Register van Verwerkingen Gemiva-SVG Groep

Versiedatum: 28 februari 2023

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 op basis van categorieën van betrokkenen per verwerking in op de doelen, 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 privacyreglement en de in dat reglement opgenomen procedure voor het uitoefenen van rechten – zoals het recht op inzage of correctie – onder de AVG. Ook deze documenten vind je op onze website.

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) 575800. Wil je ons mailen over 'privacyzaken', stuur dan een bericht naar secretariaat@gemiva-svg.nl.

De Gemiva-SVG Groep – hierna: Gemiva - neemt deel aan samenwerkingsverbanden die zorg en ondersteuning aan burgers leveren en in dat kader 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. De samenwerkingsverbanden waarin wij als 'combinant' participeren zijn:

- De Coöperatie Dichtbij in de Rijnstreek (TOM2). Tom in de buurt, Alphen aan den Rijn (Wmo)
- Go! voor jeugd, Alphen aan den Rijn (Jeugdzorg)

Wij delen geen persoonsgegevens met organisaties in het buitenland.

Functionaris voor de gegevensbescherming

Alhoewel niet verplicht heeft Gemiva vanwege onze omvang en de omstandigheid dat wij gegevens over de gezondheid en begeleiding van cliënten verstrekken ervoor gekozen 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 privacy beleid. Deze functie wordt nu vervuld door Dirk van der Star. Hij is per post bereikbaar: functionaris gegevensbescherming Gemiva, 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. Wij baseren ons hierbij op de actuele versie van de NEN7510 en noemen hier de belangrijkste:

- we besteden de nodige aandacht aan voorlichting en bewustwording van onze medewerkers op dit gebied. 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;
- met geplande tussenpozen laten we een audit voor informatiebeveiliging doen door een externe partij, waar we opvolging aan geven. Ook laten we periodiek penetratietesten doen door een ethische hacker;
- wij eisen van softwareleveranciers die persoonsgegevens verwerken dat zij gecertificeerd zijn voor informatiebeveiliging volgens de normen ISO27001 en/of NEN 7510. Wij houden hier toezicht op en op het nakomen van gemaakte (contractuele) afspraken;
- 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 c.q. muteren;
- we beschikken per maart 2023 over Single Sign On en maken daarbij gebruik van tweewegauthenticatie. We voeren een strikt wachtwoordbeleid, dat dwingt tot het ingeven van relatief sterke wachtwoorden die als het om applicaties gaat waarin bijzondere persoonsgegevens worden verwerkt periodiek moeten worden gewijzigd;
- we controleren de audit logs van databases die persoonsgegevens bevatten om te kunnen toetsen of er geen ongewenst c.q. onnodig gebruik van toegangsrechten wordt gemaakt;
- vermoeden we een datalek**,** dan treedt een procedure in werking waarbij de fg, het hoofd van de afdeling ICT 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.

Datalekken

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

Privacy risico's

Veel van de gegevens die wij verwerken van cliënten en medewerkers kunnen geschaard worden onder de zogenoemde bijzondere of 'gevoelige' persoonsgegevens. Dit zijn gegevens met een hoog privacy risico. Hierbij kan gedacht worden aan respectievelijk gezondheids- en financiële gegevens. In dit register worden de verwerkingsactiviteiten met een hoog privacy risico benoemd en waar van toepassing aangegeven welke applicaties worden gebruikt. Deze applicaties zijn in onderstaande tekst vetgedrukt. De gebruikte applicaties en de verwerkingen worden met regelmaat beoordeeld en geëvalueerd op basis van ons informatiebeveiligingsbeleid. Bij verandering in het gebruik van de applicatie of nieuwe verwerkingen wordt bovendien een zogenoemde gegevensbescherming-effectbeoordeling (GBEB) uitgevoerd.

2.1 Verwerking gegevens (potentiele) cliënten en vertegenwoordigers

We verwerken persoonsgegevens van cliënten en potentiële cliënten die te kennen hebben gegeven mogelijk met ons een zorgverleningsrelatie te willen aangaan – waaronder ook gezondheidsgegevens - op basis van de met cliënten gesloten (zorg)overeenkomsten en toepasselijke wetgeving (Wlz, Jeugdwet. Zorgverzekeringswet, Wmo, Wet Zorg en Dwang, Wgbo). Voor zorgovereenkomsten geldt dat ze schriftelijk kunnen zijn overeengekomen, maar – conform onze algemene voorwaarden – ook door de gebruikmaking van ons zorgaanbod. De cliëntgegevens worden verwerkt via diverse gekoppelde applicaties (met name **Ons Dossier, Entrace, TriasWeb en arQive**). De verwerkingen zijn noodzakelijk met het oog op een goede behandeling of verzorging van de betrokkene en voor het beheer van de instelling.

Het doel van de verwerking van cliëntgegevens 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.

2.2 Verwerkingsactiviteiten en doelbinding

Vrijheidsbeperking, vermoedens van misbruik en klachtbehandeling

In het kader van deze verwerking van cliëntgegevens registreren en verwerken we 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 Medezeggenschap Raad.

Medicatie

Er worden medicijngegevens vastgelegd met betrekking tot cliënten ten behoeve van de adequate begeleiding en behandeling van onze cliënten. Ook schrijven onze artsen verstandelijk gehandicapten medicijnen voor. Op basis van de (elektronische) voorschrijving dienen medewerkers de medicatie toe en geven aan dat de toediening heeft plaatsgevonden. Het medicatieproces vindt in een aantal gevallen digitaal en beveiligd plaats via de applicatie **Medimo** (Swetterhage) of **N-care** (locaties het Hof en Castorstraat). Overige locaties gebruiken papieren aftekenlijsten die worden bewaard in een afgesloten kast. Het is onze ambitie om in al onze (woon)locaties over te stappen op elektronische toedienregistratie (ETDR). Daartoe voeren we pilots uit met **ONS Medicatie en Medimo**.

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.

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 goede 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. Formeel wordt die overeenkomst gesloten met onze dochterstichting SBBG, waarvan Gemiva de statutaire bestuurder is. 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 kalenderjaar na het jaar dat de dienstverlening is beëindigd. De afdeling bewonersgelden is daarvoor verantwoordelijk. Er wordt gebruik gemaakt van **Bizon** en **Pro-Active**. **Pro-Active** is een applicatie waarbij geen bijzondere persoonsgegevens worden gebruikt.

Melding Incidenten en Calamiteiten (MIC)
Medewerkers maken melding van incidenten en calamiteiten waar zij bij betrokken of getuige van waren. Hierbij worden ook de voor de melding relevante persoonsgegevens verwerkt. De MIC-registratie heeft als doel bij te dragen aan verbetering van dienstverlening en arbeidsomstandigheden. De commissie MIC registreert, doet zo nodig onderzoek en adviseert over mogelijke maatregelen om herhaling te voorkomen. Er zullen geen preventieve maatregelen worden genomen op grond van een of een zeer beperkt aantal meldingen. Veeleer zal een actie gebaseerd zijn op rapportage, waarbij personen beschermd worden, maar feiten helder gepresenteerd zijn. Voor het melden wordt gebruik gemaakt van de applicatie **TriasWeb**.

Beeldmateriaal
Soms maken we beeldmateriaal van cliënten (opnames en foto's) met als doel het verbeteren van de dienstverlening aan de cliënt. Voordat de opname gemaakt wordt, wordt bepaald waarvoor de opname nodig is. Dit wordt vastgelegd in het cliëntdossier. De cliënt of vertegenwoordiger moet vooraf geïnformeerd worden en toestemming geven voor het maken van beeldmateriaal. Het beeldmateriaal is onderdeel van het cliëntdossier. Voor het veilig opslaan en delen van beeldmateriaal wordt gebruik gemaakt van de applicatie **arQive**.

Behandeling Hersenz
Voor de doelgroep van cliënten met niet aangeboren hersenletsel is via een landelijk samenwerkingsverband tussen een aantal instellingen een behandeling ontwikkeld. Deze behandeling wordt ondersteund door de applicatie **Jouw Omgeving**. M.b.v. de applicatie worden bijzondere persoonsgegevens van cliënten vastgelegd en gegevens van betrokken medewerkers en verwanten van cliënten.

Cliëntcommunicatie
Onze afdeling communicatie onderzoekt opties om de digitale communicatie met cliënten en verwanten te stroomlijnen. De bijbehorende pakketkeuze is voorzien in 2023.

2.3 Gegevensbescherming

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.

Bewaartermijnen
(Medische) behandelgegevens dienen wij op grond van wetgeving 20 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 20 jaar na de 'uitstroom' (als gevolg van overlijden, vertrek naar een andere zorgaanbieder of anderszins) van de cliënt uit onze organisatie. Hierbij past de kanttekening dat we niet kunnen overzien binnen welke applicaties we – gelet op de digitale ontwikkelingen – we over 20 jaar nog kunnen 'lezen'. We bewaren deze gegevens ook omdat zorgkantoren daar op basis van hun wettelijke taken tijdens hun zogenaamde materiële controle naar kunnen informeren. Vanwege technische beperkingen in de applicatie Plan Care kunnen we sommige gegevens (nog) niet 'deleten'. We zetten ze daarom na ommekomst van de genoemde termijn in een aparte archiefmap, 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 wordt uitgevoerd door de beheerders van het ECD **Ons Dossier**.

2.4 Delen gegevens

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 de zorgkantoren verplicht de door ons aangeleverde informatie over de door cliënten genoten zorg door te leveren aan het Centraal Administratiekantoor, dat de zogenaamde eigen bijdrageregelingen voor de zorgsector uitvoert. Cliënten die worden ondersteund vanuit Pgb-gelden worden geacht zelf de relevante informatie aan de Sociale Verzekeringsbank te leveren. 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 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. Voor de declaratie van de behandelkosten van onze paramedici richting zorgverzekeraars maken we gebruik van **Ons Dossier**.

Digitaal cliëntportaal
Cliënten en door hen (of hun wettelijke vertegenwoordigers) aangewezen derden kunnen via het digitaal portaal **Caren** online inzage krijgen in delen van hun eigen dossier: de agenda, het ondersteuningsplan en de dagrapportage. Om in te kunnen loggen wordt gebruik gemaakt van een inlognaam en een zelfgekozen wachtwoord in combinatie met een verificatiecode per sms. Via **Caren** kunnen cliënten en hun vertrouwenspersonen communiceren met hun persoonlijk begeleider. De beheerder van het **Caren**-account is zelf verantwoordelijk voor het beheer van het door hen ingestelde wachtwoord en het aantal derden (vertrouwenspersonen) dat toegang heeft. De cliënt of vertegenwoordiger kan de 'aanwijzing' van een derde ook intrekken. Daarvoor geldt dezelfde procedure als voor 'aanwijzen'.

3.1 Verwerking gegevens medewerkers en vrijwilligers

Via diverse gekoppelde applicaties (met name **SDB HR, SDB Planning, Hello ID, Azure AD, SDB Leren en Ontwikkelen en Ons Dossier**) 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 FIT-gesprekken, 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, bieden we verzuim- en loopbaanbegeleiding en regelen we de toegang tot benodigde applicaties. De grondslag is dus de gesloten arbeidsovereenkomst in combinatie met wettelijke verplichtingen.

Vrijwilligers en stagiaires

Een bijzondere categorie medewerkers wordt gevormd door vrijwilligers. Met hen sluiten we een vrijwilligersovereenkomst. We registreren contactgegevens, 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 stagelopen. Ook hier vormt de gesloten overeenkomst de grondslag voor de verwerking. Een jaar nadat de vrijwilligers-overeenkomst is geëindigd, verwijderen we de betrokken gegevens. We beschikken overigens niet over een centraal register van vrijwilligers.

Leerlingen

Ten behoeve van de begeleiding van leerlingen houden de praktijkbegeleiders middels een Excel-bestand een dossier bij waarin persoonsgegevens worden opgeslagen, inclusief beoordelingen en voortgang leertrajecten. Hierbij wordt gebruik gemaakt van de applicatie Competent.

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.

3.2 Verwerkingsactiviteiten en doelbinding

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 salto tags. Via de verwerker kunnen we ook nagaan welke medewerker het voertuig bestuurd heeft wanneer er een verkeersovertreding is begaan als ons daarvoor een boete (administratieve sanctie) wordt opgelegd of wanneer bijvoorbeeld er een klacht van derden over het rijgedrag binnen komt. 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.

Loonbeslag

Om te voldoen aan wettelijke verplichtingen registreren we gegevens m.b.t. loonbeslag. Gegevens over loonbeslagen verwijderen we uit onze systemen zodra het loonbeslag is opgeheven.

Verzuim & Re-integratie
Ten behoeve van het beheer van de organisatie en het nakomen van wettelijke verplichtingen worden persoonsgegevens van medewerkers verwerkt die te maken hebben met verzuim en re-integratie. We gebruiken daarvoor de applicaties **Visma Verzuim en SDB-HR**.

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.

3.3 Gegevensbescherming

Toegang tot gegevens medewerkers
De toegang tot de gegevens van medewerkers is beperkt tot leidinggevenden en een aantal medewerkers die uit hoofde van functie ondersteuning bieden op het servicecentrum. Toegangsrechten zijn vastgelegd in **SDB** middels zogenoemde autorisatiematrixen. Ten behoeve van het roosteren hebben een aantal medewerkers toegang tot de voor het roosteren relevante gegevens van medewerkers. Het gaat hierbij niet om bijzondere of gevoelige persoonsgegevens. Rechten van roostermedewerkers zijn eveneens vastgelegd in **SDB** middels een autorisatiematrix.

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.

Bewaartermijnen
Als de medewerker uit dienst gaat, verwijderen we de gegevens 7 jaar na datum uitdiensttreding. We sluiten daarmee aan op de voorschriften die in de Wet op de Rijksbelastingen zijn opgenomen. De Dienst 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 **SDB Leren & Ontwikkelen** – 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.

3.4 Delen gegevens

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 medewerker tevredenheidsonderzoek uitvoert en instrumentarium voor zogenaamde teamreflecties verzamelt, bewerkt en terug levert.

Digitaal medewerkersportaal
Medewerkers kunnen via het digitale **Medewerkersportaal** van SDB met een inlognaam en een zelfgekozen wachtwoord online inzage krijgen in het eigen personeelsdossier, het salaris en het verlofoverzicht. Medewerkers zijn zelf verantwoordelijk voor het beheer van het door hen ingestelde wachtwoord.

4. Verwerking gegevens zakelijke contacten

(Een deel van onze) Leveranciers, dienstverleners etc. registreren we in een door ons secretariaat beheerd **Excel-**bestand. In een aantal gevallen maken we daartoe ook mailgroepen aan. 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. Het gaat hierbij niet om bijzondere persoonsgegevens en de verwerking kent een laag privacy-risico. Het aantal personen dat toegang heeft tot het bestand is na een kritische evaluatie beperkt tot medewerkers van het directiesecretariaat en de afdeling Communicatie.

5. Enkele specifieke verwerkingen

Managementinformatie
Dagelijks worden gegevens uit **Ons Dossier** (cliënten), **SDB** (medewerkers) en **UBW** (financiën) bij elkaar gebracht in ons datawarehouse om hiermee vervolgens managementinformatie beschikbaar te stellen via de Business Intelligence Tool **Infent**. Het betreft hoofdzakelijk geaggregeerde informatie op het niveau van de kostenplaats. **Infent** wordt ook gebruikt voor informatievoorziening met betrekking tot medewerkers (functie, dienstverband, schaal, salaris) en cliënten (actuele ondersteuningsplannen, cliëntervaringen via Dit vind ik ervan!). Hierbij worden ook bijzondere persoonsgegevens verwerkt. We verwachten dat we **Infent** ook kunnen benutten om invulling te geven aan het beginsel van ‘datagedreven zorg’.

Zorgtechnologie
We maken steeds vaker gebruik van zorgtechnologie die moet leiden tot meer comfort en veiligheid voor de cliënt, aan besparingen op de inzet van de factor arbeid, aan verbetering van de arbeidsomstandigheden van medewerkers of aan meerdere van deze doelstellingen tegelijkertijd. Denk aan de slimme sok (HUME; signaleren spanningsopbouw en voorkomen escalatie/agressie), slim incontinentiemateriaal (Abena en Tena), de Nightwatch (epilepsiedetectie) en dwaaldetectie. Deze ontwikkelingen hebben uiteraard invloed op het applicatielandschap en daarmee ook op beleid en praktijk rond informatiebeveiliging.

Meldingen Helpdesk en Servicedesk
In de applicatie **Topdesk** worden gegevens verwerkt met betrekking tot storingen en andere functioneringsproblemen rond vastgoed. Voor incidenten m.b.t. de computer en het netwerk ligt de verantwoordelijkheid voor de verwerking bij de Helpdesk ICT. Voor incidenten met betrekking tot **Ons Dossier**, **Plancare** en andere zorgapplicaties ligt deze bij de Servicedesk Digitale Zorg. Sinds kort kunnen medewerkers zelf ook storingen via **Topdesk** vastleggen met betrekking tot huisvesting. In een enkel geval worden persoonsgegevens functioneel op basis van de melding vastgelegd.

Auteur: GG
Volgende evaluatie: 3/2024