Privacyreglement Joris Zorg

Onderwerp:	Privacyreglement Joris Zorg
Documentverantwoordelijke:	Manager Bedrijfsvoering
Vastgesteld op:	19-12-2024
Volgende evaluatie op:	19-12-2026

Inhoudsopgave

1 Inleiding

1.1 Waarom dit privacyreglement?

Alle medewerkers van Joris Zorg zijn verantwoordelijk voor het beschermen van de gegevens die onze cliënten, medewerkers, vrijwilligers en bezoekers aan ons toevertrouwen. Het is bij Joris Zorg een bewuste keus ons hierbij aan de wet- en regelgeving te houden. Niet omdat het moet, maar omdat we als betrouwbare partner bekend willen staan.

In ons privacybeleid staan de uitgangspunten voor privacybescherming beschreven. Het beleid bevat een aantal principes en hoofdregels die we binnen Joris Zorg hanteren om de privacy van cliënten en medewerkers en ieder ander van wie wij persoonsgegevens verwerken, te beschermen. Dit privacyreglement is een verdieping van het privacybeleid en beschrijft hoe Joris Zorg met de bescherming van persoonsgegevens omgaat. Dit is een uitwerking van de privacywetgeving.

1.1.1 Privacywetgeving

De regels die vertellen hoe Joris Zorg om moet gaan met persoonsgegevens zijn vastgelegd in verschillende wetten. In de Algemene verordening gegevensbescherming (AVG) staan de algemene regels rondom privacybescherming. Ook gelden voor Joris Zorg een aantal zorg specifieke wetten, waarin regels over privacy zijn opgenomen. Bijvoorbeeld de Wet op de geneeskundige behandelingsovereenkomst (Wgbo), de Zorgverzekeringswet (Zvw), de Wet langdurige zorg (Wlz) en de Wet Maatschappelijke Ondersteuning 2015 (Wmo 2015).

De AVG stelt het opstellen van privacybeleid (gegevensbeschermingsbeleid) verplicht als onderdeel van de verantwoordingsplicht. Omdat Joris Zorg op grote schaal gezondheidsgegevens verwerkt, geldt dit zeker voor ons. Op verzoek van een cliënt of medewerker stellen wij ons privacybeleid en privacyreglement ter beschikking.

1.2 Voor wie is dit reglement bedoeld?

Dit privacyreglement is bedoeld voor alle medewerkers, waaronder inhuurkrachten, vrijwilligers en stagiaires van Joris Zorg. Zij zijn bij de start van hun werkzaamheden bij Joris Zorg op dit privacyreglement gewezen. Iedere medewerker moet aan de vereisten in dit privacyreglement voldoen. Ons privacyreglement, in combinatie met ons privacybeleid, kan ook worden gebruikt voor het informeren van cliënten over hoe Joris Zorg omgaat met de bescherming van persoonsgegevens.

2 Uitgangspunten verwerking persoonsgegevens

2.1 Verwerking van persoonsgegevens

Onder persoonsgegevens verstaan we alle informatie die over een persoon gaat, of herleidbaar is tot een persoon. Bijvoorbeeld een naam, telefoonnummer of e-mailadres. Maar ook IP-adressen zijn persoonsgegevens. Bijzondere persoonsgegevens, zoals gezondheidsgegevens, krijgen extra bescherming volgens de privacywet. De privacywetgeving is van toepassing als we te maken hebben met een verwerking van persoonsgegevens. Hier is al snel sprake van. Verwerking is het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door doorsturen, verspreiden of in een andere vorm beschikbaar stellen, samenbrengen, met elkaar in verband brengen en het afschermen, uitwissen of vernietigen van gegevens.

2.2 Beginselen over verwerking persoonsgegevens

Joris Zorg is verantwoordelijk voor het naleven van onderstaande beginselen bij de verwerking van persoonsgegevens. Wij moeten de naleving van deze beginselen kunnen aantonen (“verantwoordingsplicht”). Binnen Joris Zorg worden persoonsgegevens alleen verwerkt:

1. op een wijze die voor de betrokkene rechtmatig, behoorlijk en transparant is.
2. voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt. De verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd (“doelbinding”).
3. voor zover zij toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (“minimale gegevensverwerking” ook wel “dataminimalisatie”).
4. als de persoonsgegevens juist zijn en zo nodig worden geactualiseerd. Alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, zo snel mogelijk te wissen of te rectificeren (“juistheid”)
5. en bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren, dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is. Persoonsgegevens mogen voor langere perioden

worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen ("opslagbeperking").

6. door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier dat een passende beveiliging ervan gewaarborgd is en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ("integriteit en vertrouwelijkheid").

3 Rechtmatige gegevensverwerking

3.1 Voorwaarden verwerking persoonsgegevens

Persoonsgegevens mogen alléén worden verwerkt als aan een van de onderstaande voorwaarden, als rechtsgrond voor de verwerking, is voldaan:

- de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden.
  Joris Zorg moet kunnen aantonen dat toestemming is gegeven. Toestemming wordt daarom schriftelijk gevraagd en vastgelegd in het elektronisch dossier van de cliënt of medewerker. Ook moet de toestemming voldoende specifiek en geïnformeerd zijn en vrijelijk zijn gegeven. Toestemming wordt zoveel mogelijk op voorhand, bij inschrijving, start behandeling cliënt of indiensttreding medewerker vastgelegd.
  Betrokkenen hebben altijd het recht hun toestemming weer in te trekken. Bij indiening van het verzoek wordt de verwerking waarvoor toestemming is gegeven, direct gestopt. Het intrekken van toestemming doet geen afbreuk aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan.
- de gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, bijvoorbeeld de zorgovereenkomst of de arbeidsovereenkomst.
- de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen, bijvoorbeeld de dossierplicht in de Wgbo of gegevensverstrekking bij gedwongen opname en gedwongen behandeling op grond van de Wet zorg en dwang.
- de gegevensverwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of een ander natuurlijk persoon.
- de gegevensverwerking noodzakelijk is voor de goede vervulling van een taak van algemeen belang, dat elders in een wet is vastgelegd met eventuele nadere bepalingen.
- de gegevensverwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde én de belangen, grondrechten of fundamentele vrijheden van degene van wie de gegevens worden verwerkt niet prevaleren.

3.2 Voorwaarden voor het verwerken van gezondheidsgegevens

Gezondheidsgegevens zijn één van de categorieën bijzondere persoonsgegevens. Het is in de AVG verboden bijzondere categorieën persoonsgegevens te verwerken, tenzij voldaan wordt aan één van de onderstaande voorwaarden:

- Als de verwerking noodzakelijk is voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de medewerker, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, voor zover dit is toegestaan in nationale wetgeving.
- Zo mogen gegevens over gezondheid worden verwerkt met het doel gezondheidszorg te leveren, onder de verantwoordelijkheid van een beroepsbeoefenaar, die aan het beroepsgeheim gebonden is of door een ander persoon die op grond van de wet of overeenkomst tot geheimhouding is gehouden.

Nb.: naast de opheffing van het verbod om bijzondere gezondheidsgegevens te verwerken, zoals hierboven genoemd, moet ook nog een verwerkingsgrondslag (zie hoofdstuk 3.1) aanwezig zijn om dergelijke gegevens te verwerken.

3.3 Wanneer mogen andere bijzondere gegevens dan de gezondheidsgegevens worden verwerkt?

Andere bijzondere gegevens, bijvoorbeeld gegevens over ras/etniciteit of godsdienst/ levensovertuiging mogen alleen als aanvulling op gezondheidsgegevens worden verwerkt als dat nodig is voor een goede behandeling of verzorging van de betrokkene. Dus niet systematisch bij elke cliënt. Bijvoorbeeld voor het inschakelen van een tolk/vertaler als dat voor de uitleg van de behandeling aan de cliënt nodig is.

3.4 Gegevensverwerking door een verwerker

Joris Zorg kan de verwerking (extern) uitbesteden aan een verwerker. Bijvoorbeeld voor salarisverwerking of bij hosting van persoonsgegevens. In een verwerkersovereenkomst worden de verplichtingen uit de AVG opgelegd aan de verwerker. Joris Zorg doet uitsluitend een beroep op verwerkers, die afdoende garanties bieden voor het toepassen van passende technische en organisatorische maatregelen, opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd. Joris Zorg controleert dit, voordat de overeenkomst wordt afgesloten.

De verwerking door een verwerker wordt geregeld in een (verwerkers)overeenkomst die de verwerker aan Joris Zorg bindt. Hierin staan de volgende zaken omschreven:

- het onderwerp
- de duur van de verwerking
- de aard en het doel van de verwerking
- het soort persoonsgegevens
- de categorieën van betrokkenen
- de rechten en verplichtingen van Joris Zorg

Een dergelijke overeenkomst moet voldoen aan de eisen die de AVG daaraan stelt.

Joris Zorg maakt in principe gebruik van een modelovereenkomst, die is gebaseerd op de zogenaamde BOZ-modelverwerkersovereenkomst. De inhoud van alle af te sluiten verwerkersovereenkomsten wordt beoordeeld door de Functionaris Gegevensbescherming.

De verwerker en eenieder die onder het gezag van Joris Zorg of van de verwerker handelt en toegang heeft tot persoonsgegevens, verwerkt deze uitsluitend in opdracht van Joris Zorg, tenzij hij door wet- of regelgeving tot verwerking gehouden is.

3.5 Gezamenlijke verwerkingsverantwoordelijken

Als twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijk verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectievelijke verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze AVG vast, met name voor de uitoefening van de rechten van de betrokkene en hun respectievelijke verplichtingen om de verplichte informatie te verstrekken met een onderlinge regeling. In de regeling kan een contactpunt voor betrokkenen worden aangewezen. Uit de bedoelde regeling blijkt duidelijk welke rol de gezamenlijke verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun respectievelijke verhouding met de betrokkenen is. De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld. Ongeacht een dergelijke regeling kan een betrokkene zijn rechten uit de AVG voor en jegens iedere verwerkingsverantwoordelijke uitoefenen.

3.6 Aansprakelijkheid verwerkingsverantwoordelijke en/of verwerker

Joris Zorg is als verwerkingsverantwoordelijke verantwoordelijk en aansprakelijk voor schade die voortvloeit uit het toerekenbaar tekortschieten of niet voldoende naleven van de AVG, waaronder het wel/niet naleven van de beveiligingseisen.

De verwerker, waaraan Joris Zorg (een deel van) gegevensverwerking heeft uitbesteed, kan daarnaast zelfstandig aansprakelijk zijn voor schade of een deel van de schade die voortvloeit uit zijn werkzaamheden. Hoe die aansprakelijkheid wordt verdeeld, wordt beoordeeld door de schadeverzekeraar of de rechter. Van belang is dat Joris Zorg goede afspraken maakt met de verwerker en deze vastlegt in een verwerkersovereenkomst.

4 Verstrekking van gegevens aan derden

4.1 Geheimhoudingsplicht

Voor alle medewerkers van Joris Zorg geldt een geheimhoudingsplicht. Dit is geregeld in een overeenkomst bij de aanstelling. Daarnaast geldt voor persoonsgegevens verkregen in de uitoefening van een beroep in de (geestelijke) gezondheidszorg de geheimhoudingsplicht van de hulpverlener. Deze geheimhoudingsplicht is onder andere vastgelegd in de Wgbo en de wet BIG en in verschillende beroepscodes. Vanwege de geheimhoudingsplicht mogen medewerkers géén gegevens verstrekken aan personen of instanties binnen en buiten Joris Zorg, tenzij aan een aantal voorwaarden is voldaan.
Let wel: ondanks dat aan deze voorwaarden is voldaan, houdt Joris Zorg haar verantwoordelijkheid om proportioneel te handelen bij overtreding van de geheimhoudingsplicht.

4.2 Verstrekking van cliëntgegevens aan derden

4.2.1 Informatie-uitwisseling met rechtstreeks betrokkenen

Zorgverleners mogen medische informatie delen met anderen, die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en met degene die optreedt als vervanger van de hulpverlener. Dit mag alleen als die informatie noodzakelijk is voor hun werkzaamheden.

4.2.2 Toestemming

Je mag informatie aan derden verstrekken als cliënten of medewerkers hiervoor toestemming hebben gegeven. Uit de gegeven toestemming moet blijken dat deze vrijelijk, specifiek en geïnformeerd is gegeven. Toestemming wordt altijd vastgelegd in het elektronisch dossier van de betrokkene, onder vermelding van datum van toestemming.

Intrekken van toestemming
Betrokkenen hebben altijd het recht hun toestemming weer in te trekken. Verzoeken om intrekken van toestemming worden ingediend bij het ServicePunt, cliënten-administratie, of HR-administratie. Bij het indienen van het verzoek wordt de verwerking waarvoor toestemming is gegeven, direct gestopt. Het intrekken van toestemming doet geen afbreuk aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan.

Verwijzing medisch specialist
Bij een verwijzing naar een medisch specialist is het gebruikelijk dat medische informatie over de cliënt wordt meegestuurd. Omdat de cliënt instemt met de verwijzing, wordt verondersteld dat de laatstgenoemde ook voor het verstrekken van informatie aan de medisch specialist toestemming geeft. Hiervoor hoeft dus niet opnieuw toestemming worden gevraagd.

Toestemming bij terugkoppeling naar verwijzer
Voor terugkoppelingen van specialisten naar verwijzers is toestemming nodig van de cliënt.

Opvragen cliëntgegevens bij derden
Als het voor de zorg- en ondersteuning nodig is om cliëntgegevens bij externe partijen op te vragen, dan moet de medewerker hiervoor de toestemming van de cliënt vragen. Per opvraging moet toestemming worden gevraagd.

4.2.3 Wettelijke verplichting

Gegevens moeten worden verstrekt als hiervoor een wettelijke verplichting is. Dit is bijvoorbeeld het geval voor verstrekkingen aan gemeenten en zorgkantoren in het kader van de Wmo en Wlz of de verstrekking van bepaalde gegevens van medewerkers aan de belastingdienst.
Let wel: verstrekkingen in het kader van een wettelijke verplichting betekent niet dat alle gegevens verstrekt mogen worden. De verstrekking bevat altijd specifieke gegevens voor specifieke doeleinden. Ook moet de betrokkene op de hoogte gesteld worden van deze verstrekkingen.

4.2.4 Conflict van plichten

Als geen toestemming verkregen kan worden, maar de zorgprofessional ernstige schade aan de cliënt of aan een ander kan voorkomen door informatie aan een derde te verstrekken, dan mag informatie met een beroep op een conflict van plichten aan derden worden verstrekt. Daarbij moet wel aan de volgende voorwaarden zijn voldaan:

- Alles is in het werk gesteld om eerst toestemming van de cliënt te verkrijgen.
- De zwijgplichtige zorgprofessional verkeert in gewetensnood door het handhaven van de zwijgplicht.
- Er is geen andere weg dan doorbreking van het geheim om het probleem op te lossen.
- Het niet doorbreken van de zwijgplicht levert voor een ander ernstige schade op.

- Het moet vrijwel zeker zijn dat de door de geheimdoorbreking schade kan worden voorkomen of beperkt.

Als de geheimhoudingsplicht (en het beroepsgeheim) op basis van 'conflict van plichten' wordt doorbroken, dan moet het geheim zo min mogelijk geschonden worden. Alleen direct relevante gegevens mogen verstrekt worden. Voor zover mogelijk moet je ook aan een cliënt melden dat gegevens aan een ander zijn verstrekt.

4.2.5 Meldrecht

In bepaalde gevallen geldt een meldrecht. Bijvoorbeeld bij vermoedens van huiselijk geweld.

5 Gebruik gegevens voor wetenschappelijk onderzoek

5.1 Wanneer mogen gegevens aan een ander worden verstrekt voor wetenschappelijk onderzoek en statistiek op het gebied van de volksgezondheid?

De gegevensverwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden is onderworpen aan passende waarborgen in overeenstemming met de AVG voor de rechten en vrijheden van de betrokkene. De waarborgen zorgen ervoor dat er technische en organisatorische maatregelen zijn getroffen om de inachtneming van het beginsel van minimale gegevensverwerking te garanderen. Deze maatregelen kunnen pseudonimisering omvatten, mits aldus die doeleinden in kwestie kunnen worden verwezenlijkt. Wanneer die doeleinden kunnen worden verwezenlijkt door verdere verwerking die de identificatie van betrokkenen niet of niet langer toelaat, moeten zij aldus worden verwezenlijkt. Ook kan in nationale wetgeving worden afgeweken van bepaalde rechten van betrokkenen uit de AVG, voor zover die rechten de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken.

De Wgbo geeft onderstaande afwijkende bepalingen voor wetenschappelijk onderzoek op het gebied de van gezondheidszorg. Het uitgangspunt is dat voor het verstrekken van niet geanonimiseerde gegevens toestemming van de cliënt is vereist. In afwijking van dit uitgangspunt kan ook zonder toestemming van de cliënt voor statistiek of wetenschappelijk onderzoek op het gebied van de volksgezondheid aan een ander desgevraagd inlichtingen over de cliënt of inzage in de bescheiden, worden verstrekt als:

- het vragen van toestemming in redelijkheid niet mogelijk is en bij de uitvoering van het onderzoek zodanige waarborgen gelden, dat de persoonlijke levenssfeer van de cliënt niet onevenredig wordt geschaad of
- het vragen van toestemming, gelet op de aard en het doel van het onderzoek, in redelijkheid niet kan worden verlangd en de hulpverlener ervoor zorgt dat gegevens in zodanige vorm worden verstrekt dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen.

Verder moet:

- het onderzoek een algemeen belang dienen
- aangetoond zijn dat het onderzoek niet zonder de gegevens kan worden uitgevoerd
- de betrokken cliënt tegen een verstrekking niet uitdrukkelijk bezwaar hebben gemaakt

Belangrijk om te beseffen is dat bovenstaande voorwaarden cumulatief werken. Verstrekking is pas mogelijk als aan alle voorwaarden is voldaan.

5.2 Afspraken met de onderzoeker

Joris Zorg en de onderzoeker maken schriftelijke afspraken over de maatregelen die de onderzoeker neemt om de privacy van betrokkenen te beschermen. Deze afspraken staan in de samenwerkingsovereenkomst. In de samenwerkingsovereenkomst is opgenomen dat de onderzoeker toestemming vraagt aan de cliënt, waarbij gebruik wordt gemaakt van het toestemmingsformulier van Joris Zorg. Toestemmingsformulieren worden opgeslagen in het elektronisch dossier van de cliënt.

6 Rechten van betrokkenen

6.1 Voorwaarden met betrekking tot de uitvoering van de rechten van de betrokkenen

Het verstrekken van de in dit hoofdstuk bedoelde informatie, het verstrekken van de communicatie en het treffen van de maatregelen gebeuren kosteloos. Als het verzoek kennelijk ongegrond of buitensporig is, met name vanwege het repetitieve karakter, mag Joris Zorg:

- een redelijke vergoeding aanrekenen in het licht van de administratieve kosten, waarmee het verstrekken van de gevraagde informatie of communicatie en het treffen van de gevraagde maatregelen gepaard gaan ***of***
- weigeren gevolg te geven aan het verzoek.

Het is aan Joris Zorg om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.

Joris Zorg verstrekt de betrokkene zo snel mogelijk en in ieder geval binnen een maand na ontvangst van het verzoek informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van het verzoek en van het aantal verzoeken kan die termijn als dat nodig is met nog eens twee maanden worden verlengd. Joris Zorg stelt de betrokkene binnen een maand, na ontvangst van het verzoek, in kennis van een dergelijke verlenging. Als de betrokkene zijn verzoek elektronisch indient, wordt de informatie als dat mogelijk is elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.
Als Joris Zorg het verzoek van betrokkene afwijst, geeft zij daarvan schriftelijk de reden. Joris Zorg deelt een afwijzing van het verzoek zo snel mogelijk en uiterlijk binnen een maand na ontvangst van het verzoek aan de verzoeker mee. Ook informeert Joris Zorg de verzoeker over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens en de mogelijkheid om beroep in te stellen bij de rechter.

Betrokkenen kunnen verzoeken voor de uitoefening van hun rechten richten tot het ServicePunt, cliënten-administratie, of HR-administratie. Om verzoeken van betrokkenen in te willigen wordt de identiteit van de betrokkene gecontroleerd. Dit is noodzakelijk om te verifiëren dat verzoeken niet onrechtmatig (door onbevoegden) worden ingediend.

6.2 Recht op inzage en afschrift/kopie

De betrokkene heeft recht op inzage en een kopie van de op zijn of haar persoon betrekking hebbende verwerkte gegevens. De inzage of afschrift verstrekking vindt plaats voor zover daarbij de persoonlijke levenssfeer van een ander niet wordt geschaad. Bijvoorbeeld: informatie over, of verstrekt door derden (niet-professionals), zoals familie en naastbetrokkenen of omstanders, wordt niet zonder voorafgaande toestemming van die derde verstrekt.

Een wettelijk vertegenwoordiger van een wilsonbekwame volwassene, heeft recht op inzage in, of afschrift van het dossier met dezelfde uitzondering voor informatie over of verstrekt door derden (de andere ouder, familie, naastbetrokkenen en omstanders) voor zover van die vertegenwoordigers toestemming voor de behandeling is vereist. De vertegenwoordiger krijgt alleen die informatie die noodzakelijk is voor het uitoefenen van zijn taken als vertegenwoordiger.

Als de zorgverlener door inlichtingen over de cliënt dan wel inzage in of afschrift van de bescheiden aan de (wettelijk) vertegenwoordiger te verstrekken niet geacht kan worden de zorg van een goede zorgverlener in acht te nemen, laat hij dit achterwege. Bijvoorbeeld als een wilsonbekwame volwassene bezwaar maakt tegen het verstrekken van (bepaalde) informatie aan kinderen. In dat geval kan een kind inzage in het dossier van de wilsonbekwame volwassene worden geweigerd. Onder omstandigheden kan de zorgverlener in dat geval feitelijk worden belemmerd om de wettelijk vertegenwoordigers voldoende te informeren om hun toestemming voor de behandeling van de wilsonbekwame volwassene te verkrijgen.

Inzagerecht cliënten

Cliënten kunnen inzage krijgen in hun dossier via het cliëntenportaal. Inzageverzoeken voor gegevens, die niet via het cliëntenportaal beschikbaar zijn, kunnen worden gericht aan het ServicePunt of cliënten-administratie.

Inzagerecht medewerkers

Medewerkers kunnen inzage krijgen in hun medewerkersdossier via de online werkplek.

6.3 Recht op informatie

6.3.1 Te verstrekken informatie

Als Joris Zorg gegevens bij de betrokkene zelf opvraagt om te verwerken, informeert zij de betrokkene in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm, voorafgaand aan het verkrijgen van zijn persoonsgegevens, over:

- de identiteit en de contactgegevens van Joris Zorg
- de contactgegevens van de Functionaris Gegevensbescherming
- de verwerkingsdoelen waarvoor de gegevens zijn bestemd, en de rechtsgrond voor de verwerking
- in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens

Daarnaast moet onderstaande aanvullende informatie worden verstrekt om behoorlijke en transparante verwerking te waarborgen:

- de periode gedurende welke de persoonsgegevens worden opgeslagen of, als dat niet mogelijk is, de criteria om die termijn te bepalen.
- de mogelijkheden die de betrokkene heeft om een verzoek om inzage, rectificatie of wissing van de persoonsgegevens of beperking van de hem betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid.
- Als de gegevensverwerking op toestemming is gebaseerd, moet de betrokkene geïnformeerd worden over het recht om te allen tijde die toestemming in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming voor de intrekking daarvan.
- het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens en op welke wijze de betrokkene deze rechten kan inroepen.
- of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt.

Als Joris Zorg van plan is de persoonsgegevens verder te verwerken voor een ander doel dan waarvoor de persoonsgegevens zijn verzameld, verstrekt Joris Zorg de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in het tweede lid van deze bepaling.
Bovenstaande is niet van toepassing als en voor zover de betrokkene al over de informatie beschikt.

6.3.2 Te verstrekken informatie als de persoonsgegevens niet van de betrokkene zijn verkregen

Als persoonsgegevens niet van de betrokkene zijn verkregen, verstrekt Joris Zorg de betrokkene alle informatie volgens hierboven. Bovendien verstrekt zij de betrokken categorieën van persoonsgegevens en de bron waar de persoonsgegevens vandaan komen.

Joris Zorg verstrekt de in hoofdstuk 6.3.1 bedoelde informatie:

- binnen een redelijke termijn, maar uiterlijk binnen een maand na het verkrijgen van de persoonsgegevens, afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt.
- als de persoonsgegevens worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene *of*
- als de verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.

Joris Zorg hoeft de betrokkene niet te informeren over de hiervoor genoemde informatie als:

- de betrokkene al over de informatie beschikt;
- het informeren van betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In het bijzonder bij verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, behoudens de in artikel 89, lid 1, AVG bedoelde voorwaarden en waarborgen, of voor zover de in dit artikel bedoelde verplichting de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. In dergelijke gevallen neemt Joris Zorg passende maatregelen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie;
- het verkrijgen of verstrekken van informatie (zoals hiervoor genoemd) op grond van wet- en regelgeving verplicht is voor Joris Zorg en die wet- en regelgeving voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen *of*
- de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van wet- en regelgeving, waaronder een statutaire geheimhoudingsplicht.

6.3.3 Wijze van informatieverstrekking

De informatie wordt in een verklaring bescherming persoonsgegevens (privacyverklaring) aangeboden. Deze verklaringen zijn voor iedereen op papier en digitaal (Joris Familie en website) beschikbaar.

Joris Zorg stelt de verklaringen bescherming persoonsgegevens actief beschikbaar bij het eerste contactmoment met cliënten en medewerkers (waaronder externen, stagiaires en vrijwilligers). Dit is in ieder geval op het moment van aanmelding van de cliënt of op het eerste contactmoment van de cliënt met Joris Zorg, op het moment van indiensttreding van medewerkers (waaronder stagiaires, vrijwilligers en externen) en bij het eerste contact met de sollicitant. Als betrokkenen vragen hebben over hun persoonsgegevensbescherming, dan verwijst Joris Zorg naar de verklaringen bescherming persoonsgegevens.

6.4 Recht op gegevensoverdraagbaarheid (dataportabiliteit)

De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan Joris Zorg heeft verstrekt, in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen. Hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke (bijvoorbeeld andere zorgaanbieder) over te dragen, zonder daarbij te worden gehinderd door Joris Zorg. Dit geldt alleen als de verwerking berust op toestemming of op uitvoering van een overeenkomst en de verwerking geautomatiseerd wordt verricht. Bij de uitoefening van het recht op gegevensoverdraagbaarheid heeft de betrokkene het recht dat de persoonsgegevens, als dit technisch mogelijk is, rechtstreeks van de ene zorgaanbieder naar de andere worden doorgezonden. Bij de uitoefening van dit recht mag dit geen afbreuk doen aan de rechten en vrijheden van anderen.

6.5 Recht op rectificatie, aanvulling en beperking van persoonsgegevens

De betrokkene kan Joris Zorg vragen om rectificatie (verbetering) van de hem of haar betreffende persoonsgegevens als die onjuist zijn. Hij kan ook Joris Zorg verzoeken om vervolledigen van zijn of haar persoonsgegevens. Dit met in achtneming van het doel van de verwerking, onder meer door een eigen aanvullende verklaring toe te voegen aan zijn dossier. Betrokkenen kunnen ook aan Joris Zorg vragen om bepaalde gegevens voor bepaalde personen af te schermen en hen de toegang tot die gegevens te laten blokkeren.

Cliënten en medewerkers kunnen hiervoor terecht bij respectievelijk het ServicePunt, cliënten-administratie, of HR-administratie. Het verzoek van een betrokkene en beslissing van Joris Zorg tot rectificatie (verbetering), aanvulling of beperking van gegevens blijft bewaard in het dossier van de cliënt of medewerker.

6.6 Recht op gegevenswissing (recht op vergetelheid)

De betrokkene heeft het recht van Joris Zorg zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen. Joris Zorg is verplicht deze persoonsgegevens te wissen als één van de volgende gevallen van toepassing is:

- de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt
- de betrokkene trekt de toestemming waarop de verwerking berust in en er geen andere rechtsgrond is voor de verwerking
- de persoonsgegevens onrechtmatig zijn verwerkt
- op basis van een wettelijke verplichting, die op Joris Zorg rust, waarbij de persoonsgegevens moeten worden gewist

Joris Zorg stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van de wissing (verwijdering) van persoonsgegevens, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. Joris Zorg verstrekt de betrokkene informatie over deze ontvangers als de betrokkene hierom vraagt.

Als Joris Zorg de persoonsgegevens openbaar heeft gemaakt en verplicht is de persoonsgegevens te wissen, neemt zij, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen, waaronder technische maatregelen, om verwerkingsverantwoordelijken die de persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene de verwerkingsverantwoordelijken heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen.

Als het gezondheidsgegevens betreft, wist Joris Zorg de gegevens zonder onredelijke vertraging en verstrekt de betrokkene in ieder geval binnen een maand na ontvangst van het verzoek informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn als dat nodig is met nog eens twee maanden worden verlengd. Joris Zorg stelt de betrokkene binnen een maand na ontvangst van het verzoek in kennis van een dergelijke verlenging.

Een verzoek tot gegevenswissing mag alleen worden geweigerd als:

- de wet zich tegen de vernietiging verzet.
- een derde een aanmerkelijk belang heeft bij bewaring van die gegevens. Bijvoorbeeld als een kind van een cliënt een erfelijke ziekte heeft.
- de cliënt heeft een procedure tegen de hulpverlener aangespannen of het is waarschijnlijk dat dit zal doen.

- Joris Zorg de gegevens nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering.
- om redenen van algemeen belang op het gebied van volksgezondheid.

Cliënten en medewerkers kunnen zich voor verzoeken tot wissing van gegevens wenden tot respectievelijk het ServicePunt, cliënten-administratie, of HR-administratie. Het verzoek tot wissing van een betrokkene en reactie van Joris Zorg hierop blijft bewaard in het dossier van de cliënt of medewerker.

6.7 Recht van bezwaar

De betrokkene heeft te allen tijde het recht om vanwege, met zijn specifieke situatie verband houdende redenen, bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens. Dit op basis van de noodzakelijkheid voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan Joris Zorg is opgedragen of op basis van de noodzakelijkheid voor de behartiging van de gerechtvaardigde belangen van Joris Zorg of van een derde.

Joris Zorg beoordeelt zo snel mogelijk en in ieder geval binnen een maand na ontvangst van het bezwaar of het bezwaar gerechtvaardigd is. Als het bezwaar gerechtvaardigd is, beëindigt zij onmiddellijk de verwerking, tenzij sprake is van dwingende gerechtvaardigde gronden voor de verwerking die zwaarder wegen dan de belangen, vrijheden en rechten van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.

6.8 Vertegenwoordiging

6.8.1 Wilsonbekwame cliënt

Is de betrokkene wilsonbekwaam ter zake, dan treedt als vertegenwoordiger voor hem op:

- een (toegewezen) curator of mentor
- als er geen curator of mentor is, de persoon die de cliënt schriftelijk heeft gemachtigd
- als de persoonlijk gemachtigde ontbreekt of niet optreedt, dan de echtgenoot of levensgezel van de betrokkene
- als de echtgenoot of levensgezel ontbreekt of niet optreedt, dan een kind, broer of zus van de betrokkene.

In het uiterste geval treedt Joris Zorg als zorgaanbieder op als goed hulpverlener. Joris Zorg zorgt er dan voor dat zo snel mogelijk een wettelijk vertegenwoordiger voor de betrokkene optreedt. Zo nodig, als familie of naaste dat niet kan of wil, verzoekt Joris Zorg de rechter om een vertegenwoordiger te benoemen.

7 Bewaartermijnen

Joris Zorg moet de papieren en elektronische persoonsgegevens op een veilige wijze bewaren, die in overeenstemming is met de geldende wet- en regelgeving. Persoonsgegevens worden niet langer bewaard dan noodzakelijk is om de doelen te bereiken waarvoor de gegevens worden verwerkt, tenzij de gegevens worden geanonimiseerd of als het noodzakelijk is voor de uitoefening van het recht op vrijheid van meningsuiting en van informatie, voor de nakoming van een wettelijke verplichting, voor de uitvoering van een taak in het algemeen belang of in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend, om redenen van algemeen belang op het vlak van volksgezondheid, met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden of voor de vaststelling, uitoefening of onderbouwing van een rechtsvordering.[1]

Joris Zorg stelt vast hoelang de vastgelegde/geregistreerde persoonsgegevens bewaard blijven in overeenstemming met de geldende wet- en regelgeving. Als nog geen specifieke termijn kan worden genoemd dan worden de criteria vastgesteld voor het vaststellen van de bewaartermijn.
Voor gezondheidsgegevens die binnen de zorgrelatie worden verwerkt, zoals het dossier van de cliënt, gelden verschillende bewaartermijnen. De bewaartermijnen van Joris Zorg staan benoemd in het 'bewaartermijnenbeleid' van Joris Zorg. Deze is terug te vinden op Joris Familie.

[1] Artikel 17, derde lid, AVG (overweging 65).

8 Veilige omgang met gegevens

8.1 Verantwoordelijkheid van de verwerkingsverantwoordelijke

Rekening houdend met de aard, de omvang, de context en het doel van de verwerking en met de, wat waarschijnlijkheid en ernst betreft, uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft Joris Zorg passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Die maatregelen worden geëvalueerd en, als dat nodig is, geactualiseerd.

8.2 Gegevensbescherming door ontwerp en standaardinstellingen (Privacy by design en default)

Joris Zorg treft passende technische en organisatorische maatregelen, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen om de naleving van de voorschriften van deze verordening en om de bescherming van de rechten van de betrokkenen. Deze maatregelen worden bij de bepaling van de verwerkingsmiddelen én bij de verwerking zelf getroffen. Joris Zorg houdt hierbij rekening met de stand van de techniek, de uitvoeringskosten, de aard, de omvang, de context en het doel van de verwerking en met de, wat waarschijnlijkheid en ernst betreft, uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, die aan de verwerking zijn verbonden.
Joris Zorg treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt. Een goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat aan de voorschriften is voldaan.

Praktische uitwerking:

- Joris Zorg beoordeelt of er voor de veilige verwerking van zorggegevens al voldaan wordt aan de NEN-normen 7510, 7512 en 7513.
- Voor de verstrekking van gegevens via e-mail wordt gebruik gemaakt van een beveiligde e-mailverbinding.
- Joris Zorg werkt volgens de 'Richtsnoeren beveiliging persoonsgegevens' van de Autoriteit Persoonsgegevens en de 'Praktijkgids patiëntgegevens in de cloud' van de Autoriteit Persoonsgegevens.
- De identificerende gegevens zijn zoveel mogelijk gescheiden opgeslagen van de inhoudelijke gegevens, gepseudonimiseerd of versleuteld.
- De standaardinstellingen zijn 'nee, tenzij' (opt-in) in plaats van 'ja, mits' (opt-out), tenzij de wetgeving opt-out toelaatbaar stelt.
- Joris Zorg beoordeelt per verwerking of voldaan wordt aan het autorisatieprotocol. Daarin staat welke gegevens door wie/welke (groepen) medewerkers verwerkt kunnen worden en waarom en welke bevoegdheden zij hebben voor welke gegevens (inzage, toevoegen, wijzigen, verwijderen).

8.3 Gezamenlijke verwerkingsverantwoordelijken

Als twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectievelijke verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze AVG vast, met name voor het uitoefenen van de rechten van de betrokkene en hun respectievelijke verplichtingen om de verplichte informatie te verstrekken in een onderlinge regeling. In deze regeling kan een contactpunt voor betrokkenen worden aangewezen.

Uit de bedoelde regeling blijkt duidelijk welke rol de gezamenlijke verwerkings-verantwoordelijken respectievelijk vervullen en wat hun respectievelijke verhouding met de betrokkenen is. De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld.

Ongeacht een dergelijke regeling kan een betrokkene zijn rechten uit de AVG voor en jegens iedere verwerkingsverantwoordelijke uitoefenen.

8.4 Register van verwerkingen

Joris Zorg houdt een register bij van de verwerkingsactiviteiten die onder haar verantwoordelijkheid plaatsvinden. Dit register bevat in ieder geval de volgende gegevens:

- de naam en de contactgegevens van Joris Zorg en eventuele gezamenlijke verwerkingsverantwoordelijken en van de Functionaris Gegevensbescherming
- de verwerkingsdoeleinden
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties
- als het van toepassing is de doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, van de AVG bedoelde doorgiften, de documenten inzake de passende waarborgen
- als het mogelijk is de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist
- als het mogelijk is een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen

Het register is in schriftelijke vorm, waaronder in elektronische vorm, opgesteld. Op verzoek stelt Joris Zorg het register ter beschikking aan de Autoriteit Persoonsgegevens.

8.5 Medewerking verlenen aan/samenwerken met de Autoriteit Persoonsgegevens[2]

Joris Zorg, de verwerker en, in voorkomend geval, hun vertegenwoordigers, werken op verzoek samen met de Autoriteit Persoonsgegevens bij het vervullen van haar taken.

8.6 Gegevensbeschermingseffectbeoordeling (DPIA)

Als een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert Joris Zorg vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden. Bij het uitvoeren van een gegevensbeschermingseffectbeoordeling wordt het advies van de Functionaris Gegevensbescherming ingewonnen.

Een gegevensbeschermingseffectbeoordeling is met name vereist in de volgende gevallen:

- als sprake is van verwerking van persoonsgegevens met het oog op het nemen van besluiten over specifieke natuurlijke personen, na een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen
- er sprake is van een grootschalige verwerking van bijzondere categorieën van persoonsgegevens, zoals gezondheidsgegevens
- er sprake is van stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten

De beoordeling bevat ten minste:

- een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden
- een beoordeling van het eerste lid van dit artikel bedoelde risico's voor de rechten en vrijheden van betrokkenen *en*
- de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie

Bij het beoordelen van het effect van de door Joris Zorg verrichte verwerkingen en met name ter wille van een gegevensbeschermingseffectbeoordeling, wordt de naleving van gedragscodes naar behoren in aanmerking genomen.

[2] Artikel 31 AVG.

Joris Zorg vraagt in voorkomend geval de betrokkenen of hun vertegenwoordigers naar hun mening over de voorgenomen verwerking, met inachtneming van de bescherming van commerciële of algemene belangen of de beveiliging van verwerkingen.

Als het nodig is, verricht Joris Zorg een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd, in ieder geval ten minste als sprake is van een verandering van het risico dat de verwerkingen inhouden.

8.7 Voorafgaande raadpleging van de Autoriteit Persoonsgegevens

Als uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren als Joris Zorg geen maatregelen neemt om het risico te beperken, raadpleegt Joris Zorg voorafgaand aan de verwerking de Autoriteit Persoonsgegevens.

Wanneer de Autoriteit Persoonsgegevens van oordeel is dat de bedoelde voorgenomen verwerking inbreuk zou maken op deze verordening, met name wanneer Joris Zorg het risico onvoldoende heeft onderkend of beperkt, geeft de Autoriteit Persoonsgegevens binnen maximaal acht weken na de ontvangst van het verzoek om raadpleging schriftelijk advies aan Joris Zorg en in voorkomend geval aan de verwerker, en mag zij al haar bevoegdheden uitoefenen. Die termijn kan, naargelang de complexiteit van de voorgenomen verwerking, met zes weken worden verlengd. Bij een dergelijke verlenging stelt de Autoriteit Persoonsgegevens Joris Zorg en, in voorkomend geval, de verwerker binnen een maand na ontvangst van het verzoek om raadpleging in kennis van onder meer de redenen voor de vertraging. Die termijnen kunnen worden opgeschort totdat de Autoriteit Persoonsgegevens informatie heeft verkregen waarom zij met het oog op de raadpleging heeft verzocht.

- Bij de raadpleging verstrekt Joris Zorg de nodige informatie zoals benoemd in de AVG. In ieder geval moeten de volgende gegevens worden verstrekt:
    - als het van toepassing is de verantwoordelijkheden van Joris Zorg, bij de verwerking betrokken gezamenlijke verwerkingsverantwoordelijken en verwerkers, in het bijzonder voor een verwerking binnen een concern
    - de doeleinden en middelen van de voorgenomen verwerking
    - de maatregelen en waarborgen die worden geboden ter bescherming van de rechten en vrijheden van betrokkenen uit hoofde van de AVG
    - de contactgegevens van de Functionaris Gegevensbescherming
    - de gegevensbeschermingseffectbeoordeling voor die verwerking
    - alle andere informatie waar de Autoriteit Persoonsgegevens om verzoekt

8.8 Beveiliging van de verwerking

Rekening houdend met de stand van de techniek, de uitvoeringskosten en met de aard, de omvang, de context en de verwerkingsdoeleinden en de, wat waarschijnlijkheid en ernst betreft, uiteenlopende risico's voor de rechten en vrijheden van personen, treffen Joris Zorg en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

- de pseudonimisering en versleuteling van persoonsgegevens
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking

Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk, hetzij onrechtmatig.

Het aansluiten bij een goedgekeurde gedragscode of een goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat de in hoofdstuk 9 bedoelde vereisten worden nageleefd.

Joris Zorg en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van Joris Zorg of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van Joris Zorg verwerkt, tenzij hij daartoe volgens wet- en regelgeving is gehouden.

8.9 Meldplicht datalekken

8.9.1 Melding van een inbreuk in verband met persoonsgegevens aan de Autoriteit Persoonsgegevens (datalekken melden aan de AP) en datalekkenregister

Als een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt Joris Zorg dit zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat zij er kennis van heeft genomen, aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Als de melding aan de Autoriteit Persoonsgegevens niet binnen 72 uur plaatsvindt, wordt de vertraging toegelicht (gemotiveerd).

De verwerker informeert Joris Zorg zonder onredelijke vertraging, zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.
In de melding aan de Autoriteit Persoonsgegevens wordt ten minste het volgende omschreven of meegedeeld:

- de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie
- de naam en de contactgegevens van de Functionaris Gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens
- de maatregelen die Joris Zorg heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan

Als en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

Joris Zorg houdt alle inbreuken in verband met persoonsgegevens bij in een overzicht, met inbegrip van de feiten omtrent die inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de Autoriteit Persoonsgegevens in staat de naleving van dit artikel te controleren.

8.9.2 Melding van een inbreuk in verband met persoonsgegevens aan de betrokkenen (datalekken melden aan de betrokkene)

Als de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt Joris Zorg de betrokkene de inbreuk in verband met persoonsgegevens zo snel mogelijk mee. De bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in het vorige artikel 8.9.1 bedoelde gegevens en maatregelen.

De mededeling aan de betrokkene is niet vereist als één van de volgende voorwaarden is vervuld:

1. Joris Zorg heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
2. Joris Zorg heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
3. de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.
4. als Joris Zorg de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de Autoriteit Persoonsgegevens, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, Joris Zorg daartoe verplichten of besluiten dat aan een van de in lid 3 van dit artikel, bedoelde voorwaarden is voldaan.

8.10 Afhandeling datalekken

(Vermoedens van) datalekken worden gemeld via de knop 'Datalek melden' op ServicePunt**.** De Functionaris Gegevensbescherming beoordeelt of het datalek moet worden gemeld aan de Autoriteit Persoonsgegevens. Als dit het geval is, meldt de Functionaris Gegevensbescherming het datalek binnen 72 uur. Als het datalek nadelige gevolgen heeft voor cliënten en/of medewerkers, wordt dit zo snel mogelijk aan hen gemeld. Zij kunnen dan maatregelen nemen. Dit is bijvoorbeeld als wachtwoorden of pincodes verloren zijn geraakt. De Functionaris Gegevensbescherming zorgt ervoor dat maatregelen worden getroffen om de gevolgen van het datalek te beperken.

8.11 Aanstelling van de Functionaris Gegevensbescherming

Joris Zorg is wettelijk verplicht om een Functionaris Gegevensbescherming aan te stellen. Deze plicht vloeit voort uit het feit dat Joris Zorg hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens, namelijk gezondheidsgegevens. De Functionaris Gegevensbescherming wordt binnen en buiten de organisatie bekend gemaakt en is aangemeld bij de Autoriteit Persoonsgegevens.

De Functionaris Gegevensbescherming wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk over gegevensbescherming en zijn vermogen de hieronder bedoelde taken te vervullen. De vereiste expertise en vaardigheden omvatten in ieder geval

- kennis van nationale en Europese privacywet- en regelgeving over gegevensbescherming
- begrip van de gegevensverwerkingen die de organisatie uitvoert
- begrip van IT en informatiebeveiliging
- kennis van de organisatie en de sector waarin die actief is
- vaardigheden om binnen de organisatie een cultuur van gegevensbescherming te ontwikkelen.

De Functionaris Gegevensbescherming kan een personeelslid van Joris Zorg zijn of kan de taken op grond van een dienstverleningsovereenkomst verrichten.
Joris Zorg maakt de contactgegevens van de Functionaris Gegevensbescherming bekend en deelt die mee aan de Autoriteit Persoonsgegevens.

De contactgegevens van de Functionaris Gegevensbescherming worden via de gangbare kanalen voor iedereen toegankelijk gepubliceerd.

8.12 Positie van de Functionaris Gegevensbescherming

Joris Zorg zorgt ervoor dat de Functionaris Gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Concreet heeft een Functionaris Gegevensbescherming onder meer het volgende nodig om de functie in te vullen:

- de actieve steun vanuit het management
- voldoende tijd om de taken uit te voeren
- voldoende praktische ondersteuning (budget, faciliteiten en personeel)
- heldere communicatie aan al het personeel over de benoeming van de FG
- scholing

Joris Zorg ondersteunt de Functionaris Gegevensbescherming bij de vervulling van hieronder bedoelde taken door hem toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in standhouden van zijn deskundigheid.

Joris Zorg zorgt ervoor dat de Functionaris Gegevensbescherming geen instructies ontvangt voor het uitvoeren van die taken; de Functionaris Gegevensbescherming werkt zelfstandig en onafhankelijk. De Functionaris Gegevensbescherming wordt niet ontslagen of gestraft voor de uitvoering van zijn taken en ondervindt geen nadeel van de uitoefening van zijn taak. De Functionaris Gegevensbescherming brengt rechtstreeks verslag uit aan de raad van bestuur.

Betrokkenen kunnen met de Functionaris Gegevensbescherming contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun persoonsgegevens en met de uitoefening van hun rechten uit de AVG. De Functionaris Gegevensbescherming is voor het uitvoeren van zijn taken tot geheimhouding of vertrouwelijkheid gehouden. De Functionaris Gegevensbescherming kan andere taken en plichten vervullen. Joris Zorg zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden. Om belangenverstrengeling te voorkomen, mag de Functionaris Gegevensbescherming binnen de organisatie niet ook een functie hebben waarin hij het doel en de middelen van een gegevensverwerking bepaalt. Dit kan

bijvoorbeeld zo zijn als de Functionaris Gegevensbescherming een managementpositie vervult, zoals hoofd financiën, strategie, marketing, IT of HRM.

8.13 Taken van de Functionaris Gegevensbescherming

De Functionaris Gegevensbescherming vervult ten minste de volgende taken:

- Joris Zorg en haar werknemers informeren en adviseren over hun verplichtingen die voortkomen uit de privacywetgeving
- toezien op naleving van deze AVG, van andere gegevensbeschermingsbepalingen en van het beleid van Joris Zorg voor de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits
- op verzoek advies verstrekken met betrekking tot de gegevensbeschermingseffectbeoordeling (DPIA) en toezien op de uitvoering daarvan
- met de Autoriteit Persoonsgegevens samenwerken
- optreden als contactpunt voor de Autoriteit Persoonsgegevens voor aangelegenheden die verband houden met verwerking, met inbegrip van de voorafgaande raadpleging, en, waar passend, overleg plegen over enige andere aangelegenheid
- Onderhouden van het register met verwerkingsactiviteiten

De Functionaris Gegevensbescherming houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.

8.14 Klachten

Bij een klacht over de naleving van dit reglement kunnen cliënten en medewerkers zich richten tot de Functionaris Gegevensbescherming van Joris Zorg: **fg@joriszorg.nl**. Betrokkenen hebben ook het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens via: **www.autoriteitpersoonsgegevens.nl**.

Voor andere klachten volgen betrokkenen de reguliere klachtenprocedure.

9 Wijzigingen en inzage van dit reglement

Dit reglement gaat in per december 2024 en is te vinden op Joris Familie. Wij kunnen dit reglement wijzigen. Als deze wijzigingen gevolgen heeft voor betrokkenen, dan maken wij dit bekend op Joris Familie.

10 Begripsbepalingen

In dit reglement wordt verstaan onder:

Autoriteit Persoonsgegevens (AP):	de toezichthoudende autoriteit, de onafhankelijke instantie die erover waakt dat persoonsgegevens zorgvuldig en veilig worden verwerkt en zo nodig sancties kan opleggen als dat niet gebeurt.
Bestand:	elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn.
Betrokkene:	degene op wie een persoonsgegeven betrekking heeft, meestal de cliënt, of zijn (wettelijk) vertegenwoordiger.
Bijzondere categorieën persoonsgegevens:	persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid
Derde:	elke persoon of instantie die geen betrokkene, verwerkingsverantwoordelijke, verwerker, of een persoon is die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd is persoonsgegevens te verwerken.

Functionaris Gegevensbescherming (FG):	functionaris die door Joris Zorg moet of kan worden aangesteld voor het informeren en adviseren over en het toezicht houden op de toepassing en naleving van de AVG en andere gegevensbeschermingsbepalingen.
Gezondheidsgegevens	gegevens over de lichamelijke of geestelijke gezondheid van een persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;
Datalek:	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.
Medewerker:	alle in de organisatie werkzame personen, waaronder vaste medewerkers, externe (inhuur) krachten, stagiaires en vrijwilligers.
Persoonsgegevens:	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, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Pseudonimisering:	het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkenen kunnen worden gekoppeld zonder dat aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.
Toestemming:	door betrokkene, op goede informatie berustende, specifieke, in vrijheid en ondubbelzinnig gegeven toestemming waarbij betrokkene hem betreffende verwerking van persoonsgegevens aanvaardt. Dat kan door middel van een schriftelijke verklaring of een ondubbelzinnige actieve handeling.
Verwerker:	degene die in opdracht van en voor de verwerkingsverantwoordelijke persoonsgegevens verwerkt
Verwerking van persoonsgegevens:	Alle 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 in een andere vorm beschikbaar stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Verwerkingsverantwoordelijke:	degene die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; meestal de bestuurder van Joris Zorg.

Versie informatie

Versie	Medewerker	Wijziging
20241120	Paul Verlaek	Initiële versie

Dataclassificatie

Openbaar (laag)	**Deze data vormt geen direct risico voor de vertrouwelijkheid van de organisatie en is vrij toegankelijk.**
Intern	Deze data mag alleen beschikbaar zijn voor interne medewerkers en mag derhalve niet extern worden gepubliceerd.
Vertrouwelijk	Data in deze classificatiecategorie mag alleen ingezien, gemuteerd of verwijderd worden door bepaalde groep(en) gebruikers.
Geheim (hoog)	Alleen topmanagement mag inzicht krijgen in documentatie van deze categorie.