenkomst aangaan – bewaren we tot maximaal vier weken na afronding van de procedure, tenzij de betrokkene uitdrukkelijk te kennen heeft geven bij ons als gegadigde voor een passende functie in beeld te willen blijven.

Loonbeslag

Gegevens over loonbeslagen verwijderen we uit onze systemen zodra het loonbeslag is opgeheven.

Waarschuwingregister

We zijn aangesloten bij het waarschuwingsregister Zorg en Welzijn. We verwerken de gegevens van ex-medewerkers die we aldaar conform de geldende protocollen hebben gemeld. De

betrokkene is daarvan altijd op de hoogte. Uitsluitend de Manager PO&C en de leden van de Raad van Bestuur hebben toegang tot deze gegevens.

Personenalarmering

In een aantal locaties waarin cliënten met (potentieel) agressief gedrag ondersteuning ontvangen, zijn de medewerkers toegerust met een vorm van personenalarmering, zodat zij in noodsituaties onmiddellijk de bijstand van collega's kunnen inroepen. Dit systeem koppelt de naam van de collega die alarmeert aan de fysieke plek waar deze zich op het moment van de alarmering bevindt.

Rittenregistratie

Om te voldoen aan fiscale vereisten en te voorkomen dat medewerkers die voor zakelijk gebruik onze voertuigen (bijvoorbeeld de auto's van de technische dient of busjes voor rolstoelvervoer) besturen voor de zogenaamde 'fiscale bijtelling' worden aangeslagen, hebben we een digitaal rittenregistratiesysteem ingekocht dat werkt met persoonlijke keyfobs. Via de verwerker kunnen we ook nagaan welke medewerker een verkeersovertreding heeft begaan als ons daarvoor een boete (administratieve sanctie) wordt opgelegd. We maken van de mogelijkheden tot controle die dit personenvolgsysteem biedt alleen gebruik als daartoe een concrete aanleiding bestaat. De geregistreerde gegevens worden na 7 jaar (fiscale bewaartermijn) vernietigd.

Internetgebruik

Uit beveiligingsoogpunt en om onrechtmatige toegang tot persoonsgegevens tegen te gaan, loggen we internetgebruik gedurende een periode van maximaal 6 maanden. De grondslag is hier de gerechtvaardigde afweging van belangen. Na genoemde periode worden deze gegevens gewist. Uitsluitend bij een ernstige verdenking van ontoelaatbaar gebruik van onze digitale faciliteiten kan de afdeling Netwerkbeheer op verzoek van de Raad van Bestuur het digitale gedrag van een medewerker onderzoeken.

Sleutelsysteem

De fysieke toegang tot onze accommodaties verloopt via (een combinatie van) sleutels, keyfobs en/of alarmcodes. We registreren per medewerker over welke toegangsmogelijkheden hij of zij beschikt.

4. Enkele specifieke verwerkingen

Relatie-informatiesysteem

(Een deel van onze) Leveranciers, dienstverleners etc. hebben we geregistreerd in een applicatie die N-adres heet. Het gaat dan om partijen die een zakelijke relatie met ons wensen (en wij met hen) en het komt ons als volstrekt logisch voor dat wij dan ook de namen en contactgegevens van de daarbij betrokken functionarissen registreren. We zullen eenieder die in dat register voorkomt voor 31 december 2018 een mailbericht sturen met de mededeling dat hij of zij is vermeld. Bij

bezwaar of als de gegevens onjuist zijn, ontvangen we graag een reactie. Bij uitblijven daarvan veronderstellen we dat de geregistreerde akkoord is.

Gemiva Plus

Een aantal oud-medewerkers (gepensioneerden) van onze organisatie heeft zich aangemeld voor Gemiva Plus. Wij hebben deze oud-medewerkers geregistreerd (NAW-gegevens, verjaardagen) om hen te kunnen benaderen voor de manifestaties die we voor Gemiva Plus organiseren en om hen met hun verjaardag te kunnen feliciteren. Als deze oud-medewerkers zich afmelden of overlijden, verwijderen we hun gegevens uit het bestand.

Datalekken

De AVG verplicht ons in een register ook meldingen over mogelijke datalekken bij te houden. Ook als die niet tot een melding aan de Autoriteit Persoonsgegevens leiden en uit onderzoek blijkt dat er ‘niets aan de hand is’. Afhankelijk van de context kunnen in dat register ook namen van cliënten en medewerkers voorkomen. Het is in principe alleen toegankelijk voor de fg, het hoofd Netwerkbeheer, de leden van de Raad van Bestuur en (op verzoek) de Autoriteit Persoonsgegevens.

Gouda, juli 2018