Privacy beleid OmniaZorg

Anne De Lorenzo, www.omniazorg.nl

info@omniazorg.nl

Inhoud

1 Inleiding

OmniaZorg is een thuiszorgorganisatie, gevestigd te Zoetermeer. OmniaZorg levert de zorg in de zogeheten H4 gemeenten (Delft, Westland, Rijswijk en Midden-Delfland) en H6 gemeenten (Zoetermeer, Pijnacker-Nootdorp, Leidschendam-Voorburg, Lansingerland, Voorschoten en Wassenaar) en Den Haag. De organisatie heeft ca. 140 cliënten en ca. 25 fte aan medewerkers en staf.
OmniaZorg biedt thuiszorg op maat aan iedereen die thuiszorg nodig heeft. Jong en oud, chronisch ziek of tijdelijk beperkt, ongeacht culturele of religieuze achtergrond.

OmniaZorg biedt de volgende diensten:

- Hulp in de huishouding
- Persoonlijke verzorging
- Verpleging
- Begeleiding/ondersteuning
- Opleiding en training

OmniaZorg biedt naast deze diensten ook advies en voorlichting en verwijst zorgvrager, indien nodig, door.

De Wet bescherming persoonsgegevens (Wbp) bestaat sinds 2000. Internet was nog een betrekkelijk nieuw fenomeen en privacybescherming stond nog in de kinderschoenen. Nu is privacybescherming een belangrijk onderwerp. Vanaf 25 mei 2018 geldt nog maar één privacywet in de hele Europese Unie: de Algemene Verordening Gegevensbescherming (AVG). De AVG zorgt voor versterking van de privacy rechten van burgers en daarmee voor meer verantwoordelijkheden voor organisaties die persoonsgegevens verwerken.
De AVG is rechtstreeks van toepassing in Nederland. Daar waar de Europese AVG ruimte laat voor nationale keuzes bij de uitvoering van de AVG zijn deze ingevuld in de Uitvoeringswet AVG (UAVG).

Opslag en verwerking van persoonsgegevens is noodzakelijk voor de bedrijfsprocessen van OmniaZorg. Dit dient met de grootste zorgvuldigheid te gebeuren omdat foutief gebruik of zelfs misbruik van persoonsgegevens grote schade kan berokkenen aan medewerkers, bezoekers, klanten, vrijwilligers, sponsoren, studenten (stagiaires) en andere betrokkenen bij OmniaZorg. Het kan leiden tot imago schade voor de organisatie, met alle gevolgen van dien. De Stichting hecht dan ook veel waarde aan het beschermen van de persoonsgegevens die aan haar in bruikleen worden gegeven en aan de wijze waarop persoonsgegevens worden verwerkt. Het op een juiste manier verwerken van persoonsgegevens valt onder de eindverantwoordelijkheid van het bestuur van OmniaZorg.

Met het beschrijven van de maatregelen in dit beleidsdocument neemt OmniaZorg haar verantwoordelijkheid om de kwaliteit van de verwerking van alsmede de beveiliging van persoonsgegevens te garanderen en daarmee te voldoen aan de Algemene Verordening Gegevensbescherming (AVG).

1.1 Definities

Beleid: dit beleid met betrekking tot het verwerken van persoonsgegevens bij OmniaZorg.

Betrokkene: een natuurlijke persoon op wie een persoonsgegeven betrekking heeft.

Derde Partij: Ieder ander natuurlijke of rechtspersoon, niet zijnde de betrokkene, de verwerkingsverantwoordelijke of de verwerker, of enig persoon die onder rechtstreeks gezag valt van de verwerkingsverantwoordelijke of de verwerker en gemachtigd is om persoonsgegevens te verwerken.

Inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (data lek).

Persoonsgegeven: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd. Ofwel: Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (zoals naam, adres, geboortedatum, telefoonnummer, emailadres). Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren en gezondheid.
Het Burgerservicenummer (BSN) is volgens de wet geen bijzonder persoonsgegeven, echter omdat dit nummer (in Nederland) persoonsinformatie bevat, wordt het wel als gevoelige informatie beschouwd. In de zorg is het gebruik van het BSN bij communicatie over een cliënt wettelijk geregeld.

Privacy by design: Het beheer van de gehele levenscyclus van persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen, waarbij stelselmatig aandacht wordt besteed aan allesomvattende waarborgen m.b.t. nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijdering van de persoonsgegevens.

Privacy Impact Assessment/Privacy effectbeoordeling: Een tool dat helpt bij het identificeren van privacy risico's en de handvatten levert om deze risico's te verkleinen tot een acceptabel niveau.

Uitvoeringsverantwoordelijke: het bestuur van de OmniaZorg die het doel van en middelen voor de verwerking van persoonsgegevens bepaalt.

Verwerker: een door de OmniaZorg ingeschakelde (derde) partij die ten behoeve van de Stichting persoonsgegevens verwerkt.

Verwerkersovereenkomst: de overeenkomst die OmniaZorg sluit met de verwerker. Dit doen wij ter garantie dat de verwerker zorgvuldig omgaat met de persoonsgegevens.

Verwerking: 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.

1.2 Reikwijdte en doelstelling van het Beleid

Het Beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen de brede bedrijfsvoering van OmniaZorg waaronder in ieder geval alle medewerkers, cliënten, bezoekers, vrijwilligers, studenten, financiers, sponsoren en externe relaties (inhuur/outsourcing).

In het beleid ligt de nadruk op de geheel of gedeeltelijk geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van OmniaZorg alsmede op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Eveneens is het beleid van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Bij OmniaZorg wordt het beschermen van persoonsgegevens breed geïnterpreteerd. Er is een belangrijke relatie en gedeeltelijke overlap met het aanpalende beleidsterrein informatiebeveiliging, waarbij het gaat om de beschikbaarheid, integriteit en de vertrouwelijkheid van data, waaronder persoonsgegevens. Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht.

Het beleid bij OmniaZorg heeft tot doel de kwaliteit van verwerkingen en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.

Beoogd wordt de persoonlijke levenssfeer van de betrokkene zoveel mogelijk te respecteren. De gegevens, die betrekking hebben op een betrokkene dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik dan wel misbruik op basis van het fundamenteel recht op bescherming van zijn/haar persoonsgegevens. Dit brengt met zich mee dat het verwerken van persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat persoonsgegevens veilig zijn bij OmniaZorg

Doelstelling van het beleid voor OmniaZorg is concreet het volgende:

- *Het bieden van een kader:* het beleid biedt een kader om (toekomstige) verwerkingen van persoonsgegevens te toetsen aan een vastgestelde norm; en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen.
- *Het stellen van normen:* de basis voor de beveiliging van persoonsgegevens ligt vast in het Informatiebeveiligingsbeleid, gebaseerd op NEN 7510/12/13.
- *Het nemen van de verantwoordelijkheid*: door het bestuur van de Stichting door de uitgangspunten en de organisatie van het verwerken van persoonsgegevens vast te leggen voor OmniaZorg.
- *Daadkrachtige implementatie* van het beleid door duidelijke keuzes in maatregelen te maken en actieve controle toe te passen op de uitvoering van de beleidsmaatregelen.
- *Compliant zijn/worden* met de Nederlandse en Europese wetgeving

Naast bovenstaande concrete doelstellingen is een meer algemeen doel het creëren van bewustwording van het belang en de noodzaak van het beschermen van persoonsgegevens, mede ter vermijding van risico's als gevolg van het niet compliant zijn met de relevante wet- en regelgeving.

2 Beleidsprincipes Verwerking Persoonsgegevens

2.1 Beleidsuitgangspunt en -principes

Algemeen beleidsuitgangspunt is dat persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke en zorgvuldige wijze worden verwerkt. Hierbij dient een goede balans te worden aangebracht tussen het belang van OmniaZorg om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens.

Om aan bovenstaand beleidsuitgangspunt te voldoen gelden de volgende principes:

Een Verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals genoemd in artikel 5 Algemene Verordening Gegevensbescherming (AVG).

- Persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.
- Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking geformuleerd.
- De verwerking van persoonsgegevens moet toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ("minimale gegevensverwerking").
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.
- Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen.
- Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
- Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen.
- Iedere betrokkene heeft recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van de in de afzonderlijke verwerkingen hem betreffende persoonsgegevens, en heeft het recht van bezwaar, zoals geformuleerd in hoofdstuk 8 van dit Beleid.

3 Wet- en regelgeving

Bij OmniaZorg wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

3.1 Specifieke wetgeving OmniaZorg

Onderstaand een overzicht van de belangrijkste wetten waarin bepalingen omtrent opslag of verwerking van persoonsgegevens zijn opgenomen waaraan OmniaZorg zich dient te conformeren en de relatie van de wet met de AVG:

Wet	**Relatie met AVG**
Wet op de langdurige zorg (Wlz)	Vaststellen identiteit, kosteloze verstrekking van persoons- en medische gegevens, tussen en aan derde partijen
Burgerlijk Wetboek, Boek 7; Bijzondere overeenkomsten, Titel 7; Opdracht (artikelen 400 – 468), afdeling 5; de overeenkomst inzake geneeskundige behandeling (artikelen 446 -468)	Basis voor de WGBO; aangaande omgang met persoonsgegevens in relatie tot ethische vragen en medisch-wetenschappelijk onderzoek.
Wet op de Geneeskundige Behandelingsovereenkomst (WGBO)	Bewaartermijn medisch dossier: 20 jaar. Vernietiging dossier indien de client hiertoe een verzoek indient, art 7:455 lid 1 BW
Wet Zorg en Dwang (WZD)	Bewaartermijn van de beschikking van de Burgemeester obv art 7:454 BW 20 jaar of obv art 18a lid 5 WZD: vanaf 5 jaar na einde onvrijwillige zorg vernietiging binnen drie maanden indien de client daartoe een verzoek indient.
Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wab-vpz)	Art. 8: De zorgaanbieder neemt het BSN van de cliënt in zijn administratie op bij het vastleggen van persoonsgegevens met betrekking tot de verlening van zorg.
Wet op de identificatieplicht (WID), Politiewet	Verplichting tot identificatie met een geldig identiteitsbewijs voorafgaand aan de zorgverlening. Het maken van een volledige kopie van het identiteitsbewijs van een cliënt/bewoner is niet toegestaan.
Wet cliëntenrechten bij elektronische verwerking van gegevens in de zorg	Regelt de rechten en plichten voor elektronische gegevensuitwisseling tussen zorgverleners
Wet kwaliteit, klachten en geschillen zorg (Wkkgz)	Art. 9 lid 1 stelt "voor een goede werking van … de zorg … worden in een register, zonder toestemming van betrokkene, persoonsgegevens verwerkt betreffende intern gemelde incidenten, waaronder gegevens betreffende de gezondheid".

Voor administratie betreffende medewerkers gelden o.a. deze wetten met betrekking tot de verwerking van persoonsgegevens:

Wet	**Relatie met AVG**
Burgerlijk Wetboek (arbeidsovereenkomst)	Welke persoonsgegevens zijn nodig om de arbeidsovereenkomst te kunnen uitvoeren? Wordt er niet meer vastgelegd dan nodig? Staan alle processen hiervoor in het register verwerkingen?
CAO VVT (collectieve arbeidsovereenkomst)	Vastlegging van persoonsgegevens conform CAO
Wet op de loonbelastingen (WL)	Art . 29 WL: kopie legitimatiebewijs medewerkers, bewaren tot minstens 5 jaar na het kalenderjaar van uit dienst treden. Ook de bewaartermijn voor salarisgegevens is gedefinieerd; deze gegevens dienen 7 jaar bewaard te blijven.

Dit is geen volledige lijst. Er zijn meer wetten van toepassing. De AVG is derhalve niet te beschouwen als geïsoleerde nieuwe wetgeving; het bepaalt en versterkt bestaande wetgeving op privacy regels.

3.2 Algemene Verordening Gegevensbescherming

OmniaZorg heeft de wettelijke vereisten - waaronder het rechtmatig en zorgvuldig verwerken van persoonsgegevens en nemen van passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking van data c.q. persoonsgegevens - geïmplementeerd door middel van het beleid.

3.3 Telecommunicatiewet

De maatregelen die OmniaZorg genomen heeft om aan de privacywetgeving te voldoen zijn tevens toereikend om de bescherming van de persoonlijke levenssfeer van gebruikers op openbare netwerken te waarborgen.

4 Rollen, verantwoordelijkheden en toegang Verwerking Persoonsgegevens

Om de verwerkingen van persoonsgegevens gestructureerd en gecoördineerd op te pakken wordt bij OmniaZorg een aantal rollen onderkend die aan functionarissen in de organisatie worden toegewezen. Per rol/ functie wordt bepaald tot welke persoonsgegevens deze functie toegang geeft.

4.1 De Bestuurder

De bestuurder is eindverantwoordelijk voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen OmniaZorg en stelt het beleid, de maatregelen en de procedures op het gebied van verwerkingen vast. Hij heeft toegang tot de persoonsgegevens van medewerkers, algemene gegevens maar ook BSN en contracten.

4.2 Portefeuillehouder beveiliging persoonsgegevens

De portefeuillehouder beveiliging persoonsgegevens is het bestuurslid dat privacy in portefeuille heeft. Hij is eindverantwoordelijk voor beveiliging van persoonsgegevens binnen OmniaZorg. De rol van portefeuillehouder is nu belegd bij de voorzitter van de Raad van Bestuur. Er is voor deze functie geen toegang tot persoonsgegevens nodig. Het kan zijn dat deze persoon in een andere rol wel toegang heeft tot persoonsgegevens.

4.3 Functionaris Gegevensbescherming/ Privacy Officer/Privacy Functionaris

OmniaZorg heeft de mogelijkheid zelf de rol van interne toezichthouder op de verwerking van persoonsgegevens in te vullen. Deze toezichthouder wordt Functionaris Gegevensbescherming (FG) genoemd. De benoeming van een FG is verplicht indien:

1. Verwerking wordt uitgevoerd door overheidsinstanties of -organen (hieronder vallen ook publiekrechtelijke instellingen en organisaties, nader te definiëren in het nationale recht),
2. Er verwerkingen worden uitgevoerd die regelmatige en stelselmatige observatie vereist,
3. Er grootschalige verwerking van bijzondere persoonsgegevens en strafrechtelijke gegevens plaatsvindt.

De AP adviseert de zorgsector over hoe de grootschaligheid van verwerkingen voor de sector te begrijpen. Een eenduidige richtlijn is echter niet voorhanden. Eind 2018 heeft de AP het volgende advies afgegeven:
“De verwerking van persoonsgegevens door ziekenhuizen, huisartsenposten en zorggroepen interpreteert de Autoriteit Persoonsgegevens (AP) altijd als grootschalig. Voor alle overige zorgaanbieders geldt dat zij grootschalig persoonsgegevens verwerken als zij van meer dan 10.000 patiënten gegevens verwerken in één informatiesysteem. Met deze uitleg heeft de AP nu voor alle sectoren binnen de zorg verduidelijkt wanneer er sprake is van grootschalige gegevens-verwerking” (AP, nieuwsbericht, 11 december 2018).

Deze bepaling laat vele zorgaanbieders vrij een FG aan te stellen. Elke zorgaanbieder dient daarom, op juiste inschatting van de verwerking van persoonsgegevens, de eigen conclusie te trekken of een PF noodzakelijk is. Daarbij mag in acht worden genomen dat een FG ook een externe partij kan zijn. De taken en rollen van een FG bij een zorgaanbieder zijn evident van belang. Het verdient daarom aanbeveling, op een wijze naar keuze, een FG in te zetten.

Het is eveneens mogelijk een Privacy Officer (PO) aan te stellen. De PO bewaakt het beleid en stelt nadere regels en protocol op. De PO houdt in zijn rol toezicht op de toepassing en naleving van de Algemene Verordening Gegevensverwerking (AVG) (zie Bijlage 1: functiebeschrijving FG en PO). Het is een vrije keuze een PO in te zetten.
OmniaZorg heeft ervoor gekozen om de twee functies samen te brengen in de functie Privacy Functionaris (PF). Deze is de interne toezichthouder op de verwerking van persoonsgegevens. De PF bewaakt het beleid en stelt nadere regels en protocollen op en houdt in zijn rol toezicht op de toepassing en naleving van de Algemene Verordening Gegevensverwerking (AVG).

FG, PO of PF; allen bekleden een onafhankelijke positie. Volgens de principes van Good Governance wordt de onafhankelijke positie gewaarborgd door deze hiërarchisch los te koppelen van de bedrijfsvoering, met een directe (verantwoordings-)lijn richting de bestuurder en de Raad van Toezicht.
Deze functionaris heeft geen toegang tot persoonsgegevens van medewerkers of cliënten, behalve als er een incident is en er onderzoek moet plaatsvinden naar bijvoorbeeld een datalek. De toegang zal altijd beperkt blijven tot het minimum wat nodig is (proportioneel).

OmniaZorg kiest voor een Privacy Functionaris omdat dit past bij de omvang van de organisatie.

4.4 Regiehouder ICT

De regiehouder ICT is er verantwoordelijk voor dat de applicatie en bijbehorende ICT-faciliteiten een goede ondersteuning bieden aan het proces waar deze verantwoordelijk voor is en voldoet aan het beleid. Dit betekent dat de systeemeigenaar ervoor zorgt dat zowel nu, als in de toekomst de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers en aan wet- en regelgeving.
OmniaZorg heeft deze taak belegd bij de manager Finance & Control. Deze heeft toegang tot alle systemen en daarmee tot de gegevens van de medewerkers en cliënten. Er wordt door haar niet meer dan noodzakelijk is ingezien (proportioneel). Zij kent, binnen de systemen, rechten toe aan de medewerkers, dus wel of niet in SDB Cliënten en SDB Planning en de personeel/ salaris administratie.

4.5 (Integraal) Managers

Het creëren van bewustwording en de naleving van het beleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

- Ervoor te zorgen dat zijn medewerkers op de hoogte zijn van het beleid;
- Toe te zien op de naleving van het beleid door zijn medewerkers;
- Periodiek het onderwerp privacy onder de aandacht te brengen in werkoverleggen.

Met behulp van het Protocol bescherming persoonsgegevens (zie bijlage 2: Privacy protocol 2021) wordt er geregeld aandacht gevraagd voor dit onderwerp. Per functie wordt er een beoordeling gemaakt of er toegang nodig is tot (bijzondere) persoonsgegevens. Dit doet de Manager Finance & Control.

4.6 Medewerkers van OmniaZorg die met persoonsgegevens werken

Medewerkers van de loonadministratie: deze medewerkers verwerken persoonsgegevens van medewerkers die nodig zijn om de salarissen uit te betalen. Zij hebben naast de algemene

persoonsgegevens, zoals adresgegevens ook toegang tot bankgegevens en BSN. Zij hebben geen toegang tot cliënten gegevens.

Medewerkers van HRM: zij hebben toegang tot de algemene persoonsgegevens van medewerkers, BSN en bankgegevens. Zij verzorgen de contracten en zaken rond ziekmeldingen en re-integratie. Zij hebben geen toegang tot cliënten gegevens.

Planners: zij hebben toegang tot alle gegevens van de cliënten die nodig zijn om een goede indeling van zorgroutes en begeleiding van cliënten te maken, via ECD Planning. Zij hebben geen toegang tot medewerker persoonsgegevens, behoudens contactgegevens, zoals tel. nr. en emailadres.

Zorgmedewerkers: zij hebben toegang tot algemene en bijzondere persoonsgegevens van de cliënten via SDB ECD. Zij kunnen in het zorgdossier van de cliënten. Zij gaan hier zorgvuldig mee om en bekijken alleen die gegevens die zij voor hun taak nodig hebben. Bij teambesprekingen wordt hier aandacht aan besteed. Zij hebben geen toegang tot persoonsgegevens van hun collega's, behoudens contactgegevens, zoals tel.nr. en emailadres.

Alle overig personeelsleden kunnen niet in het systeem van SDB en hebben geen toegang tot medewerker gegevens behalve de telefoonlijst en emailadressen van medewerkers.

5 Implementatie Beleid

Het bestuur van OmniaZorg is verantwoordelijk voor verwerkingen van persoonsgegevens waarvan zij het doel en de middelen voor de verwerking vaststelt. Zij wordt aangemerkt als de **verwerkingsverantwoordelijke** in de zin van de AVG.

De feitelijke verwerking van persoonsgegevens wordt echter binnen verschillende organisatie-eenheden bij OmniaZorg uitgevoerd. Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term 'governance'. OmniaZorg bewerkstelligt dat de omgang met persoonsgegevens georganiseerd is en dat hierover verantwoording kan worden afgelegd. Een goed corporate governance-beleid draagt zorg voor de rechten van alle betrokkenen.

5.1 Verdeling van de verantwoordelijkheden

- Het zorgvuldig ***verwerken*** van persoonsgegevens is een **lijnverantwoordelijkheid;** de lijnmanagers zijn primair verantwoordelijk voor een zorgvuldige verwerking van persoonsgegevens op hun afdeling/eenheid. Onder de lijnverantwoordelijkheid valt ook de taak om het beleid met betrekking tot de verwerking van persoonsgegevens te communiceren met alle relevante partijen.

- Het zorgvuldig ***omgaan*** met persoonsgegevens is **ieders verantwoordelijkheid.** Er wordt van medewerkers en bezoekers verwacht dat ze zich integer gedragen. Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies van OmniaZorg of van individuen. Het is om deze reden dat er gedragscodes zijn geformuleerd en geïmplementeerd (zie bijlage 2: Privacy protocol 2021 en bijlage 3: Privacy verklaring OmniaZorg 2021).

5.2 Inpassing in de governance /afstemming met aanpalende beleidsterreinen

Om de samenhang in de organisatie met betrekking tot gegevensbescherming goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van verwerking van persoonsgegevens binnen de verschillende onderdelen op elkaar af te stemmen, is het belangrijk om gestructureerd overleg te voeren over het onderwerp privacy op verschillende niveaus.

Op **strategisch niveau** wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van privacy-aspecten. (Het strategisch niveau wordt ingevuld in het Management Team (MT)

Op **tactisch niveau** wordt de strategie vertaald naar plannen, te hanteren normen, en evaluatiemethoden. Deze plannen en instrumenten zijn sturend voor de uitvoering. (Het tactisch niveau wordt ingevuld in het afdelingsoverleg).

Op **operationeel niveau** worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. (Het operationeel niveau wordt ingevuld in de teams).

5.3 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Noodzakelijk is het om bij OmniaZorg het bewustzijn

voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag wordt aangemoedigd.

OmniaZorg zoekt aansluiting bij landelijke bewustwordingscampagnes en/of bij elders ontwikkelde (beveiligings)campagnes. Bijvoorbeeld worden posters op kantoren opgehangen of filmpjes getoond tijdens overleg als input voor discussie en reflectie. Er is een privacy protocol gemaakt die besproken wordt tijdens teambesprekingen.

5.4 Controle en naleving

Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De PF initieert, indien van toepassing gezamenlijk met een (externe) auditor en/of security officer, de controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens.

Eventuele externe controles worden uitgevoerd door onafhankelijke accountants. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale Planning & Control cyclus.

Mocht de naleving op de bescherming van data- en privacygegevens ernstig tekortschieten, dan kan OmniaZorg de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten OmniaZorg maken het noodzakelijk om periodiek te bezien of men nog voldoende op koers zit met het beleid.

6 Rechtmatige en zorgvuldige Verwerking van Persoonsgegevens

6.1 Grondslag, doelbinding en belangenafweging

Het verwerken van persoonsgegevens moet gebaseerd zijn op een van de wettelijke gronden zoals beschreven in artikel 6 van de Algemene Verordening Gegevensverwerking. De verwerkingsverantwoordelijke omschrijft vooraf de doeleinden voor de verwerking. Deze doeleinden zijn concreet en specifiek geformuleerd. Bij elke verwerking wordt getoetst in hoeverre het verwerken van persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen en wordt gekeken naar de rechtmatigheid, de doelbinding[1], de datakwaliteit en de proportionaliteit.

OmniaZorg treft de nodige maatregelen om te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn.

Bij (onderzoeks-)projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met de inrichting van privacy door een Privacy Impact Assessment (PIA) uit te voeren.

OmniaZorg hanteert bij de implementatie de principes “Privacy by Design” en “Privacy by Default”. De letterlijke vertaling van Privacy by Design is: gegevensbescherming door ontwerp. Het idee is om al in een vroeg stadium zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens af te dwingen. Het houdt in dat er al bij de ontwikkeling van producten en diensten aandacht moet zijn voor privacy. In het bijzonder bij ICT-producten en -diensten gaat het erom dat al in het ontwikkelproces gebruik gemaakt wordt van privacy-verhogende maatregelen (ook wel privacy enhancing technologies of PET genoemd).
Privacy by Default kan gezien worden als een onderdeel van Privacy by Design. Privacy by Default vereist dat de standaardinstellingen altijd zo privacy-vriendelijk mogelijk zijn.
Er moet voor gezorgd worden dat persoonsgegevens nooit standaard openbaar zichtbaar zijn. Het meest sprekende voorbeeld is wellicht een profiel op social media. Dit mag wel openbaar zijn, maar slechts als een gebruiker daar eerst zélf actief voor kiest (Uitleg op nldigital.nl).
OmniaZorg werkt met het Privacy by Design Framework. Zie hiervoor bijlage 4 (blz. 30).

6.2 Melden en documenteren van verwerkingen

Een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens dient gemeld te worden bij de PF van OmniaZorg. De PF beoordeelt de rechtsgeldigheid van de registratie en draagt zorg voor adequate documentatie.

De verwerkingen worden voldoende gedocumenteerd (register verwerkingen) en gepubliceerd op voor de betrokkenen toegankelijke media met vermelding van het doel van de registraties en de verantwoordelijken (= privacy verklaring). En dat wordt bijgesteld indien daar reden voor is. De actuele versie is altijd online te vinden op de website van OmniaZorg, onder het kopje Privacy.

[1] *Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen*

6.3 De organisatie van de beveiliging

OmniaZorg draagt zorg voor een adequaat beveiligingsniveau en past technische en organisatorische maatregelen toe voor de beveiliging van persoonsgegevens tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen zijn er mede op gericht onnodige c.q. onrechtmatige verzameling en verwerking van persoonsgegevens te voorkomen.

Een risicoanalyse op privacybescherming en informatiebeveiliging maakt deel uit van het intern risicobeheersings- en controlesysteem van OmniaZorg. Jaarlijks wordt er een privacy audit uit gevoerd aan de hand van het Privacy by Design Framework (Bijlage 4).

6.4 Geheimhouding

Bij OmniaZorg worden alle persoonsgegevens als vertrouwelijk geclassificeerd. Eenieder behoort de vertrouwelijkheid van persoonsgegevens te kennen en daarnaar te handelen. Ook personen voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennisnemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

6.5 Bewaartermijnen/ vernietigingstermijnen per soort gegeven

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt. Persoonsgegevens dienen na het verlopen van de bewaartermijn[2] buiten het bereik van de actieve administratie gebracht te worden.
OmniaZorg zal de persoonsgegevens na het verlopen van de bewaartermijn vernietigen of, indien de persoonsgegevens bestemd zijn voor historische, statistische of wetenschappelijke doeleinden, in een archief bewaren (cf. UAVG art.24).
Jaarlijks in maart wordt het opschonen gedaan door de medewerker systeembeheer. Zij overlegt met SDB (de leverancier van het ECD) hoe dit moet gebeuren.

6.6 Bijzondere Persoonsgegevens

Het verwerken van bijzondere persoonsgegevens is in beginsel verboden, tenzij er sprake is van een wettelijke grondslag, uitdrukkelijke toestemming van de betrokkene of een zwaarwegend algemeen belang. Tevens gelden zwaardere eisen voor de beveiliging van deze persoonsgegevens. Daar waar de basisbescherming niet voldoende is moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen.

Onder bijzondere persoonsgegevens vallen gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke gegevens. Conform de UAVG, art. 30 lid 3 kan OmniaZorg gegevens over de gezondheid verwerken, voor zover de verwerking **noodzakelijk** is met het oog op goede verzorging van de betrokkene. Deze gegevens worden alleen verwerkt door medewerkers die het beroepsgeheim dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht.

[2] Bewaartermijnen kunnen wettelijk zijn bepaald, zoals bij financiële gegevens of archivering, maar ze kunnen ook zijn vastgelegd door OmniaZorg, bijvoorbeeld in een overeenkomst tussen OmniaZorg en de betrokkenen.

Indien de noodzakelijkheid wordt aangetoond kan verwerking van bijzondere persoonsgegevens bij het geheel van goede verzorging van betrokkene plaatsvinden, conform UAVG art. 30 lid 5.

Indien de noodzakelijkheid niet direct kan worden aangetoond maar de kennis van culturele identiteit (waaronder ook spreektaal) en/of religie voorwaardelijk is voor de juiste en goede zorg wordt uitdrukkelijk toestemming gevraagd deze gegevens te verwerken.

6.7 Doorgifte Persoonsgegevens aan Derden

6.7.1 Uitbesteden van Verwerking aan een Verwerker.

Indien OmniaZorg persoonsgegevens laat verwerken door een verwerker, wordt de uitvoering van verwerkingen geregeld in een schriftelijke overeenkomst tussen OmniaZorg, de verwerkingsverantwoordelijke, en de verwerker.
OmniaZorg vermeldt de verwerker en de aanwezigheid van de verwerkersovereenkomst in het Register Verwerkingen.

6.7.2 Doorgifte Persoonsgegevens binnen de Europese Unie

OmniaZorg verstrekt persoonsgegevens alleen aan derden, als deze doorgifte is gebaseerd op een wettelijke grondslag.

Met betrekking tot bijzondere persoonsgegevens worden deze niet aan derden verstrekt zonder expliciete toestemming van de betrokkene.

6.7.3 Doorgifte Persoonsgegevens buiten de Europese Unie (inclusief de EEA)

OmniaZorg verstrekt Persoonsgegevens alleen aan derden die zich bevinden in een land buiten de Europese Unie indien dat land in zijn geheel of dat bedrijf/die instelling specifiek een passend beschermingsniveau waarborgt.

Als passend beschermingsniveau hanteert OmniaZorg:

- De algemene lijst van landen met passend beschermingsniveau gepubliceerd door de Europese Commissie[3]
- Privacy Shield voor bedrijven in de Verenigde Staten, gepubliceerd door de Europese Commissie i.s.m. de US Department of Commerce[4]

OmniaZorg verstrekt persoonsgegevens alleen aan instellingen in landen zonder passend beschermingsniveau waarvoor zij een vergunning van de Minister van Justitie & Veiligheid heeft verkregen, dan wel waarmee o.b.v. een modelcontract (als opgesteld door de Europese Commissie) een contract is aangegaan. In beide gevallen voorziet OmniaZorg het AP van een melding van doorgifte naar een land buiten de EU.

6.7.4 Lijst van (niet limitatieve) derden met wie OmniaZorg persoonsgegevens uitwisselt.

- Pensioenfonds
- Arbodienst
- Overheidsinstellingen (b.v. UWV)
- Gemeenten

[3] Deze kunt u vinden via de volgende link http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm
[4] Deze kunt u vinden via de volgende link https://www.privacyshield.gov/list

- Belastingdienst
- Scholen (i.v.m. Stage opdrachten)
- Host website
- IT-dienstverlener
- Arbodienst indien actief i.h.k.v. Wet Poortwachter
- (Huis)artsen en andere eerstelijns werkenden
- Zorgverzekeraars

7 Incidenten met betrekking tot Persoonsgegevens

Iedere vraag, klacht of melding met betrekking tot de verwerking van persoonsgegevens binnen OmniaZorg is te zien als een incident. De bekendste vorm van zo'n incident is een datalek[5]. Dit hoofdstuk beschrijft het beleid met betrekking tot de melding, registratie en afhandeling van incidenten of het vermoeden van incidenten in de reguliere bedrijfsvoering en in bijzondere omstandigheden.

7.1 Melding en registratie

Incidenten moeten gemeld worden aan de Privacy Functionaris van OmniaZorg. Dit moet zo snel mogelijk (in ieder geval binnen 24 uur na ontdekken) gebeuren. Van elk incident en de afhandeling daarvan wordt een registratie bijgehouden in het register datalekken. Een incident kan gemeld worden door iedereen die een incident ziet, ervaart of ervan hoort. Dit geldt zeker de betrokkene, een medewerker, een verwerker of een derde.

7.2 Afhandeling

Incidenten worden zo veel mogelijk doorgezet naar de verantwoordelijke afdeling of persoon en vervolgens conform de daarvoor vastgestelde procedures afgehandeld.

Als de persoonsgegevens van betrokkene(n) of de bedrijfsprocessen, de financiën of goede naam van OmniaZorg ernstig in gevaar zijn, wordt in ieder geval de bestuurder op de hoogte gesteld.

Indien sprake is van ernstige datalekken worden deze conform de in de relevante wet- en regelgeving opgenomen specifieke bepalingen over datalekken afgehandeld[6]. Zie ook het separate protocol datalekken (bijlage 5) en register datalekken. Een datalek wordt gemeld bij de raad van bestuur. Deze geeft de melding binnen 72 uur door aan de Autoriteit Persoonsgegevens (AP).

7.3 Evaluatie

Het is van belang om te leren van incidenten. Registratie van incidenten en een periodieke rapportage daarover horen thuis bij een professionele manier van verwerken van persoonsgegevens. De rapportages over incidenten met betrekking tot persoonsgegevens maken daarom een vast onderdeel uit van de jaarrapportage van het bestuur.

[5] Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben spreken we van een datalek. OmniaZorg heeft een separaat protocol datalekken.
[6] Zie tevens h*ttps://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken*

8 Rechten van betrokkenen

8.1 Informatieplicht

OmniaZorg maakt de verwerking van persoonsgegevens bekend aan betrokkenen. Dit start met de privacy verklaring op internet. Deze verklaring wordt ook besproken met (potentiële) nieuwe cliënten, medewerkers, vrijwilligers, studenten en andere betrokkenen. Medewerkers lichten in persoonlijke gesprekken met cliënten en stakeholders eveneens het door OmniaZorg gevoerde privacy beleid toe.

OmniaZorg verstrekt de betrokkene tenminste het volgende:

- De identiteit en contactgegevens van de verwerkingsverantwoordelijke, in voorkomende gevallen de Privacy Functionaris;
- De verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, alsook de rechtsgrond voor de verwerking;
- De periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria ter bepaling van die termijn;
- Het recht om de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissen van de persoonsgegevens of beperking van de hem betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid;
- Het recht om een klacht in te dienen bij de toezichthoudende autoriteit (AP);
- De ontvangers of categorieën van ontvangers van de Persoonsgegevens.

Mededeling van aanpassingen

Als het beleid in de toekomst (ingrijpend) wordt aangepast dan wel veranderd, deelt OmniaZorg deze algemeen/per individu mede, om zorgvuldige en behoorlijke verwerking te waarborgen (zie ook Hoofdstuk 9).

In het navolgende worden de rechten van betrokkenen kort benoemd. Voor de aanspraak op de rechten is het gestelde in de AVG, artikel 15 t/m 22, onverkort van toepassing.

8.2 Recht op inzage

Verzoek op inzage

Iedere betrokkene heeft recht op inzage in de hem/haar betreffende verwerkte persoonsgegevens. Een verzoek hiertoe kan schriftelijk worden ingediend bij ***info@omniazorg.nl*** **.** Bijvoorbeeld kunt u dit verzoek doen om te kijken of de gegevens juist en volledig zijn. Maar u hoeft niet uit te leggen waarom u dit verzoek doet. Overigens: in de tweede helft van 2021 wordt het cliënten portaal toegankelijk voor betrokkenen. Dan kunnen zij zelf inloggen en hun zorgdossier en persoonsgegevens inzien.

Termijn

Op het verzoek wordt zo spoedig mogelijk, maar uiterlijk binnen vier weken na indiening schriftelijk gereageerd. OmniaZorg draagt hierbij zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker.

Mededeling

Indien gegevens worden verwerkt, bevat de mededeling van OmniaZorg een volledig overzicht daarvan in begrijpelijke vorm, een omschrijving van de doeleinden van de verwerking, de categorieën van gegevens waarop verwerking betrekking heeft en de categorieën van ontvangers, alsmede beschikbare informatie over herkomst van de gegevens en de termijn van bewaring van gegevens.

Kosten

Iedere eerste aanvraag kan kosteloos worden ingediend. Per aanvullende aanvraag zal OmniaZorg een vergoeding van administratieve kosten in rekening brengen bij de betrokkene.

8.3 Recht op verbetering, aanvulling, verwijdering of afscherming

Verzoek tot verbetering, aanvulling verwijdering of afscherming

Iedere betrokkene kan met betrekking tot over hem opgenomen persoonsgegevens bij OmniaZorg van deze gegevens verzoeken die te wijzigen, verbeteren, aan te vullen, te verwijderen of af te schermen.

Bij alle registraties op vrijwillige basis zal aan de betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden. Dat houdt in dat er geen toestemming zal worden gevraagd maar dat er altijd een verzoek tot niet registreren kan worden gedaan door de betrokkene.

Termijn

OmniaZorg deelt binnen vier weken na ontvangst van het verzoek schriftelijk aan de betrokkene mede of zijn verzoek gegrond is.

Kennisgeving

Indien opgenomen persoonsgegevens van de betrokkene feitelijk onjuist zijn (niet overeenkomstig het Basisregistratie Personen; BRP), voor het doel of doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift zijn verwerkt, verbetert de gegevensbeheerder (dat kan zowel de functioneel beheerder als de verwerker zijn) deze gegevens.

Bovendien worden derden aan wie de gegevens, voorafgaand aan de correctie, zijn verstrekt hiervan in kennis gesteld. De verzoeker mag opgave verzoeken van degene aan wie OmniaZorg deze mededeling heeft gedaan.

Termijn voor uitvoering

De gegevensbeheerder zorgt ervoor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

8.4 Recht van bezwaar

Gronden voor bezwaar

In verband met zijn of haar persoonlijke omstandigheden, mag iedere betrokkene bezwaar aantekenen tegen verwerking bij OmniaZorg van zijn/haar persoonsgegevens, als deze verwerking plaatsvond op grond van:

a) de vervulling van een publiekrechtelijke taak van de gegevensbeheerder of

b) de behartiging van het gerechtvaardigd belang van OmniaZorg of van een derde aan wie de gegevens worden verstrekt.

Termijn

OmniaZorg beoordeelt binnen vier weken na ontvangst van het bezwaar of deze gerechtvaardigd is. Indien het bezwaar gerechtvaardigd is, treft OmniaZorg maatregelen die nodig zijn om de verwerking de beëindigen.

Kosten

OmniaZorg brengt naar redelijkheid kosten voor de uitvoering van het bezwaar in rekening bij de betrokkene.

8.5 Rechtsbescherming

Algemene klachten

Indien de betrokkene van mening is dat de wettelijke bepalingen inzake de privacybescherming dan wel de bepalingen van dit reglement jegens hem niet correct worden gehandhaafd, kan hij een schriftelijke klacht indienen bij het bestuur van OmniaZorg. Op de website staat een klachtenformulier dat hiervoor kan worden gebruikt.

Bezwaarmogelijkheden na indienen algemene klacht

Indien het antwoord van OmniaZorg voor de betrokkene niet leidt tot een voor hem acceptabel resultaat, heeft de betrokkene de mogelijkheid een verzoekschriftprocedure te starten bij de kantonrechter.

Bezwaarmogelijkheden na afwijzing van een verzoekschrift tot inzage

Indien OmniaZorg afwijzend heeft beslist op een verzoek tot inzage in of verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens, of OmniaZorg heeft het verzoek van de betrokkene afgewezen, heeft de betrokkene de mogelijkheid een verzoekschriftprocedure te starten bij de kantonrechter.

Termijn indienen bezwaar

Het bezwaarschrift moet binnen zes weken na ontvangst van het antwoord van OmniaZorg worden ingediend bij de kantonrechter. Indien OmniaZorg niet binnen de gestelde termijn heeft geantwoord, moet het verzoekschrift binnen zes weken na afloop van die termijn worden ingediend.

9 Tot slot

Dit beleid is vastgesteld door het bestuur van OmniaZorg dd. <datum>, na instemming|positief advies van het management team. Een review van het beleid maakt onderdeel uit van de 2-jaarlijkse plan-do-check-act cyclus van OmniaZorg. Daarin is ook een controle op de effectiviteit van de maatregelen opgenomen.

Aanpassingen van dit beleid worden aangekondigd via organisatie-brede email en de meest recente versie is gepubliceerd op de website van OmniaZorg.

Voor vragen of opmerkingen met betrekking tot dit beleid kunt u terecht bij de portefeuillehouder privacy en de Privacy Functionaris.

Bijlage 1: Functiebeschrijving FG, PO en PF

De Functionaris Gegevensbescherming (FG):

- Is onafhankelijk toezichthouder op de toepassing van de AVG en krijgt geen instructies over de uitvoering van de taken;
- Informeert en adviseert over de verplichtingen die de organisatie heeft met betrekking tot de bescherming van persoonsgegevens;
- Levert een belangrijke bijdrage aan juist gebruik van persoonsgegevens door de organisatie;
- Is aangewezen door het bestuur op grond van zijn professionele kwaliteiten en deskundigheid op het gebied van de wetgeving en de praktijk;
- Mag werkzaam zijn voor meerdere organisaties;
- Heeft toegang tot alle persoonsgegevens in de organisatie en de verwerkingsactiviteiten daarvan;
- Wordt betrokken bij alles wat verband houdt met de bescherming van persoonsgegevens;
- Is verplicht tot geheimhouding en vertrouwelijkheid.

De FG heeft minimaal de volgende taken en bevoegdheden:

- Ziet toe op de naleving van wet- en regelgeving en het door het bestuur vastgestelde beleid met betrekking tot de bescherming van persoonsgegevens;
- Ziet toe op het toewijzen van verantwoordelijkheden, bewustmaking en opleiding van de organisatie op het gebied van de bescherming van persoonsgegevens;
- Geeft advies over Privacy Impact Analyses;
- Werkt samen met en treedt op als contactpersoon voor de Autoriteit Persoonsgegevens;
- In samenspraak met de privacyfunctionaris evalueren van het privacy beleid;
- Rechtstreeks rapporteren aan de bestuurder

De Privacy Officer (PO):

- Bevordert en adviseert de organisatie over de bescherming van persoonsgegevens;
- Informeert en adviseert over de verplichtingen die de organisatie heeft met betrekking tot de bescherming van persoonsgegevens;
- Stelt, indien nodig, in overleg met het betreffende organisatieonderdeel voor dat organisatieonderdeel een specifiek privacy beleid op, vraagt hierover advies aan de FG en legt het aan het bestuur voor ter vaststelling;
- Controleert en evalueert de naleving van wet- en regelgeving en het door het bestuur vastgestelde beleid met betrekking tot de bescherming van persoonsgegevens;
- Evalueert, in samenspraak met de Raad van Bestuur, het privacy beleid en doet voorstellen tot implementatie en aanpassingen van het privacy beleid;
- Heeft een coördinerende rol in het kader van datalekken;
- Is verantwoordelijk voor het inrichten en bijhouden van het register van verwerkingsactiviteiten;
- Rapporteert rechtstreeks aan de directie.

De Privacy Functionaris (PF):

Functie: De Privacyfunctionaris (PF) is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG). De PF is niet persoonlijk verantwoordelijk bij niet-naleving van de AVG, dat zijn de verwerkingsverantwoordelijke of de verwerker. De PF moet in onafhankelijkheid zijn werkzaamheden kunnen verrichten. De PF ontvangt meldingen van mogelijke datalekken, misbruik van persoonsgegevens en verloren objecten waar persoonsgegevens op staan (telefoon, laptop, dossier etc.). De PF houdt het register datalekken en het register verwerkingen bij en houdt het beleid bij. De registers worden gedeeld met de Raad van Bestuur. De PF brengt in alle relevante overleggen de privacy als agendapunt in en bespreekt actualiteiten.

Taken:

- Het maken van inventarisaties van gegevensverwerkingen;
- Meldingen van gegevensverwerkingen bijhouden in het register verwerkingen;
- Vragen en klachten van mensen binnen en buiten de organisatie afhandelen;
- Interne regelingen ontwikkelen en kennis op niveau houden door het volgen van nieuws, o.a. van de Autoriteit Persoonsgegevens (AP);
- Input leveren bij het opstellen of aanpassen van een gedragscode;
- Samenwerken met de AP;
- Meldingen van mogelijke datalekken of verlies van datadragers ontvangen en verwerken in het register datalekken en de nodige maatregelen nemen of adviseren aan de Raad van Bestuur;
- Verslagleggen en dit jaarlijks delen met de Raad van Bestuur. Het verslag wordt gebruikt voor het Jaarverslag en het Jaarplan.

Bijlage 2: Privacy protocol

Protocol bescherming persoonsgegevens

Het is OmniaZorg er veel aan gelegen om AVG-compliant te zijn. Hierin hebben we een gezamenlijke taak en verantwoordelijkheid. Om die reden vragen we jullie aandacht voor de volgende zaken. Het is zeer belangrijk dat persoonsgegevens niet te vinden zijn door personen die daar geen toegang toe mogen hebben. Ook het risico op een data-lek moeten we zien te beperken. Daarom moeten we ons houden aan een aantal regels:

1. **Wachtwoorden, die toegang geven tot organisatiesystemen en/of persoonsgegevens, worden niet gedeeld;**
2. **Documenten niet laten liggen bij de printer;**
3. **Cliënt gerelateerde documenten niet op de tafel laten liggen als je de ruimte verlaat;**
4. **Computer afsluiten als je je plaats verlaat;**
5. **Niet onnodig documenten, betreffende cliënten, printen en niet in de prullenbak gooien maar in de daarvoor aanwezige papierbakken (2x);**
6. **Neem geen geprinte documenten mee naar huis die client-/ medewerkersgegevens bevatten;**
7. **Inloggen op de organisatiesystemen alleen voor noodzakelijk gebruik. Niet aanmelden bij openbare werkplekken, zoals bibliotheken/ scholen en onbekende aanbieders;**
8. **Email: onbekende afzenders goed controleren op tekens en namen achter het @ teken. Is de naam niet aangepast, bewerkt en/of eindigt niet op .nl, .com of .org? Bij twijfel niet openen en/of er op klikken en om advies vragen;**
9. **Bij vermoeden data-lek dit melden aan privacyfunctionaris.**

Checklist bij het verlaten van de ruimte:

1. **Is de computer uit? Ben je uitgelogd?**
2. **Liggen er geen privacy gevoelige papieren op het bureau of in je laadjes?**
3. **Zijn de andere privacy gevoelige documenten in de ruimte niet toegankelijk? B.v. de kast afsluiten.**

Bijlage 3: Privacy verklaring OmniaZorg 2021

Privacyverklaring OmniaZorg

Dit is de Privacyverklaring van stichting OmniaZorg. Hierin leggen we uit welke persoonsgegevens wij verzamelen en verwerken, wat we ermee doen en welke rechten u heeft als wij uw persoonsgegevens verwerken. We vinden het heel belangrijk om zorgvuldig met uw gegevens om te gaan.

Wie zijn wij?

OmniaZorg is een thuiszorgorganisatie, gevestigd te Zoetermeer. OmniaZorg levert de zorg in de zogeheten H4 gemeenten (Delft, Westland, Rijswijk en Midden-Delfland) en H6 gemeenten (Zoetermeer, Pijnacker-Nootdorp, Leidschendam-Voorburg, Lansingerland, Voorschoten en Wassenaar), Den Haag, Leiden, Gouda en Rotterdam. Wij zijn een zorgorganisatie die zich richt op cultuursensitieve zorg.
Wij verwerken persoonsgegevens. Deze persoonsgegevens beschermen wij. U leest in deze verklaring hoe wij uw privacy beschermen. Heeft u vragen neemt u dan contact met ons op of stuur een e-mail aan info@omniazorg.nl. Dan neemt onze Privacy Functionaris contact met u op.

Cookies

Wij maken op deze website gebruik van cookies. Een cookie is een eenvoudig klein bestandje dat met pagina's van deze website wordt meegestuurd en door uw browser op uw harde schijf van uw computer wordt opgeslagen. De daarin opgeslagen informatie kan bij een volgend bezoek wee naar onze servers teruggestuurd worden.

Waarom verwerken wij persoonsgegevens?

OmniaZorg verwerkt persoonsgegevens voor het vaststellen van de identiteit van cliënten en de administratie bij het vastleggen voor verlening van zorg. Ook worden persoonsgegevens gebruikt voor onderzoek naar kwaliteit van de zorg. Persoonsgegevens die ingevuld worden op de website worden daar binnen 24 uur vanaf gehaald (bv als u reageert op een vacature).
Om goede zorg te kunnen leveren hebben we een aantal persoonsgegevens nodig. Alleen als die gegevens echt nodig zijn vragen wij u om uw gegevens. Soms vragen wij, als de AVG daarom vraagt, expliciet uw toestemming om gegevens te verwerken. Die toestemming kunt u als u dat wilt altijd weer intrekken.

Welke gegevens verzamelen en gebruiken we?

OmniaZorg verzamelt en verwerkt gewone persoonsgegevens die een persoon direct of indirect kunnen identificeren. Ofwel: alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen: naam, adres, geboortedatum. Ook verzamelen we bijzondere gegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond en gezondheid. Deze gegevens krijgen wij van u, uw begeleider of arts. We verzamelen de gegevens alleen als die echt nodig zijn.
We verzamelen de volgende gegevens:

- Gewone persoonsgegevens: naam, geboortedatum en adres;
- Gegevens over de persoonlijke situatie (woonsituatie, familie, etnische gegevens);

- BSN nummer;
- Bankrekening gegevens;
- Verzekeringsgegevens;
- Medische gegevens;
- Zorg gerelateerde gegevens.

Het Burgerservicenummer (BSN) is volgens de wet geen bijzonder persoonsgegeven, echter omdat dit nummer (in Nederland) persoonsinformatie bevat, wordt het wel als gevoelige informatie beschouwd. In de zorg is het gebruik van het BSN bij communicatie over een cliënt wettelijk geregeld. OmniaZorg gebruikt daarom ook het BSN.

Mogen wij uw persoonsgegevens verwerken?

OmniaZorg verwerkt uw persoonlijke gegevens om aan haar wettelijke taken, bevoegdheden en verantwoordelijkheden te kunnen voldoen. Wij houden ons hierbij aan de Algemene Verordening Gegevensbescherming (AVG)
Zo vindt er jaarlijks een kwaliteitsonderzoek plaats. Dit onderzoek wordt door een derde partij uitgevoerd. Het kan zijn dat u benaderd wordt om aan dit onderzoek deel te nemen. Etnische achtergrond verwerken wij in het kader van cultuur sensitieve zorg en voor medisch-wetenschappelijk onderzoek. Dit onderzoek vindt altijd geanonimiseerd plaats. Bij dit onderzoek bent u dus niet herkenbaar.

Mogen/ moeten wij uw persoonsgegevens delen met anderen?

Soms is OmnaZorg verplicht om uw persoonsgegevens door te geven. Bijvoorbeeld als er andere zorgverleners betrokken worden bij uw zorg, dan moeten wij hen goed informeren.
Daarnaast heeft OmniaZorg computerprogramma's die onderhouden moeten worden. De leveranciers van deze programma's hebben toegang tot uw persoonsgegevens.
OmniaZorg sluit een verwerkersovereenkomst af als derden persoonsgegevens kunnen inzien. Daarmee verplichten zij zich om zorgvuldig om te gaan met uw persoonsgegevens.

Hoe beschermen wij uw persoonsgegevens?

OmniaZorg heeft een Privacy Functionaris. Deze zorgt ervoor dat uw persoonsgegevens worden beschermd tegen verlies of onrechtmatig gebruik ervan. Zij houdt bij welke gegevens gedeeld worden en zorgt voor de verwerkersovereenkomsten. Ook controleert zij of iedereen zich aan de regels houdt en als er een datalek is, dat kan het verlies van een tablet of computer zijn waar persoonsgegevens op staan of en zogenaamde Hack (als iemand van buiten de organisatie binnendringt in de computer van OmniaZorg), dan neemt zij maatregelen, zoals zorgen voor het melden van het lek aan de Autoriteit Persoonsgegevens (AP).

Wat zijn uw rechten?

U heeft een aantal privacy rechten. U kunt ons bijvoorbeeld vragen welke persoonsgegevens wij van u verwerken. En als de gegevens niet kloppen kunt u ons vragen deze aan te passen of te verwijderen. Dit is niet altijd mogelijk omdat we sommige gegevens verplicht zijn te bewaren. De bewaartermijn van een medisch dossier is 20 jaar. Daarna wordt het dossier vernietigd.

Welke rechten heeft u:

- Recht op inzage: u kunt vragen of u in het dossier mag kijken. In 2021 gaan we over naar een digitaal cliënten dossier en dan kunt u overal, met een computer of tablet, in uw dossier kijken;
- Controle van de persoonsgegevens: als die niet kloppen kunt u ons opdracht geven ze aan te passen. Alleen als we een wettelijke plicht hebben om gegevens te bewaren kunnen we dat niet doen. Dat bespreken we dan met u;
- Recht op vernietiging van gegevens: als er dingen in uw dossier staan die u daar niet in wilt hebben kunt u ons opdragen deze te verwijderen. Echter: soms zijn wij wettelijk verplicht om gegevens te bewaren. Als dat zo is dan bespreken we dat met u;
- Recht om toestemming in te trekken: als wij u eerder om toestemming gevraagd hebben en u die toestemming heeft gegeven dan kunt u altijd die toestemming weer intrekken en dan wordt de verwerking van de gegevens gestopt.

Contact met OmniaZorg:

Als u vragen heeft over het beschermen van uw persoonsgegevens of uw recht wilt uitoefenen dan kunt u contact opnemen met OmniaZorg.
U kunt bellen of mailen naar:
Tel: 085-4019210 (algemeen nummer, vragen naar de Privacy Functionaris)
Email: info@omniazorg.nl (ter attentie van de Privacy Functionaris)

De Privacy Functionaris neemt dan, zo spoedig mogelijk, contact met u op.

Bent u niet tevreden over hoe er met uw persoonsgegevens omgegaan wordt en niet goed naar uw wensen geluisterd wordt dan kunt u een klacht indienen bij de Klachtenfunctionaris. Dit kan door het klachtenformulier in te vullen (link naar klachtenformulier).

Wilt u meer weten over het privacy beleid bij OmniaZorg dan kunt u het Privacy beleidsplan lezen. (link naar het Privacy beleidsplan).

Bijlage 4: Privacy by Design Framework

Waarom dit framework?

In de AVG wordt Privacy by Design expliciet vereist bij het verwerken van persoonsgegevens. Privacy by Design betekent dat organisaties bij de ontwikkeling van (nieuwe) producten en diensten zo vroeg mogelijk aandacht besteden aan het beschermen van persoonsgegevens. Door privacybeschermende maatregelen aan het begin mee te nemen in de ontwikkeling is men eerder compliant met privacyregelgeving en worden kosten bespaard doordat deze maatregelen niet later alsnog moeten worden genomen. Maar hoe laat je zien dat je voldoet aan het vereiste van Privacy by Design?

Hoe gebruik je dit framework?

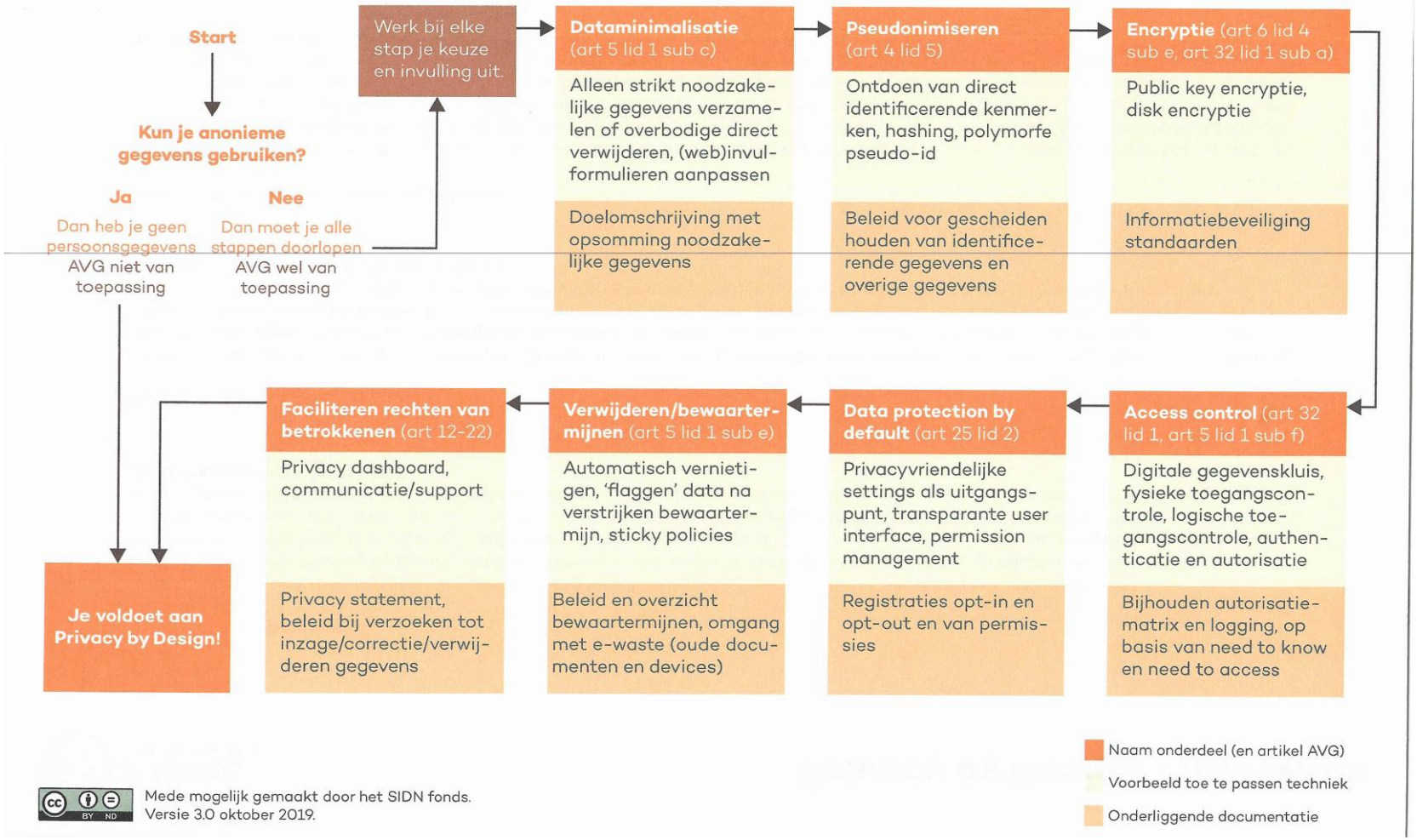
Dit framework geeft invulling aan Privacy by Design op basis van vereisten die door de AVG verspreid zijn opgenomen. Indien mogelijk kun je werken met anonieme gegevens. Als dat niet mogelijk is doorloop je de overige blokken. Steeds is er een technische component met ondersteunende documentatie of organisatorische maatregelen. Door het schema te doorlopen en te registreren welke aspecten zijn meegenomen ontstaat een overzicht van de manier waarop OmniaZorg aan Privacy by Design voldoet.

Maak het onderdeel van de organisatie

Het framework kan binnen de organisatie gebruikt worden als onderdeel van de algehele privacy governance. Om te borgen dat de organisatie compliant blijft wordt er regelmatig een privacy audit uitgevoerd aan de hand van het framework. Daarnaast kan een privacy impact assessment helpen om inzichtelijk te maken welke maatregelen vereist zijn bij het ontwerpen van een nieuwe dienst of gegevensverwerking. Privacy by design omvat slechts een gedeelte van de algehele privacy governance. Denk bijvoorbeeld aan interne privacy awareness, intern beleid, beleggen van verantwoordelijkheden, transparantie naar betrokkenen, samenwerking met derde partijen en verwerkers (incl. contracten en verwerkersovereenkomsten).

PRIVACY COMPANY

Privacy by Design Framework



Mede mogelijk gemaakt door het SIDN fonds.
Versie 3.0 oktober 2019.

Bijlage 5: Protocol Datalekken

De AVG bepaalt dat datalekken direct, binnen 72 uur, gemeld moeten worden aan de Autoriteit Persoonsgegevens (AP), tenzij het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Daarnaast moet het datalek ook aan de betrokkenen gemeld worden indien het waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt.

Aan de beantwoording van de vraag moet een zorgvuldige (belangen)afweging voorafgaan. Hierbij is bijvoorbeeld de aard en de omvang van de persoonsgegevens die gelekt zijn van belang. Als er bijzondere persoonsgegevens, zoals gegevens over gezondheid, gelekt zijn, dan is de melding meestal noodzakelijk.

Dit protocol datalekken is bedoeld als hulpmiddel voor de beantwoording van de vraag of er sprake is van een datalek en of deze gemeld moet worden.

1: Wat is een datalek?

Er is sprake van een datalek als er een inbreuk in verband met persoonsgegevens heeft plaatsgevonden. Alleen een dreiging of een tekortkoming in de beveiliging is niet voldoende; er moeten daadwerkelijk persoonsgegevens gelekt zijn.

Onder een datalek verstaat de AP persoonsgegevens die gelekt of vernietigd zijn als gevolg van een beveiligingsincident. Bij het lek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Bij verlies zijn de persoonsgegevens er niet meer. Onder onrechtmatige verwerking vallen bijvoorbeeld onbevoegde kennisneming, wijziging, aantasting of de verstrekking daarvan.

Voorbeelden van inbreuken in verband met persoonsgegevens kunnen zijn:

- Kwijtraken van een USB -stick;
- Diefstal van een laptop;
- Inbraak door een hacker;
- Persoonsgegevens per ongeluk gepubliceerd;
- Hacking, mailware of fishing;
- Persoonsgegevens aan verkeerde persoon verstuurd;
- Calamiteiten zoals brand in een datacentrum.

2: Contactpersoon aanwijzen

De organisatie moet een eigen contactpersoon aangewezen aan wie eventuele datalekken gemeld moeten worden. Dit is bij OmniaZorg de Privacy Functionaris. (hierna: ‘Contactpersoon”)

3: Informeren medewerkers

Medewerkers binnen de organisatie dienen zich er van bewust te zijn dat als er sprake is van een datalek, zij dit datalek direct (diezelfde dag nog) moeten melden bij de aangewezen Contactpersoon, zodat deze tijdig het datalek kan melden bij de Autoriteit Persoonsgegevens. Zij dienen bekend te zijn met het in dit protocol opgenomen stappenplan.

4: Uitvoeren van het stappenplan Datalekken

De binnen de organisatie aangewezen Contactpersoon draagt zorg voor de invoering en naleving van het hieronder opgenomen stappenplan Datalekken. Indien er een datalek optreedt dienen de stappen in het stappenplan Datalekken doorlopen te worden.

STAPPENPLAN DATALEKKEN

Processtappen	**Activiteit**	**Verantwoordelijke persoon**
1. Er wordt een (mogelijk) datalek ontdekt	- Maak direct intern melding van (mogelijke) datalek aan de manager - Informeer de Privacy Functionaris	Medewerker die het ontdekt
2. Beoordeel het datalek	- Onderzoek het beveiligingsincident - Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden - Beoordeel wie of welke afdelingen binnen de organisatie hierbij betrokken zijn - Beoordeel of er een verwerker betrokken is bij het incident. Zo ja dan dient deze bij het proces betrokken te worden	Manager van afdeling waar binnen het datalek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) Privacy Functionaris
3. Bestrijdt het datalek	- Stop het datalek als het nog kan - Neem andere maatregelen om het datalek en de daaruit voortvloeiende schade te beperkten - Leg de acties van de genomen maatregelen vast in het dossier	Manager van afdeling waar binnen het datalek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) Aangewezen contactpersoon
4.Vaststellen impact datalek	- Onderzoek het datalek en de gevolgen daarvan - Onderzoek de aard van de gegevens die gelekt zijn. Bijv. gezondheidsgegevens, wachtwoorden, gegevens over	Manager van afdeling waar binnen het datalek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT)

	financiële situatie of die kunnen leiden tot stigmatisering/misbruik - Onderzoek de omvang van de gelekte gegevens - Beoordeel welke impact het lek kan hebben op de betrokken personen - Stel vast wat de nadelige gevolgen kunnen zijn	Privacy Functionaris
5. Vaststellen Meld en Herstelaanpak	- Bepaal aanpak/informeren AP - Bepaal aanpak/informeren betrokkenen - Bepaal acties voor nazorg betrokkenen - Bepaal acties voor belang van de organisatie - Bepaal acties voor verbetering beveiliging	Manager van afdeling waar binnen het datalek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) Privacy Functionaris
6. Melden AP*	- Indien besloten wordt om AP te informeren dan moet dat binnen 72 uur - Melding via de website van het AP - Van tevoren kan het Meldformulier Datalekken gebruikt worden	Privacy Functionaris Bestuur
7. Melden betrokkenen**	- Melding via bijvoorbeeld brief - Meedelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn. - Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen	Privacy Functionaris Bestuur Marketing/communicatie
8. Uitvoeren herstelwerkzaamheden	- Herstel het datalek - Verbeteren van de beveiliging	Manager van de afdeling die verantwoordelijk is voor de

	- Lever nazorg aan de betrokkenen	beveiligingsincidenten (bijvoorbeeld IT) Privacy Functionaris
9. Optimaliseer het beveiligings- en het Datalek proces	- Registreer, evalueer en verbeter de beveiliging en het proces inzake melding datalekken	Privacy Functionaris Bestuur Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT)

* Melding aan de Autoriteit Persoonsgegevens (AP) kan alleen achterwege blijven indien het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Of hiervan sprake is hangt mede af van de aard en omvang van de gelekte persoonsgegevens. Indien bijvoorbeeld uitsluitend de adresgegevens zijn gelekt van een kleine groep betrokkenen, dan is het onwaarschijnlijk dat er sprake is van een hoog risico. Dat is wellicht anders indien de adresgegevens in combinatie met het lidmaatschap van de patiënten of cliëntenorganisatie zijn gelekt. Het lidmaatschap van de organisatie kan gezien worden als een gevoelig gegeven en de leden van de organisatie kunnen wellicht behoren tot een kwetsbare groep, die extra bescherming nodig heeft. Bij de afweging van het risico voor de rechten en vrijheden van de betrokken zal altijd de Privacy Functionaris betrokken moeten worden.

** Indien het datalek waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen veroorzaakt, moet het datalek ook aan de betrokkenen gemeld worden. Het risico zal bijvoorbeeld moeten worden beoordeeld aan de hand van de aard en de hoeveelheid van de gelekte gegevens. Als er persoonsgegevens van gevoelige aard (bijv. gezondheidsgegevens) gelekt zijn, zal het lek in ieder geval gemeld moeten worden aan de betrokkenen. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Privacy Functionaris betrokken moeten worden.

Verwerker

Het kan gebeuren dat het datalek optreedt bij de verwerker. De organisatie is en blijft (als verwerkingsverantwoordelijke) altijd verantwoordelijk voor het datalek bij de verwerker. In dat geval moet dus hetzelfde stappenplan worden afgewerkt. De verwerker zal bij de stappen betrokken moeten worden.

Via de verwerkersovereenkomst moet afgedwongen worden dat de verwerker eventuele datalekken terstond (binnen 24 uur) meldt bij de organisatie en de organisatie helpt bij het beoordelen of er gemeld moet worden en de afwikkeling van het datalek. Belangrijk is dat de verwerker niet buiten de organisatie om een datalek meldt bij de Autoriteit Persoonsgegevens. De verwerker moet verder alle redelijke instructies van de organisatie opvolgen.