

PRIVACY EN GEGEVENSBESCHERMING

Inleiding

Een belangrijk aandachtspunt in de zorg is de omgang met persoonsgegevens van cliënten en medewerkers. Dit wordt verder benadrukt door de Algemene Verordening Gegevensbescherming (AVG). Tegen die achtergrond beschrijft en analyseert Onder de Bomen in dit document zijn gebruik en verwerking van persoonsgegevens. Het gaat dan zowel om persoonsgegevens van cliënten als om de gegevens van medewerkers van Onder de Bomen.

Onder de Bomen houdt bij gegevensverwerking rekening met de wettelijke eisen. Een belangrijk uitgangspunt is dat verwerking van persoonsgegevens beperkt wordt tot het hoogst noodzakelijke. Onder de Bomen wil naar betrokkenen transparant zijn over wat er met hun persoonsgegevens gebeurt.

Onder de Bomen hanteert als uitgangspunt dat gegevens niet voor een ander doel worden gebruikt, dan waarvoor zij zijn verzameld.

Dit reglement vloeit voort uit de Algemene Verordening Gegevensbescherming, die sinds mei 2018 van kracht is.

Concreet: de spelregels samengevat

- 1 Alle cliëntgegevens die moeten worden opgeslagen, dienen te worden opgeslagen in ONS;
- 2 Interne communicatie met cliëntgegevens gebeurt via de berichtenapplicatie van ONS;
- 3 Externe mail, berichtenuitwisseling met cliëntgegevens gebeurt enkel met toestemming van de cliënt via de extra beveiligde applicatie Zivver;
- 4 Een belangrijk uitgangspunt is dat verwerking van persoonsgegevens beperkt wordt tot het hoogst noodzakelijke.
- 5 Twee-staps verificatie wordt afgedwongen voor Google G-Suite, ONS van Nedap en Zivver. Door Onder de Bomen verstrekte smartphones en computers zijn eigendom van Onder de Bomen en daarmee wordt het beveiligingsbeleid van de organisatie afgedwongen. Zo worden bedrijfsgegevens beschermd en het apparaat veiliger gemaakt;
- 6 Internetverbindingen van de verschillende locaties worden beheerd volgens de AVG, gebruik van openbare WiFi netwerken is niet toegestaan.
- 7 Een account van een medewerker is strikt persoonlijk en mag niet worden gedeeld;
- 8 Onder de Bomen beheert het G-Suite account op apparatuur en heeft het recht om het account te verwijderen van een apparaat;

- 9 Accounts worden ingericht op basis van de functie en de locatie waar iemand werkzaam is, meer kan hij/zij niet zien. Dit bepaalt de autorisatie tot gegevens;
- 10 Laat een cliënt altijd formulieren Fo8 en Fog invullen, zodat het duidelijk is waar een cliënt toestemming voor geeft;
- 11 Cliënten krijgen toegang tot CarenZorgt, zodat zij hun zorgdossier kunnen inzien;
- 12 Rapportage in een zorgdossier wordt enkel in hoge uitzondering verborgen voor een cliënt wanneer de veiligheid van de cliënt, gezinsleden of medewerker in het geding zijn;

1 Algemene bepalingen

1.1 Begripsbepalingen

In dit reglement wordt verstaan onder:

Persoonsgegevens

Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

Verwerking van persoonsgegevens

Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwisselen of vernietigen van gegevens.

Verstrekken van persoonsgegevens

Het bekendmaken of ter beschikking stellen van gegevens.

Verzamelen van persoonsgegevens

Het verkrijgen van persoonsgegevens.

Bestand

Elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.

Verantwoordelijke

Onder de Bomen verzamelt als rechtspersoon persoonsgegevens, en is uit dien hoofde verantwoordelijk voor implementatie en naleving van de AVG.

Bewerker

Degene die ten behoeve van Onder de Bomen persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Betrokkene

Degene op wie een persoonsgegeven betrekking heeft (cliënt en/of een medewerker van Onder de Bomen).

Derde

Ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van Onder de Bomen of de bewerker gemachtigd is om persoonsgegevens te verwerken.

ISO 27002

De ISO normering voor het op de juiste wijze verwerken van persoonsgegevens. Een juiste implementatie van de ABG legt de basis voor eventuele ISO 27002-certificering.

MIC

Melding Incidenten Cliënten.

MIM

Melding Incidenten Medewerkers.

Nen-normen

De bepalingen uit de AVG worden voor de zorg deels specifiek vormgegeven in de NEB-normen 7510, 7512 en 7513. Ontvanger Degene aan wie de persoonsgegevens worden verstrekt (binnen de organisatie of er buiten).

Medewerkersdossier

Persoonsgegevens van werknemers welke, ter uitvoering van de arbeidsovereenkomst, door Onder de Bomen worden opgeslagen in een medewerkersdossier. Ook stagiaires en vrijwilligers vallen hier onder. De gegevens worden opgeslagen in de Talent en Salarismodule van VISMA.

Cliëntdossier

Persoonsgegevens van cliënten welke, ter uitvoering van de zorgovereenkomst, door Onder de Bomen worden opgeslagen in een cliëntdossier. De gegevens worden opgeslagen in ONS van NEDAP.

Toestemming van de betrokkene

Elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.

Autoriteit Persoonsgegevens

Autoriteit die tot taak heeft toe te zien op de verwerking van persoonsgegevens. Dit doet zij als onafhankelijke instantie op grond van de AVG. Tot 1-1-2016 heette dit het College Bescherming Persoonsgegevens.

Klachtencommissie

De commissie die is ingesteld overeenkomstig de Wet klacht-recht cliënten zorgsector. Vanaf 1-1-2016 is deze wet gewijzigd in Wet kwaliteit, klachten en geschillen in de zorg.

1.2 Reikwijdte

Dit document is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens van Onder de Bomen alsmede de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

1.3 Doel

Dit document beoogt een uitwerking te geven van de bepalingen van de Algemene Verordening Gegevensbescherming en voor zover van toepassing – van de bepalingen van de Wet op de geneeskundige behandelovereenkomst (Wgbo), de Wet op de beroepen in de individuele Gezondheidszorg (Wet Big) alsmede informatie te verschaffen aan personen van wie persoonsgegevens verwerkt (zullen) worden en bij te dragen aan doorzichtigheid van de gehanteerde regels met betrekking tot de door de Onder de Bomen verwerkte en te verwerken persoonsgegevens.

1.4 Omschrijving van betrokkenen

De persoonsgegevens worden verwerkt van de volgende betrokkenen:

- cliënten (personen die gebruik maken van de diensten van Onder de Bomen of hun wettelijke vertegenwoordiger(s));
- personen van wie Onder de Bomen in verband met contractuele of wettelijke verplichtingen jegens een cliënt of derde persoonsgegevens dient te verwerken;
- personen die Onder de Bomen benaderen (bijvoorbeeld verwijzers)
- personen die Onder de Bomen wil benaderen teneinde hen te bewegen een rechtsverhouding aan te gaan.

2 Rechtmatige verwerking persoonsgegevens

2.1 Voorwaarden voor rechtmatige verwerking

- 1 Persoonsgegevens worden in overeenstemming met dit reglement op behoorlijke en zorgvuldige wijze verwerkt en alleen voor welbepaalde, uitdrukkelijke omschreven en gerechtvaardigde doeleinden.
- 2 Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Bij de beoordeling of een verwerking onverenigbaar is met het doel moet men rekening houden met de verwachting tussen doel van verwerking en het doel waarvoor de gegevens zijn verkregen, met de aard van de gegevens, met de gevolgen van de verwerking voor betrokkenen, met de wijze waarop de gegevens zijn ver-

kregen en de mate waarin jegens betrokkene passende waarborgen zijn genomen.

- 3 Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.

Binnen Onder de Bomen vindt verwerking van persoonsgegevens, met inachtneming van bovenstaande voorwaarden, plaats, in het kader van een efficiënte en effectieve bedrijfsvoering, in het bijzonder gericht op de volgende activiteiten:

- Een goede uitvoering van de zorgverlening die door Onder de Bomen aan de betrokkene wordt verleend;
- Het beheer en beleid van Onder de Bomen;
- Onderzoek, evaluatie en verbetering van de zorgverlening;
- De verantwoording van Onder de Bomen aan zorgverzekeraars, gemeenten (samenwerkingsverbanden), zorgkantoren conform de geldende voorschriften en wettelijke verplichtingen.

2.2 Verwerking van persoonsgegevens

Persoonsgegevens mogen slechts worden verwerkt indien aan één van onderstaande voorwaarden is voldaan.

- A De betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming gegeven. De toestemming kan blijken uit woord of gedrag en hoeft niet schriftelijk te worden verkregen. Wel dient de betrokkene alvorens toestemming te geven goed geïnformeerd te zijn.
- B De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor handelingen die op verzoek van de betrokkene worden verricht en die noodzakelijk zijn voor het sluiten van een overeenkomst; dit is bijvoorbeeld het geval bij een behandelingsovereenkomst in de zin van de Wgbo (BW 7:446 e.v.)
- C De verwerking is noodzakelijk om een wettelijke verplichting na te komen;
- D De verwerking is noodzakelijk ter bestrijding van ernstig gevaar voor de gezondheid van betrokkene; Er is een dringende medische noodzaak de gegevens van de betrokkene te verwerken;
- E De verwerking is noodzakelijk met het oog op belang van de verantwoordelijke of van een derde én het belang van degene van wie de gegevens worden verwerkt niet prevaleert. Dit is een algemene restbepaling.

3 Specifieke regels voor het verwerken van bijzondere persoonsgegevens

De aard van sommige persoonsgegevens brengt mee dat de verwerking ervan een grote inbreuk kan vormen op de persoonlijke levenssfeer van de betrokkene, omdat die gegevens gevoelige informatie over iemand verschaffen. De AVG noemt deze gegevens bijzondere persoonsgegevens. Voor de verwerking van bijzondere persoonsgegevens geldt een strenger regime dan voor gewone persoonsgegevens. De verwerking van bijzondere persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid of seksuele leven mag op grond van de AVG alleen in uiterste gevallen verwerkt worden. Ook strafrechtelijke en aanverwante gegevens behoren tot deze categorie.

3.1 Gezondheid

Gegevens over iemands gezondheid mogen verwerkt worden door o.a.: hulpverleners, instellingen of voorzieningen voor gezondheidszorg en/of maatschappelijke dienstverlening voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene, dan wel het beheer van de betreffende instelling of beroepspraktijk noodzakelijk is.

Onder de Bomen verwerkt gegevens m.b.t. gezondheid op grond van bovenstaande bepalingen in de rol van gezondheidszorginstelling in ONS van Nedap.

Onder de Bomen registreert en vraagt niet naar gezondheidsgegevens van medewerkers.

3.2 Erfelijke eigenschappen

Persoonsgegevens betreffende erfelijke eigenschappen van cliënten worden slechts verwerkt wanneer dit diagnostiek betreft welke de hulpverlening bevordert.

3.3 Wetenschappelijk onderzoek/statistiek

Onder de Bomen zal nooit naar specifieke gegevens vragen en opslaan ten behoeve van wetenschappelijk onderzoek of statistiek. Het zou enkel kunnen gaan om gegevens die Onder de Bomen al reeds verzamelt ten behoeve van de hulpverlening. Verwerking van persoonsgegevens ten behoeve van wetenschappelijk onderzoek of statistiek is toegestaan indien het onderzoek een algemeen belang dient, de verwerking voor het betreffende onderzoek of de betreffende statistiek noodzakelijk is, het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost of bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

3.4 Godsdienst/levensovertuiging/ras

Onder de Bomen zal deze specifieke persoonsgegevens nooit vastleggen in haar systemen.

3.5 Lidmaatschap vakbond

Lidmaatschap van een vakbond mag alleen verwerkt worden door een vakbond voor zover dat gelet op de doelstelling van de vakbond noodzakelijk is. Onder de Bomen is dus niet zonder meer gerechtigd om lidmaatschap van een vakbond te registreren, behalve als de betrokkene hier toestemming voor heeft gegeven.

3.6 Algemene uitzonderingen; restbepalingen

Ook als het verbod op het verwerken van bijzondere gegevens niet via één van de bovenstaande specifieke uitzonderingen kan worden opgeheven is het onder voorwaarden toch mogelijk deze gegevens te verwerken. Dit zijn de algemene uitzonderingen. Bijzondere persoonsgegevens mogen wel verwerkt worden als:

- De betrokkene uitdrukkelijk toestemming heeft gegeven.
- Uitdrukkelijke toestemming betekent dat de betrokkene expliciet zijn wil moet hebben geuit.
- De betrokkene de gegevens zelf al duidelijk openbaar heeft gemaakt. In dat geval zal de intentie van de betrokkene om openbaar te maken, duidelijk moeten zijn.

4 Organisatorische verplichtingen

4.1 Geheimhouding

Alle medewerkers van Onder de Bomen dienen zich te houden aan hun geheimhoudingsplicht. Dit houdt in dat zij verplicht zijn geheimhouding in acht te nemen ten opzichte van al datgene wat hen bij het uitoefenen van hun beroep aan persoonsgegevens is toevertrouwd.

Voor artsen, fysiotherapeuten, GZ-psychologen en verpleegkundigen is het beroepsgeheim geregeld in artikel 88 van de Wet op de Beroepen in de Individuele Gezondheidszorg (Wet BIG). Ook in artikel 7:457 BW (WGBO) is de geheimhoudingsplicht van hulpverleners neergelegd.

Voor het verstrekken van persoonsgegevens aan derden is toestemming vereist van de betrokkene of diens vertegenwoordiger. Deze toestemming kan enkel schriftelijk worden verstrekt en dient te worden vastgelegd in het cliëntdossier.

Bij de verstrekking van gegevens aan derden moet altijd het doel duidelijk zijn en mogen alleen die gegevens verstrekt worden die het doel dienen. De gegevensverstrekking dient niet bovenmatig, toereikend en ter zake dienend te zijn.

4.2 Bewaren van persoonsgegevens

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de verwerking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.

Persoonsgegevens mogen langer worden bewaard dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, wanneer zij geanonimiseerd worden of voor zover ze uitsluitend voor historische, statistische of wetenschappelijke doeleinden worden bewaard.

Zie hiervoor ook hoofdstuk 6.

4.3 Beveiliging van persoonsgegevens

Onder de Bomen legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Indien Onder de Bomen persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, draagt Onder de Bomen zorg dat deze voldoende waarborgen biedt ten aanzien van de technische- en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen.

Onder de Bomen verwacht dat bedrijven waarvan de applicaties worden gebruikt, NEN 7510 / ISO 27002 zijn gecertificeerd of anderszels gelijkwaardig zijn gecertificeerd.

Van alle gegevensverwerkingen wordt een risico-inschatting gemaakt en maatregelen aangegeven voor een zo veilig mogelijke verwerking van persoonsgegevens. Onder de Bomen ziet toe op de naleving van die maatregelen.

4.4 Kwaliteit gegevensverwerking

Onder de Bomen draagt zorg voor de kwaliteit van de gegevensverwerking. De gegevensverwerking dient toereikend, niet bovenmatig en ter zake dienend te zijn.

4.5 Klachtenbehandeling

Indien de betrokkene van mening is dat de bepalingen van dit reglement niet worden nageleefd of andere redenen heeft tot klagen, kan hij/zij dit op verschillende manieren kenbaar maken. Onder de Bomen is lid van Klachtenportaal Zorg en heeft lidmaatschapsnummer 1448. Na het indienen van een klacht via het Klachtenportaal Zorg wordt de klachtenprocedure gestart.

- Via www.klachtenportaalzorg.nl vindt je het klachten-formulier
- Contact per e-mail kan via info@klachtenportaalzorg.nl
- Schriftelijk contact kan ook: Westerstraat 117, 1601 AD Enkhuizen

Op grond van de AVG kan de betrokkene bij de Autoriteit persoonsgegevens (tot 1-1-2016: College Bescherming Persoonsgegevens) (www.autoriteitpersoonsgegevens.nl) verzoeken een onderzoek in te stellen of de wijze van gegevensverwerking door de verantwoordelijke in overeenstemming is met de Wbp.

4.6 Gedragscode

Alle medewerkers van Onder de Bomen krijgen bij indiensttreding de door Onder de Bomen vastgestelde gedragscode uitgereikt. In deze gedragscode staan o.a. richtlijnen voor het omgaan met persoonsgegevens.

5 Rechten van betrokkenen

5.1 Informatieplicht

Onder de Bomen informeert betrokkene vóór verkrijging van de persoonsgegevens over het doel van de gegevensverzameling en verwerking.

Indien persoonsgegevens niet rechtstreeks via de betrokkene worden verkregen informeert Onder de Bomen betrokkene over de verwerking van deze gegevens.

Indien de gegevens uitsluitend verzameld worden om aan een derde te verstrekken wordt betrokkene hiervan op de hoogte gesteld, uiterlijk op het moment van de eerste verstrekking aan die derde.

5.2 Recht op inzage van persoonsgegevens

De betrokkene heeft het recht zich tot Onder de Bomen te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. Onder de Bomen deelt de betrokkene schriftelijk binnen vier weken mee of hem betreffende persoonsgegevens worden verwerkt.

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

5.3 Recht op aanvulling-,correctie- verwijdering of vernietiging van persoonsgegevens

Degene aan wie overeenkomstig het voorgaande kennis is gegeven van hem betreffende persoonsgegevens, kan Onder de Bomen verzoeken deze te verbeteren, aan te vullen, te verwijderen, of af te schermen indien deze feitelijk onjuist zijn, voor het

doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen.

Onder de Bomen bericht de verzoeker binnen vier weken na ontvangst van het verzoek schriftelijk op welke wijze aan het verzoek voldaan kan worden.

Onder de Bomen draagt zorg dat verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd. Onder de Bomen draagt zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker. De verzoeker moet zich daarvoor kunnen legitimeren met een geldig paspoort of een Nederlandse identiteitskaart, Nederlands rijbewijs of Nederlands vreemdelingendocument om te voorkomen dat er onrechtmatig inzage wordt gegeven.

Onder de Bomen is verplicht om een wijziging van persoonsgegevens, naar aanleiding van een verzoek zoals voorgaand benoemd, zo spoedig mogelijk aan derden door te geven. Onder de Bomen doet aan de verzoeker, desgevraagd opgave van degenen aan wie hij de mededeling heeft gedaan.

5.4 Recht op vertegenwoordiging

Personen jonger dan zestien jaar en personen ouder dan 16 jaar die niet tot een redelijke behartiging van hun belangen ter zake in staat zijn worden vertegenwoordigd conform de regeling die daartoe in de Wet op de Geneeskundige Behandelingsovereenkomst(Wgbo) is opgenomen.

5.5 Recht op verzet

De betrokkene kan tegen een verwerking van zijn persoonsgegevens verzet aantekenen in verband met zijn persoonlijke omstandigheden. Onder de Bomen beoordeelt binnen vier weken na ontvangst of het verzet terecht is. Indien het verzet terecht is wordt de verwerking onmiddellijk beëindigd.

6 Bewaartermijnen van gegevens

6.1 Persoonsgegevens van cliënt

Zorg- en cliëntendossiers (papier en elektronisch)

5 jaar na afsluiting zorg

Administratieve gegevens*

5 jaar

Klachten

5 jaar

MIC-meldingen**

5 jaar

Medische gegevens

5 jaar

Medicatieoverzichten***

5 jaar

Toedienlijsten medicatie

2 jaar

* Zorgverleners zijn op grond van de Wet gebruik burgerservicenummer in de zorg verplicht het bsn nummer te gebruiken en vast te leggen in hun administratie. Dit nummer wordt gebruikt bij uitwisseling van gegevens met andere zorgverleners. Voor controle op het bsn dient te cliënt een geldig identiteitsbewijs te laten zien. Er wordt geen kopie van het identiteitsbewijs van cliënten opgenomen in het dossier. Wel legt de zorgverlener soort en nummer van het gecontroleerde document vast in ONS en controleert deze door de gekoppelde landelijke database.

** De MIC melding maakt deel uit van het zorgdossier.

*** Medicatieoverzichten maken deel uit van het dossier.

6.2 Persoonsgegevens medewerkers

Medewerkerdossiers

5 jaar na einde dienstverband

Administratieve gegevens

5 jaar sociale wetgeving

7 jaar fiscale wetgeving

7 Data-stromen en applicaties

7.1 Beschrijving typen data

Onder de Bomen ontvangt, gebruikt en verstuurt de volgende drie deels overlappende typen persoonsgegevens.

Data type 1:

Financiële en persoonsgegevens medewerkers ten behoeve van indiensttreding, salariering, scholing, ziekte en ontslag.

Data type 2:

Zorggerelateerde en persoonlijke gegevens cliënten ten behoeve van het leveren van zorg.

Data type 3:

Financiële en persoonsgegevens ten behoeve van financiële administratie.

Data type 4:

Contracten en financiële en administratieve gegevens leveranciers Onder de Bomen.

7.2 Beschrijving data-applicaties en data-stromen

Onderstaand functie-, applicatie-, en data-overzicht brengt de verschillende digitale applicaties in beeld die Onder de Bomen gebruikt. Buiten de website is elke applicatie afkomstig van grote gevestigde organisaties, die ook zelf zorgdragen voor een omgang met persoonsgegevens in overeenstemming met de AVG. Dat geldt voor het gebruik binnen de applicaties, maar tevens voor de communicatie tussen de applicaties. Bij elke applicatie staat indien relevant aangegeven welke van bovenstaande typen data door Onder de Bomen wordt gebruikt. Buiten deze applicaties gebruikt en verwerkt Onder de Bomen geen data met betrekking tot persoonsgegevens.

7.3 Functionaris gegevensbescherming

Binnen de huidige omvang van Onder de Bomen is het niet mogelijk de functie gegevensbescherming ergens anders dan bij het vierkoppige bestuur te beleggen. Het bestuur is collegiaal en integraal verantwoordelijk, maar bestuurders Jasper Pors en Floris Heukelom hebben de functie gegevensbescherming als aandachtsgebied. Zij worden hierin geadviseerd en ondersteund door applicatiebeheerder Annelisa Visser-Bentinck.

7.4 Verwerkingsregister

Onder de Bomen heeft op dit moment ruim minder dan 250 medewerkers. Daarnaast betekenen de persoonsgegevens die worden verwerkt geen hoog risico voor de betrokkenen, en vallen ze niet onder de categorie bijzondere persoonsgegevens. Bovendien wordt de verwerking van persoonsgegevens geborgd door de applicaties en bijbehorende organisaties genoemd in het functie-, applicatie-, en data-overzicht. We verwachten dat bedrijven waarvan wij de applicaties gebruiken NEN 7510 / ISO 27002 zijn gecertificeerd of anders gelijkwaardig zijn gecertificeerd.

Een eigen verwerkingsregister wordt daarmee op dit moment als niet functioneel beoordeeld, en achterwege gelaten.

7.5 Gegevensbeschermings-effectbeoordeling

Indien er aanwijzingen zijn dat de bescherming van gegevensbescherming onvoldoende is, kan een gegevensbeschermings-effectbeoordeling (ook wel Privacy Impact Assessment (PIA)) uitgevoerd worden. Het model hiervoor van de Rijksoverheid – onder deze [link](#) – biedt de voor de hand liggende blauwdruk. Gezien de omvang van de organisatie en de hierboven beschreven data-typologie, en het functie-, applicatie- en dataoverzicht, wordt een dergelijke beoordeling op dit moment niet nodig geacht.

7.6 Procedure bij een (mogelijk) datalek

Wanneer een melding wordt ontvangen, of het vermoeden bestaat dat er een datalek heeft plaatsgevonden, wordt de volgende procedure gevolgd:

- A Mogelijke datalek en betrokken informatiestromen in kaart brengen; overzicht creëren;
- B Schade beperken: op basis van a) wordt besloten en uitgevoerd wat direct gedaan kan worden om lek te dichten en/of schade zoveel mogelijk te beperken;
- C Bepalen of het datalek door Onder de Bomen aan Autoriteit Persoonsgegevens moet worden gemeld. Ligt deze verantwoordelijkheid gezien de aard van het datalek bij een (software)leverancier, dan verzoek om schriftelijke bevestiging van melding bij AP;

- D Bepalen of datalek aan betrokken personen gemeld moet worden. Indien ja, wordt dit zo snel als redelijkerwijs mogelijk gedaan;
- E Datalek wordt geregistreerd in het datalekregister van Onder de Bomen.

7.7 Conclusie

Op basis van de in dit hoofdstuk beschreven en geanalyseerde omgang met persoonsgegevens, concludeert het bestuur van Onder de Bomen dat de bescherming van persoonsgegevens op dit moment voldoende wordt geborgd, en dat wordt voldaan aan de eisen van de AVG.

7.8 Functie-, applicatie- en dataoverzicht

