

# AVG verklaring



## ZONpraktijk

Uitgegeven op 27-2-2023

✓ Geldig tot 27-5-2023

## **De bescherming van persoonlijke gegevens is geen eenmalige zaak.**

Ook al heb je het eenmalig goed ingericht, de wet vereist dat je met een actueel document kunt aantonen dat je voldoet aan de AVG. De Autoriteit Persoonsgegevens (AP) controleert dat steekproefsgewijs.

Deze AVG-verklaring laat zien dat je alle verplichtingen vanuit de wet AVG hebt uitgevoerd (mits je alle onderdelen hebt ingevoerd). Als er iets verandert in jouw organisatie kun je de stappen opnieuw bekijken en eventueel aanpassen. Daarna vraag je de AVG-verklaring opnieuw op door op de "Verklaring Aanmaken" knop te klikken.

Ook ontvang je elk kwartaal automatisch een nieuwe AVG-verklaring. Bewaar deze digitaal of print hem uit. Zo ben je altijd up-to-date!

# AVG verklaring

Hierbij verklaart de Stichting AVG voor Verenigingen dat ZONpraktijk het AVG-programma geheel of gedeeltelijk heeft doorlopen. ZONpraktijk verklaart hiermee dat de inspanningen zijn verricht zoals die voortvloeien uit de Algemene Verordening Gegevensbescherming (AVG).

Indien niet alle programmaonderdelen zijn afgewerkt en de verklaring toch wordt aangevraagd, dan is geen volledige invulling gegeven aan de eisen van de wetgever. De Stichting AVG voor Verenigingen adviseert de openstaande punten alsnog zo snel mogelijk af te werken en in elk geval in het programma een aantekening te maken wanneer dit zal gebeuren.

In de hierna volgende verklaring staan alle onderdelen/stappen die ZONpraktijk heeft doorlopen om te voldoen aan de AVG-wetgeving. Per onderdeel is duidelijk aangegeven welke gegevens en onderdelen van de wet van toepassing zijn en hoe daar aan voldaan is. Waar nodig is additionele informatie verstrekt ter verduidelijking van de situatie.

ZONpraktijk begrijpt dat AVG-wetgeving continu van toepassing is en dat zij regelmatig de gegevens moeten controleren en updaten.

Met het volledig doorlopen van het AVG-programma van de Stichting AVG voor Verenigingen heeft ZONpraktijk kennis over de materie ontvangen die door de AVG wordt geraakt, en verklaart zelf naar eer en geweten aan de wet te voldoen. De onderdelen van de zelfverklaring door ZONpraktijk zijn te vinden op de volgende pagina(s) van deze verklaring.

Aldus opgemaakt te Gorinchem,

d.d. 27-2-2023,

door Stichting AVG voor Verenigingen

gevestigd aan de Stephensonweg 14 te Gorinchem.

## 2.1 Inventarisatie persoonsgegevens

Geef hieronder aan welke persoonsgegevens binnen de organisatie gebruikt worden.

### Gewone persoonsgegevens

- Naam / voorletters / tussenvoegsel
- Titels
- Adres
- Postcode
- Plaats
- Provincie
- Land
- Woonplaats
- Telefoonnummer
- Faxnummer
- E-mailadres
- Website
- Geslacht
- Geboortedatum
- Geboorteplaats
- Overlijdensdatum
- Burgerlijke staat
- LinkedIn
- Facebook
- Twitter
- Werkzaam bij organisatie

- Bankrekeningnummer
- Inloggegevens (gebruikersnaam / wachtwoord)
- Voertuig kentekenplaat
- Salarisgegevens

### **Andere gewone persoonsgegevens**

*Uw situatie:*

### **Bijzondere persoonsgegevens**

- Ras of etnische afkomst
- Politieke opvattingen
- Religieuze of levensbeschouwelijke overtuiging
- Lidmaatschap van een vakbond
- Genetische of biometrische gegevens met het oog op unieke identificatie
- Gegevens over gezondheid
- Gegevens over seksueel gedrag of seksuele gerichtheid
- Strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen
- Kopie identiteitsbewijs/paspoort, zonder voorlegger gekopieerd
- BSN-nummer

### **Aantekeningen bijzondere persoonsgegevens**

Genoemde gegevens zijn nodig voor het voeren van een BGGZ praktijk.  
Aanvullend nodig:  
Verzekeringsgegevens  
Medische-psychiatrische voorgeschiedenis  
Verwijzing van de huisarts/medisch specialist

## 3.1 Inventarisatie doelbinding

### Grondslag

Je moet een goede reden hebben om persoonsgegevens te mogen verwerken. De juridische naam voor die redenen is grondslagen. Je hebt dus een grondslag nodig om persoonsgegevens te mogen verwerken. In de AVG staan de volgende 6 grondslagen voor het verwerken van persoonsgegevens:

- U heeft toestemming van de persoon om wie het gaat,
- Het is noodzakelijk om gegevens te verwerken,
  - om een overeenkomst uit te voeren,
  - omdat u dit wettelijk verplicht bent,
  - om vitale belangen te beschermen,
  - om een taak van algemeen belang of openbaar gezag uit te oefenen.
- Het is noodzakelijk om gegevens te verwerken om uw gerechtvaardigde belang te behartigen.

Voorbeelden van grondslagen zijn:

- Toestemming = ondertekening van een toestemmingsformulier of een inschrijving door middel van een opt-in voor een nieuwsbrief,
- Overeenkomst = je hebt deze persoonsgegevens nodig voor het uitvoeren van een overeenkomst (b.v. een koopcontract of een lidmaatschapsovereenkomst),
- Gerechtvaardigd belang = bestaande klanten na een aankoop te informeren over soortgelijke, eigen producten of diensten.

### Doelbinding

Welke persoonsgegevens verwerk je, met welk doel en heb je ze daar ook voor gekregen (grondslag)? Dat noemen we 'doelbinding'. Het is belangrijk dat je persoonsgegevens alleen verwerkt (dus opslaat en gebruikt) voor de doeleinden waarvoor je deze hebt verkregen. In de doelbinding beschrijf je dus welke gegevens, met welke grondslag en wat je met die gegevens doet.

Voor de inventarisatie van de vormen van doelbinding binnen de organisatie hebben wij onderstaand schema gemaakt. Voor doelbindingen die veel voorkomen, hebben wij het schema al ingevuld en die kun je dus zo aanvinken. Komen er binnen je organisatie nog andere doelbindingen voor, dan kun je deze in de open vorm noteren bij 3.3.

## Bewaartermijn

Het uitgangspunt is dat je persoonsgegevens niet langer mag bewaren dan noodzakelijk. Wat noodzakelijk is hangt af van de situatie. Dit staat niet concreet beschreven in de AVG en dus moet je bepalen wat in jouw situatie passend is.

Wel zijn er andere wettelijke termijnen waar je je aan moet houden. Bijvoorbeeld op grond van belastingwetgeving of de Archiefwet. Zo moet je voor de belastingdienst je administratie 7 jaar bewaren.

**LET OP:** Je bent wettelijk verplicht zo min mogelijk persoonsgegevens te verwerken. Vraag dus alleen de gegevens die je echt nodig hebt voor het goed functioneren van je organisatie.

(N = Naam, A = Adres, W = Woonplaats, T = Telefoon, E = e-mailadres)

Klant of leverancier

<b>Persoonsgegevens</b>	NAWTE
<b>Grondslag</b>	Opdracht of contract
<b>Verwerkingen</b>	Administratie, bevestiging, uitlevering
<b>Verwerkt door</b>	Afdeling administratie, afdeling sales en afdeling inkoop
<b>Bewaartermijn</b>	Gedurende de looptijd van de overeenkomst

Verwerkersovereenkomst met provider EPD, Intramed.  
Verwerkersovereenkomst met beheerder website, VDP Automation.  
Opdrachtovereenkomst met TVN-zorgt te Nijmegen, als onderaannemer.  
Verwerkersovereenkomst met Zorgmail.

Klant en BSN

Organisaties buiten de overheid mogen het BSN (burger-servicenummer) alleen gebruiken als dat volgens de wet is toegestaan. Anders mag het niet! Het is toegestaan voor bijvoorbeeld werkgevers, zorgverleners, zoals huisartsen en apotheken en ook voor zorgverzekeraars. Ook in het onderwijs wordt het BSN gebruikt. Hier heet het ook wel onderwijsnummer of persoonsgebonden nummer. Organisaties kunnen niet onder het verbod uitkomen door mensen toestemming te vragen voor het gebruik van hun BSN!

<b>Persoonsgegevens</b>	NAWTE + BSN
<b>Grondslag</b>	Overeenkomst met handtekening op papier
<b>Verwerkingen</b>	Interactie met de overheid in het belang van (en met toestemming van) de klant
<b>Verwerkt door</b>	Afdeling administratie
<b>Bewaartermijn</b>	Gedurende de looptijd van de overeenkomst

Hierbij wordt verwezen naar de gegevens die we verzamelen via het aanmeldformulier, zie daartoe het formulier op de website. Deze gegevens worden digitaal bewaard in een beveiligd EPD en het aanmeldformulier wordt in een afgesloten dossierkast bewaard. Hierbij wordt ook verwezen naar de gegevens die uitgevraagd worden in de intake. Die komen in een behandelplan. Dat wordt opgeslagen in een beveiligd EPD.

 VvE-leden en -gebruikers

Het bestuur van de VvE dient op grond van het reglement ex artikel 5:112 BW een register bij te houden van eigenaars en een register van gebruikers. In dit register zijn persoonsgegevens opgenomen.

<b>Persoonsgegevens</b>	NAWTE + bankgegevens + kentekengegevens
<b>Grondslag</b>	Akte van splitsing en het reglement ex artikel 5:112 BW
<b>Verwerkingen</b>	Beheeractiviteiten van de VvE in de breedste zin van het woord in het belang van (en met toestemming van) de (gezamenlijke) eigenaars.
<b>Verwerkt door</b>	Bestuur en beheerder
<b>Bewaartermijn</b>	Gedurende lidmaatschap of gebruik en 12 maanden daarna en voorts alleen in de financiële administratie voor maximaal 7 jaar



Aanmelden voor nieuwsbrief

<b>Persoonsgegevens</b>	Naam en e-mailadres
<b>Grondslag</b>	Aanmelding voor nieuwsbrief (formulier op de website)
<b>Verwerkingen</b>	Informatie verstrekking in de vorm van nieuwsbrieven.
<b>Verwerkt door</b>	Afdeling communicatie
<b>Bewaartermijn</b>	Gedurende de periode dat men aangemeld is

Prospect, stakeholder-/lobbycontacten en geïnteresseerde

<b>Persoonsgegevens</b>	NAWTE
<b>Grondslag</b>	Mondelinge toestemming, afgifte visitekaartje en/of via LinkedIn
<b>Verwerkingen</b>	Informatieverstrekking in de vorm van nieuwsbrieven of gerichte contacten.
<b>Verwerkt door</b>	Afdeling communicatie, directie, vakkennisafdelingen en/of relatie beheerder
<b>Bewaartermijn</b>	Gedurende de periode dat men contact heeft

(Nog) geen overeenkomst maar wel geïnteresseerd in de zorg die we aanbieden. Daar vallen bv de mensen onder die via het contactformulier website of via de mail een vraag stellen en/of een afspraak willen maken.  
We houden een termijn aan van 2-4 weken. Daarna worden gegevens verwijderd.

Stakeholder-/lobbycontacten met politieke voorkeur

<b>Persoonsgegevens</b>	NAWTE + politieke voorkeur
<b>Grondslag</b>	Mondelinge toestemming, afgifte visitekaartje en/of via LinkedIn
<b>Verwerkingen</b>	Persoonlijke contacten en nieuwsvoorziening.
<b>Verwerkt door</b>	Afdeling communicatie, directie
<b>Bewaartermijn</b>	Gedurende de periode dat men contact heeft

Medewerkers

<b>Persoonsgegevens</b>	NAWTE + geboortedatum, kopie ID en bankgegevens
<b>Grondslag</b>	Arbeidsovereenkomst
<b>Verwerkingen</b>	Salariëring.
<b>Verwerkt door</b>	HRM-afdeling
<b>Bewaartermijn</b>	Gedurende de periode dat men een contract heeft

 Medewerkersfoto's op de website

<b>Persoonsgegevens</b>	Naam + foto
<b>Grondslag</b>	Aanvullende personeelsovereenkomst
<b>Verwerkingen</b>	Medewerkersfoto's op website.
<b>Verwerkt door</b>	Administratie, afdeling communicatie
<b>Bewaartermijn</b>	Gedurende de periode dat men een contract heeft

 Vrijwilligers

<b>Persoonsgegevens</b>	NAWTE
<b>Grondslag</b>	Vrijwilligersovereenkomst
<b>Verwerkingen</b>	Informatieverstrekking.
<b>Verwerkt door</b>	Afdeling communicatie, vakkennisafdelingen en/of relatie beheerder
<b>Bewaartermijn</b>	Gedurende de periode dat men een contract heeft

 Direct marketing (alleen bellen of papier)

<b>Persoonsgegevens</b>	NAWTE
<b>Grondslag</b>	Geen overeenkomst nodig
<b>Verwerkingen</b>	Toesturen van (of bellen over) informatie over de organisatie en/of producten/diensten.
<b>Verwerkt door</b>	Afdeling marketing/communicatie
<b>Bewaartermijn</b>	Gedurende de periode dat men gezien wordt als prospect voor de organisatie of haar diensten/producten

Digitale direct marketing (e-mail, facebook, LinkedIn, fax, SMS etc.)

<b>Persoonsgegevens</b>	NAWTE
<b>Grondslag</b>	Digitale toestemming vooraf, b.v. bij aanvragen van informatie of inschrijven voor een nieuwsbrief.
<b>Verwerkingen</b>	Digitaal toesturen van (of benaderen over) informatie over de organisatie en/of producten/diensten.
<b>Verwerkt door</b>	Afdeling marketing/communicatie
<b>Bewaartermijn</b>	Gedurende de periode dat men gezien wordt als prospect voor de organisatie of haar diensten/producten.

### 3.3 Beschrijving van extra doelbinding

Als je meer persoonsgegevens, verwerkingen en/of overeenkomsten hebt dan bij 3.1 beschreven, voeg deze dan hieronder toe. Voeg de extra beschrijving over doelen en doelbinding hieronder toe zodat we die kunnen opnemen in de AVG-verklaring.

**Toelichting:**

Van de ZZPers die worden ingehuurd, hierna genoemd: medebehandelaren, worden persoonsgegevens bewaard in de vorm van de facturen die ze zelf sturen. De facturen worden uitgeprint. Tevens wordt met een ZZPer een geheimhoudingsovereenkomst afgesloten en VOG is aangeleverd. Genoemde zaken worden bewaard in een dubbel afgesloten dossierkast. NI een afgesloten dossierkast in een apart afgesloten kast.

## 4.1 Privacy policy vindbaar, verwijzing in documenten

De privacy policy van de vereniging moet voor iedereen vindbaar zijn. Het eenvoudigste is om deze op de website van de vereniging te zetten en op elke pagina (onderaan) een link hier naar toe te leggen.

- Wij als organisatie hebben onze privacy policy zichtbaar gemaakt op onze website.
- Wij als organisatie hebben onze privacy policy niet vindbaar gemaakt op onze website.

### Beschrijf hieronder kort uw situatie:

ZONpraktijk hanteert de richtlijnen die verplicht zijn voor het voeren van een GGZ praktijk. Belangrijkste maatregelen zijn: mails met persoonsgegevens en/of vertrouwelijke gegevens worden beveiligd verstuurd via Zorgmail. Vertrouwelijke persoons- en clientgegevens, bijvoorbeeld medische gegevens worden verwerkt en opgeslagen in een goedgekeurd EPD. EPD en Zorgmail zijn aan elkaar verbonden. Technische informatie over de beveiliging is ook te vinden in de privacy policy. [www.zonpraktijk.nl](http://www.zonpraktijk.nl) voor privacy policy.

In alle overeenkomsten (documenten waarin persoonsgegevens gevraagd worden) moet een verwijzing staan naar de privacy policy.

- Wij als organisatie verwijzen in al onze documenten (contract, overeenkomst, aanmeldingsformulier, etc.) waarin persoonsgegevens staan naar onze privacy policy op de website van de organisatie.
- Wij als organisatie verwijzen in documenten (contract, overeenkomst, aanmeldingsformulier, etc.) waarin persoonsgegevens staan niet naar onze privacy policy op de website van de organisatie.

### Beschrijf hieronder kort uw situatie:

Alle formulieren die in de behandeling van cliënten gebruikt worden vallen onder de privacy policy zoals op de website vermeld. Op alle formulieren en documenten staat een verwijzing naar de privacy policy. [www.zonpraktijk.nl](http://www.zonpraktijk.nl) voor privacy policy.

## 5.1 Werken met verwerkersovereenkomst

Als organisatie mag je persoonsgegevens niet doorgeven aan een andere partij welke ten behoeve van jou persoonsgegevens verwerkt zonder een verwerkersovereenkomst. In een verwerkersovereenkomst spreek je af wat de ander met de gegevens mag doen én ook vooral wat niet.

- Wij als organisatie verklaren dat wij nooit persoonsgegevens doorgeven aan andere partijen waarmee we geen verwerkersovereenkomst hebben afgesloten als dit noodzakelijk is voor uitvoering van de doeleinden waarvoor we ze hebben gekregen.
- Wij als organisatie verklaren dat wij ook persoonsgegevens doorgeven aan andere partijen waarmee we geen verwerkersovereenkomst hebben afgesloten.
- Wij als organisatie verklaren dat wij geen persoonsgegevens doorgeven aan andere partijen.

### Beschrijf hieronder kort uw situatie:

Binnen ZONpraktijk zijn er 4 organisaties betrokken die indirect te maken hebben met het verwerken van de gegevens van cliënten. Dat zijn: de EPD provider, genaamd Intramed, VDP-automation die de website en mail beheert, de websitebouwer Jimdo en Zorgmail om mails beveiligd te kunnen versturen. Met deze betrokken partijen is vanuit ZONpraktijk een verwerkersovereenkomst afgesloten. Voor TVN zorgt, die gegevens van de cliënten onder de 18 jaar verwerken, geldt dat zij hoofdelijk aansprakelijk zijn voor eventuele datalekken en daarom hebben zij een opdracht- en verwerkersovereenkomst met ZONpraktijk afgesloten. De gegevens van cliënten onder de 18 jaar genieten bij ZONpraktijk dezelfde bescherming als volwassen cliënten via genoemd EPD, mail en Zorgmail.

## 6.1 Toegangsbeveiliging

Om zeker te weten dat alleen geautoriseerde personen de persoonsgegevens kunnen inzien en bewerken, moeten deze altijd beveiligd zijn met een wachtwoord en als het kan ook met een gebruikersnaam. Zo kun je een Excel-bestand beveiligen met een wachtwoord en een PC voorzien van een gebruikersnaam en een wachtwoord. Zorg er dus voor dat je altijd minimaal één keer een wachtwoord moet weten voordat je de persoonsgegevens van jouw organisatie kunt inzien of bewerken.

- Wij als organisatie hebben persoonsgegevens altijd opgeslagen achter de beveiliging van minimaal een gebruikersnaam en een wachtwoord.
- Wij als organisatie hebben persoonsgegevens niet altijd opgeslagen achter de beveiliging van minimaal een gebruikersnaam en een wachtwoord.
- Wij als organisatie hebben geen persoonsgegevens elektronisch opgeslagen en hebben daarom geen toegangsbeveiliging.

### Beschrijf hieronder kort uw situatie:

- Er is slechts 1 persoon, de praktijkhouder die toegang heeft tot de met een wachtwoord beveiligde pc met een eigen beveiligd netwerk (geen openbaar netwerk).
- Gewone email: beveiligd met wachtwoord.
- Beveiligde mail (Zorgmail): beveiligd met 2 traps beveiliging. Voldoet aan wettelijke eisen.
- Beveiligd EPD, online versie: beveiligd met 2 traps beveiliging. Voldoet aan de wettelijke eisen.
- Telefoon wordt door 1 persoon beheerd, praktijkhouder. Beveiligd middels vingerafdruk.
- De inhoudelijke informatie van ZZPers wordt gemaakt op een beveiligde PC, anoniem verstuurd via Zorgmail en door de praktijkhouder in het EPD toegevoegd.
- Dossierkast (met verwijzing huisarts, getekend behandelplan en eventueel externe rapportage per client) is afgesloten en staat in een extra afgesloten kast.
- PC ligt in de dossierkast.

## 7.1 Software en antivirussoftware up-to-date

Om systemen zo veilig mogelijk te laten zijn, moet je ze up-to-date houden. Dit doe je door het aanzetten van het automatisch ophalen en installeren van updates van de software. Zorg ook voor goede antivirussoftware. Zorg ervoor dat alle software ingesteld is op het automatisch ophalen en uitvoeren van updates. Maak goede afspraken met al je softwareleveranciers.

- Wij als organisatie hebben de persoonsgegevens alleen opgeslagen op computers/servers met beveiligingssoftware waarbij zowel de beveiligingssoftware als het besturingssysteem ingesteld zijn om automatisch updates op te halen en te installeren.
- Wij als organisatie hebben de persoonsgegevens niet alleen opgeslagen op computers/servers met beveiligingssoftware waarbij zowel de beveiligingssoftware als het besturingssysteem ingesteld zijn om automatisch updates op te halen en te installeren.
- Wij als organisatie hebben geen persoonsgegevens elektronisch opgeslagen en hebben daarom geen software updates.

### Beschrijf hieronder kort uw situatie:

Situatie tav beveiligingssoftware en besturingssysteem van de PC/server van de praktijk is zoals weergegeven in het aangevinkte punt.  
Na controle van het beveiligde Zorgmailadres van de praktijk op [www.internet.nl](http://www.internet.nl) komt naar voren dat deze voor 85% aan alle kwaliteitseisen voldoet. Een enkel verbeterpunt is naar de provider aangegeven.  
Na controle van de website naam en het gewone e-mailadres op [www.internet.nl](http://www.internet.nl) zijn een drietal verbeterpunten aangegeven die per medio okt 2022 zijn opgepakt door de hostingprovider.



## 8.1 Opslaan alleen binnen de EU

Binnen de EU is het niveau van gegevensbescherming gelijk. Dat komt omdat alle EU-lidstaten moeten voldoen aan de AVG. Als je persoonsgegevens verwerkt buiten de EU, bijvoorbeeld door deze te laten verwerken door een partij buiten de EU of er een passend beschermingsniveau bestaat voor dat land, bijvoorbeeld door een adequaatheidsbesluit van de Europese Commissie.

De wetgever is dus extra streng als je persoonsgegevens wilt verwerken/opslaan buiten de EU. Als je dat toch zou willen, dan moet er heel veel geregeld worden bovenop de normale AVG-verplichtingen. Dus check of je dienstverlener (drukker, verspreider, enz.) de toevertrouwde persoonsgegevens binnen de EU opslaat.

Het is dus het makkelijkste om persoonsgegevens alleen te verwerken binnen de EU, dit raden wij daarom ook sterk aan.

- Wij als organisatie verklaren dat wij nooit persoonsgegevens overdragen aan of opslaan bij partijen die gevestigd zijn buiten de EU.
- Wij als organisatie verklaren dat wij ook persoonsgegevens overdragen aan of opslaan bij partijen die gevestigd zijn buiten de EU.
- Wij als organisatie verklaren dat wij ook persoonsgegevens overdragen aan of opslaan bij partijen die gevestigd zijn buiten de EU. Wij hebben hiervoor de correcte maatregelen en overeenkomsten afgesloten. Onze situatie hebben wij hieronder beschreven.

### Beschrijf hieronder kort uw situatie:

Er wordt alleen samengewerkt met partijen die zijn gevestigd in Nederland.  
Er is een verwerkersovereenkomst met de provider van email en website en met de EPD leverancier. Daarin is opgenomen dat de data alleen binnen de EU mogen worden opgeslagen. Zij staan beiden garant voor gegevensbescherming door partners en derden.

## 9.1 Data back-up

Om de persoonsgegevens te beschermen tegen het verlies of diefstal moet je back-ups maken. Het is noodzakelijk om dat regelmatig te doen. Zorg ervoor dat deze back-up veilig wordt opgeborgen.

- Wij als organisatie hebben de opgeslagen persoonsgegevens beveiligd met een back-up.
- Wij als organisatie hebben de persoonsgegevens niet beveiligd met een back-up.
- Wij als organisatie hebben geen persoonsgegevens elektronisch opgeslagen en hebben daarom geen back-up.

### Beschrijf hieronder kort uw situatie:

Persoonsgegevens zijn opgeslagen in de online versie van het EPD van Intramed dat aan alle wettelijke voorwaarden voldoet. Er wordt automatisch een back up gemaakt van de opgeslagen gegevens in de beveiligde online omgeving.

## 10.1 Geautoriseerde medewerkers

Via autorisatie regel je wie binnen de organisatie welke persoonsgegevens mag verwerken.

- In onze organisatie hebben alleen geautoriseerde personen toegang tot de persoonsgegevens van de organisatie.
- In onze organisatie hebben ook niet geautoriseerde personen toegang tot de persoonsgegevens van de organisatie.

### Beschrijf hieronder kort uw situatie:

Alleen de praktijkhouder is geautoriseerd en heeft toegang tot de systemen met persoonsgegevens van cliënten, te weten: EPD en Zorgmail. De gewone email wordt ook beheerd door de praktijkhouder. De inhoudelijke rapportage van de 4 medebehandelaren wordt anoniem op een beveiligde pc gemaakt en door de regiebehandelaar I van Zon in het EPD verwerkt. Versturen van inhoudelijke rapportage gebeurt altijd zonder personalia van de betreffende client en via beveiligde Zorgmail. De volgende gegevens zijn opgeslagen van de 4 medebehandelaren: diploma/erkenning voor uit te voeren werkzaamheden, identiteitsbewijs, VOG en geheimhoudingsverklaring.

### Onderstaande vragen zijn alleen ter bewustwording en hoeven niet precies ingevuld te worden!

Wij als organisatie hebben 1 \_\_\_\_\_ personen geautoriseerd om de persoonsgegevens van de organisatie in te zien en te verwerken indien dit nodig is voor de uitoefening van hun functie. Wij als organisatie hebben van \_\_\_\_\_ personen de persoonsgegevens geregistreerd.

## 11.1 Vernietigen persoonsgegevens

Geef hieronder aan dat je organisatie alle persoonsgegevens vernietigt door bijvoorbeeld een regel te wissen in Excel en/of het versnipperen van een aanmeldingsformulier als er geen overeenkomst meer is.

Persoonsgegevens mogen niet langer worden bewaard dan voor verwezenlijking van de doeleinden waarvoor ze worden verwerkt. Dus: na beëindiging van een overeenkomst worden de persoonsgegevens van die persoon vernietigd. Wijs aan wie verantwoordelijk is voor het vernietigen van persoonsgegevens of de controle op de vernietiging.

**NB:** Verscheuren en weggooien is onvoldoende. Schaf daarom een versnipperaar aan.

**Let op:** In de financiële administratie mogen (of eigenlijk: moeten!) deze persoonsgegevens nog wel blijven staan, want daar geldt een (wettelijke) bewaarplicht van 7 jaar.

- Wij als organisatie verklaren dat wij alle persoonsgegevens vernietigen (na de bewaartermijn) als de overeenkomst op grond waarvan ze verkregen zijn verlopen is of de toestemming is ingetrokken.
- Wij als organisatie verklaren dat wij geen persoonsgegevens vernietigen als de overeenkomst op grond waarvan ze verkregen zijn verlopen is of de toestemming is ingetrokken.

### Beschrijf hieronder kort uw situatie:

De huidige wettelijke bewaartermijn van clientdossiers, opgeslagen in een beveiligd EPD, is 15 jaar. Ingaand na afloop van de behandeling. Daarbij gaat het over (gezondheid)gegevens die de praktijk zelf gegenereerd heeft en die direct verband houden met de zorg en ondersteuning van de client. Gegevens die verband houden met de financiële administratie worden 7 jaar bewaard conform de geldende richtlijn. Mails in de mailbox worden direct verwijderd na beantwoorden ervan of zn, indien van belang voor inhoudelijke dossiervorming, opgeslagen in het beveiligde EPD. Telefoonnummers in de mobiele praktijktelefoon worden 3 maanden na afsluiten van de behandeling verwijderd.

## 12.1 Toestemming voor direct marketing en bij minderjarigheid

### Bij direct marketing

De wetgever maakt onderscheid tussen gewone direct marketing (bellen en post sturen) of digitale marketing (via e-mail, fax, Facebook, LinkedIn of sms). Doordat gewone direct marketing een organisatie bij de verspreiding veel geld kost zal dat altijd beperkt blijven. Juist digitale marketing is nagenoeg gratis en kan daardoor heel veel toegepast worden met alle gevolgen van dien.

Op grond van de Telecommunicatiewet mag je bestaande klanten benaderen via digitale direct marketing zonder toestemming (maar met een opt-out).

- Wij als organisatie vragen vooraf altijd toestemming voordat we iemand benaderen via digitale direct marketing.
- Wij als organisatie vragen vooraf geen toestemming voordat we iemand benaderen via digitale direct marketing.
- Wij als organisatie maken geen gebruik van digitale direct marketing.

### Beschrijf hieronder kort uw situatie:

*Uw situatie:*

### Bij minderjarigheid (jonger dan 16 jaar)

Als je persoonsgegevens online verwerkt van personen jonger dan 16 jaar via bijvoorbeeld een app, online game, webwinkel of via sociale media, dan moet je daarvoor altijd schriftelijk/elektronisch een toestemming hebben van de ouder, verzorger of wettelijke vertegenwoordiger. Geef hieronder aan dat je organisatie dat ook altijd zo doet.

- Wij als organisatie verklaren dat wij alleen online persoonsgegevens van minderjarigen verwerken bijvoorbeeld een app, online game, webwinkel of via sociale media als daarvoor schriftelijke toestemming is gegeven door de ouder, verzorger of wettelijke vertegenwoordiger.
- Wij als organisatie verklaren dat wij persoonsgegevens van minderjarigen online verwerken bijvoorbeeld een app, online game, webwinkel of via sociale media zonder dat daarvoor schriftelijke toestemming is gegeven door de ouder, verzorger of wettelijke vertegenwoordiger.
- Wij als organisatie verklaren dat wij geen persoonsgegevens van minderjarigen online verwerken bijvoorbeeld een app, online game, webwinkel of via sociale media.

**Beschrijf hieronder kort uw situatie:**

Voor cliënten onder de 16 jaar geldt dat we handelen conform de richtlijn JeugdGGZ. Er wordt gewerkt met een behandelovereenkomst die door ouders ondertekend wordt en een apart behandelplan. De persoonsgegevens van de jongere en ouders staan in het beveiligde EPD en worden niet gebruikt voor marketing doeleinden. Er bestaan geen marketing doeleinden vanuit ZONpraktijk.

## 13.1 Papieren documenten en beveiliging

Als persoonsgegevens ook vastliggen op papier (denk aan contracten), dan moeten die papieren met persoonsgegevens achter slot en grendel zijn opgeslagen. Praktisch: bewaar dus alle papieren met persoonsgegevens in een kast die je steeds op slot doet. Alleen personen die voor hun werk voor de organisatie daarvoor toestemming hebben, mogen in die kast komen.

- Wij als organisatie hebben papieren documenten waarop de persoonsgegevens staan, opgeslagen achter slot en grendel.
- Wij als organisatie hebben niet alle papieren documenten waarop de persoonsgegevens staan, opgeslagen achter slot en grendel.
- Wij als organisatie hebben geen papieren documenten waarop de persoonsgegevens staan.

### Beschrijf hieronder kort uw situatie:

In principe bewaren we zoveel mogelijk gegevens in het beveiligde EPD. De zorgovereenkomsten en ondertekende behandelplannen van cliënten worden in een afgesloten dossierkast bewaard. De verwijzing van de huisarts is er veel sommige gevallen ook op papier en wordt dan ook in de dossierkast bewaard. Dat geldt ook voor externe rapportage (van andere organisaties) van sommige cliënten. Gegevens van medebehandelaren (zoals eerder aangegeven) worden in de afgesloten dossierkast bewaard. De praktijkhouder beheert de sleutel van de dossierkast.

## 14.1 Datalekken

Iedereen in de organisatie moet op de hoogte zijn wat een datalek is en wat je eraan moet doen. Geef aan wat voor jullie van toepassing is:

- Binnen onze organisatie is iedereen op de hoogte van wat een datalek is. Ook is bekend waar dit intern gemeld moet worden zodat wij als organisatie adequaat het datalek kunnen afhandelen en documenteren.
- Binnen onze organisatie is niet iedereen op de hoogte van wat een datalek is. Ook is niet bekend waar dit intern gemeld moet worden zodat wij als organisatie adequaat het datalek kunnen afhandelen en documenteren.

### **Beschrijf hieronder kort hoe jullie met datalekken omgaan:**

Wanneer er een datalek zou ontstaan dan wordt dat vastgelegd in het document datalekken van ZONpraktijk, zullen verbeterstappen afgesproken worden en zo nodig wordt datalek gemeld bij de Autoriteit Persoonsgegevens.



## 15.1 Medewerkers geïnstrueerd

Wij hebben onze medewerkers als volgt geïnstrueerd:

- Alle medewerkers hebben de video van de Stichting AVG bekeken.
- We hebben het onderwerp privacy bescherming in alle afdelingsoverleggen besproken.
- We hebben uitlegposters opgehangen.
- We hebben alle medewerkers een brief gestuurd met uitleg en instructie.
- We hebben met alle medewerkers een workshop over privacy bescherming gevolgd.
- We hebben een nieuwsbrief voor alle medewerkers waarin we regelmatig aandacht besteden aan privacy bescherming.
- Onze directeur/voorzitter heeft alle medewerkers opgeroepen extra aandacht te besteden aan privacy bescherming.

**Hieronder is ruimte om te beschrijven hoe jullie de medewerkers geïnstrueerd hebben:**

De praktijk eigenaar en de medebehandelaren zijn op de hoogte van de wet op de AVG en de implicaties die dat voor hen heeft. Ze werken allen ook op andere werkplekken binnen de (jeugd)GGZ en worden zo via meerdere kanalen geïnformeerd over het belang van bescherming van andermans privacy en de AVG.

## 16.3 Afronding

**Naam organisatie:**

ZONpraktijk

**Plaats:**

Haalderen

**Datum:**

27-2-2023

De AVG-verklaring is geen juridisch document maar een verklaring waarin je zelf verklaart dat je alle inspanningen hebt gepleegd om aan de Algemene Verordening Gegevensbescherming te voldoen.