



## AVG verklaring

Hierbij verklaart de Stichting AVG voor Verenigingen dat Sanimind v.o.f. het AVG-programma geheel of gedeeltelijk heeft doorlopen. Sanimind v.o.f. 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 Sanimind v.o.f. 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.

Sanimind v.o.f. begrijpt dat AVG-wetgeving continu van toepassing is en dat wij regelmatig de gegevens moeten controleren en updaten.

Met het volledig doorlopen van het AVG-programma van de Stichting AVG voor Verenigingen heeft Sanimind v.o.f. 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 Sanimind v.o.f. zijn te vinden op de volgende pagina('s) van deze verklaring.

Aldus opgemaakt te Gorinchem,

d.d. 29-8-2020,

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 Salarisgegevens worden niet gezien als bijzondere gegevens.

### Andere gewone persoonsgegevens:

### 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 Organisaties buiten de overheid mogen het BSN alleen gebruiken als dat wettelijk is bepaald. Dit geldt bijvoorbeeld voor werkgevers, zorgverleners, zoals huisartsen, apotheken en zorgverzekeraars. Ook in het onderwijs en kinderopvang wordt het BSN gebruikt.

### Aantekeningen bijzondere persoonsgegevens:

In het kader van medische diagnostiek en medische behandelingen kunnen de volgende bijzondere persoonsgegevens worden gebruikt: gegevens over gezondheid; gegevens over seksuele geaardheid; kopie identiteitsbewijs/paspoort; BSN.

In het kader van het uitvoeren van relatietherapie, gezinstherapie, mediation en/of coaching kunnen de volgende bijzondere persoonsgegevens worden gebruikt: gegevens over gezondheid; gegevens over seksuele geaardheid; kopie identiteitsbewijs/paspoort; BSN.

Specifiek in het kader van mediation (meestal maar niet uitsluitend mediation in opdracht van de rechtbank) kan gebruik gemaakt worden van strafrechtelijke gegevens of veroordelingen of daarmee verband houdende veiligheidsmaatregelen.

Genetische of biomedische gegevens met het oog op unieke identificatie: uit deze categorie wordt uitsluitend gebruik gemaakt van het maken van een aangezichtsfoto welke ter identificatie en controle in het medisch dossier wordt opgenomen.

## 3.1 Inventarisatie doelbinding.

### **Grondslag:**

Je moet een goede reden hebben om persoonsgegevens te mogen verwerken. De juridische naam voor die redenen is grondslagen. U heeft 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 u zich 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**

Persoonsgegevens: NAWTE.

Grondslag: Opdracht of contract.

Verwerkingen: Administratie, bevestiging, uitlevering.

Verwerkt door: Afdeling administratie, afdeling sales en afdeling inkoop.

Bewaartermijn: Gedurende de looptijd van de overeenkomst.

### **Beschrijf hieronder kort uw situatie:**

Sanimind levert op verzoek diensten aan klanten.

## 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!

Persoonsgegevens: NAWTE + BSN.

Grondslag: Overeenkomst met handtekening op papier.

Verwerkingen: Interactie met de overheid in het belang van (en met toestemming van) de klant.

Verwerkt door: Afdeling administratie.

Bewaartermijn: Gedurende de looptijd van de overeenkomst.

### **Beschrijf hieronder kort uw situatie:**

Bij Sanimind wordt medische diagnostiek en worden medische behandelingen verricht. Daarnaast worden psychologische/psychotherapeutische behandelingen verricht. Ook worden er activiteiten verricht in het kader van mediation en coaching. Voor een aantal van deze activiteiten en verrichtingen is het nodig en verplicht om bijzondere persoonlijke gegevens te verzamelen, zoals BSN.

De bewaartermijn is óf zolang de overeenkomst/behandeling/traject loopt óf gedurende de tijd die wettelijk wordt voorgeschreven.

## 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.

Persoonsgegevens: NAWTE + bankgegevens + kentekengegevens.

Grondslag: Akte van splitsing en het reglement ex artikel 5:112 BW.

Verwerkingen: Beheeractiviteiten van de VvE in de breedste zin van het woord in het belang van( en met toestemming van) de (gezamenlijke) eigenaars.

Verwerkt door: Bestuur en beheerder.

Bewaartermijn: Gedurende lidmaatschap of gebruik en 12 maanden daarna en voorts alleen in de financiële administratie voor maximaal 7 jaar.

### **Beschrijf hieronder kort uw situatie:**

## Aanmelden voor nieuwsbrief

Persoonsgegevens: Naam en e-mailadres.

Grondslag: Aanmelding voor nieuwsbrief (formulier op de website).

Verwerkingen: Informatie verstrekking in de vorm van nieuwsbrieven.

Verwerkt door: Afdeling communicatie.

Bewaartermijn: Gedurende de periode dat men aangemeld is.

### **Beschrijf hieronder kort uw situatie:**

Patiënten en cliënten kunnen zich aanmelden als patiënt of cliënt middels een aanmeldingsformulier. Hierbij worden persoonsgegevens, gegevens over gezinssituatie en werksituatie, evenals gezondheidsgegevens verzameld en opgeslagen. Deze gegevens worden via beveiligd systeem (FormDesk) verstuurd. De elektronisch ingevulde gegevens worden vervolgens middels een met wachtwoord beschermd formulier naar Sanimind verzonden.

De bewaartermijn is óf zolang de overeenkomst/behandeling/traject loopt óf gedurende de tijd die wettelijk wordt voorgeschreven.

**Prospect, stakeholder-/lobbycontacten en geïnteresseerde**

Persoonsgegevens: NAWTE.

Grondslag: Mondelinge toestemming, afgifte visitekaartje en/of via LinkedIn.

Verwerkingen: Informatieverstrekking in de vorm van nieuwsbrieven of gerichte contacten.

Verwerkt door: Afdeling communicatie, directie, vakkennisafdelingen en/of relatie beheerder.

Bewaartermijn: Gedurende de periode dat men contact heeft.

**Beschrijf hieronder kort uw situatie:**

**Stakeholder-/lobbycontacten met politieke voorkeur**

Persoonsgegevens: NAWTE + politieke voorkeur.

Grondslag: Mondelinge toestemming, afgifte visitekaartje en/of via LinkedIn.

Verwerkingen: Persoonlijke contacten en nieuwsvoorziening.

Verwerkt door: Afdeling communicatie, directie.

Bewaartermijn: Gedurende de periode dat men contact heeft.

**Beschrijf hieronder kort uw situatie:**

**Medewerkers**

Persoonsgegevens: NAWTE + geboortedatum, kopie ID en bankgegevens.

Grondslag: Arbeidsovereenkomst.

Verwerkingen: Salariëring.

Verwerkt door: HRM-afdeling.

Bewaartermijn: Gedurende de periode dat men een contract heeft.

**Beschrijf hieronder kort uw situatie:**

**Medewerkersfoto's op de website**

Persoonsgegevens: Naam + foto.

Grondslag: Aanvullende personeelsovereenkomst.

Verwerkingen: Medewerkersfoto's op website.

Verwerkt door: Administratie, afdeling communicatie.

Bewaartermijn: Gedurende de periode dat men een contract heeft.

**Beschrijf hieronder kort uw situatie:**

Op dit moment staat op onze website de foto's van de 2 eigenaren/behandelaren van Sanimind.

**Vrijwilligers**

Persoonsgegevens: NAWTE.

Grondslag: Vrijwilligersovereenkomst.

Verwerkingen: Informatieverstrekking.

Verwerkt door: Afdeling communicatie, vakkennisafdelingen en/of relatie beheerder.

Bewaartermijn: Gedurende de periode dat men een contract heeft.

**Beschrijf hieronder kort uw situatie:**

**Direct marketing (alleen bellen of papier)**

Persoonsgegevens: NAWTE.

Grondslag: Geen overeenkomst nodig.

Verwerkingen: Toesturen van (of bellen over) informatie over de organisatie en/of producten/diensten.

Verwerkt door: Afdeling marketing/communicatie.

Bewaartermijn: Gedurende de periode dat men gezien wordt als prospect voor de organisatie of haar diensten/producten.

**Beschrijf hieronder kort uw situatie:**

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

Persoonsgegevens: NAWTE.

Grondslag: Digitale toestemming vooraf, b.v. bij aanvragen van informatie of inschrijven voor een nieuwsbrief.

Verwerkingen: Digitaal toesturen van (of benaderen over) informatie over de organisatie en/of producten/diensten.

Verwerkt door: Afdeling marketing/communicatie.

Bewaartermijn: Gedurende de periode dat men gezien wordt als prospect voor de organisatie of haar diensten/producten.

**Beschrijf hieronder kort uw situatie:**

### 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.

Doel of soort overeenkomst: medische diagnostiek; medische behandeling; psychologische/psychotherapeutische behandeling.

Persoonsgegevens: NAWTE + BSN.

Grondslag: Overeenkomst met handtekening op papier of overeenkomst op grond van de WGBO.

Verwerkingen: Interactie in het belang van de patiënt en/of cliënt.

Verwerkt door: PMAW de Groodt en/of A. de Groodt Achterkamp.

Bewaartermijn: Gedurende de looptijd van de overeenkomst/behandeling of waar van toepassing volgens wettelijke eisen.

Toelichting

Aanmeldingsformulier:

Patiënten en cliënten kunnen zich aanmelden als patiënt of cliënt middels een aanmeldingsformulier.

Hierbij worden persoonsgegevens, gegevens over gezinssituatie en werksituatie, evenals gezondheidsgegevens verzameld en opgeslagen.

Deze gegevens worden via beveiligd systeem (FormDesk) verstuurd. De elektronisch ingevulde gegevens worden vervolgens middels een met wachtwoord beschermd formulier naar Sanimind verzonden.

## 4.1 Privacy policy vindbaar, verwijzing in documenten.

De privacy policy van de organisatie moet voor iedereen waarvan je persoonsgegevens verwerkt vindbaar zijn. Het eenvoudigste is om deze op de website van de organisatie te zetten en op elke pagina (onderaan) een link hier naartoe 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:**

De Privacy Policy is vindbaar op <https://www.sanimind.eu>. Op elke pagina is een link geplaatst naar de Privacy Policy. De Privacy Policy van Sanimind is vanaf de website van Sanimind te downloaden.

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:**

In elk document wordt verwezen naar de Privacy Policy. Daar waar mogelijk (in elektronische documenten) ook via een aanklikbare link naar de Privacy Policy op de website van Sanimind alwaar de Privacy Policy van Sanimind ook te downloaden is.



## 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:**

Sanimind heeft met zo veel mogelijk verwerkers van persoonsgegevens waarmee Sanimind samenwerkt en/of diensten aan levert en/of diensten van ontvangt een verwerkersovereenkomst gesloten. Deze verwerkersovereenkomsten worden, indien aangeleverd, digitaal door Sanimind opgeslagen in een veilige omgeving.

## 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:**

De door Sanimind verzamelde persoonsgegevens zijn beschermd doordat alle systemen waarvan Sanimind gebruik maakt zijn beveiligd met inlognamen en wachtwoorden.

De meeste persoonsgegevens worden verzameld in het Electronisch Patiënten Dossier (EPD) van de leverancier Medicore. Al deze gegevens worden niet op lokale systemen van Sanimind opgeslagen maar op systemen bij Medicore. Medicore voldoet aan de eisen van ISO 27001 / NEN 7510. Dat garandeert goede beveiliging. Toegang tot het EPD is alleen toegestaan door omschreven gebruikers en dan met inlognaam en wachtwoord.

De persoonsgegevens die door derden worden verzameld ten behoeve van dienstverlening aan Sanimind zijn op een zelfde wijze beveiligd als bij het EPD. De derden organisaties zijn ook voldoende gecertificeerd.

Er zijn binnen Sanimind ook persoonsgegevens verzameld binnen papieren dossiers (zo weinig mogelijk). Deze persoonsgegevens worden opgeslagen en bewaard in een met code beveiligde kluis waarbij de code alleen bekend is bij de twee eigenaren/behandelaren van Sanimind.

De systemen waarmee binnen Sanimind wordt gewerkt (computers, PC's, tablets en smartphones) zijn allen met wachtwoord/code beveiligd en gaan bij inactiviteit binnen enkele minuten (maximaal 10) over op een screensaver. Opnieuw activeren van dat apparaat kan dan alleen met een wachtwoord.

De door Sanimind gebruikte elektronische mappen, zowel op de gebruikte systemen als in de cloud, worden beveiligd met wachtwoord en/of code. Datzelfde wordt ook daar waar mogelijk gedaan met individuele bestanden.

Het emailverkeer vanuit Sanimind wordt indien er persoonsgegevens worden gebruikt via beveiligde email gedaan (Zorgmail).

Binnenkomende email is vaak niet beveiligd aangezien deze in merendeel afkomstig is van patiënten/cliënten/belangstellende van Sanimind.

De website van Sanimind is beveiligd via het HTTPS protocol. Er is een beveiligings servercertificaat geïnstalleerd. Er is sprake van het zogenaamde 'groene slotje'.

De wifi omgeving van Sanimind is beveiligd middels wachtwoord. Er is een gastnetwerk, wat separaat is geïnstalleerd van het door Sanimind gebruikte wifi netwerk. Toegang tot de door Sanimind gebruikte router is beveiligd via inlognaam en wachtwoord.

## 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:**

Het merendeel van de verzamelde persoonsgegevens worden door derden bewaard en opgeslagen. Deze derden zijn allen gekwalificeerd om deze gegevens te mogen en kunnen opslaan. Er is gezorgd voor backups en voor toegangsbeveiliging middels autorisaties, inlognamen en wachtwoorden. Er wordt derhalve nauwelijks persoonsinformatie bewaard op de door Sanimind gebruikte systemen.

Voor alle veiligheid zijn de systemen van Sanimind allen beveiligd middels inlognamen en wachtwoorden, is er beveiliging van mappen en zo mogelijk bestanden waarin persoonsgegevens aanwezig zijn middels wachtwoord/codes. Er is antivirus software geïnstalleerd waar mogelijk en er is automatisch ingesteld dat de gebruikte software, antivirus software en besturingssysteem up to date blijft (automatische download en installatie van updates).

## 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.

**Beschrijf hieronder kort uw situatie:**

Er zijn voorzover bij Sanimind bekend geen relaties tussen organisatie/verwerkers buiten de EU en persoonsgegevens die Sanimind heeft verzameld en/of opgeslagen.

## 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:**

De meeste verzamelde en bewaarde persoonsgegevens worden bewaard en opgeslagen door gecertificeerde derden. Deze maken automatisch versleutelde backups.

Van de op de systemen van Sanimind aanwezige mappen en documenten die persoonsgegevens bevatten worden regelmatig in de cloud backups gemaakt. Deze backups zijn ook daar waar mogelijk middels wachtwoord/code beveiligd.

## 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 hoe jullie de autorisatie geregeld hebben:**

Beide behandelaren van Sanimind zijn geautoriseerd in het verwerken van persoonsgegevens. Zij hebben beiden aparte wachtwoorden en inlogcodes.  
De geheimhouding is middels een geheimhoudingsverklaring vastgelegd.

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

Wij als organisatie hebben 2 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 2 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:**

Sanimind houdt zich aan de voor haar gestelde regels en wettelijke eisen. Indien geen sprake is van een behandeling of overeenkomst binnen de WGBO worden de gegevens na afloop van de overeenkomst of bij verzoek tot vernietiging verwijderd. Voor overeenkomsten en behandelingen die binnen de sfeer van de WGBO vallen gelden wettelijke eisen met betrekking tot bewaartermijn. Sanimind houdt zich aan deze wettelijke termijnen. Ook handelt Sanimind conform de gestelde eisen als er een verzoek komt tot vernietiging van gegevens bij overeenkomsten en behandelingen vallend onder de WGBO.

## 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:**

Sanimind maakt geen gebruik van direct marketing. Dat past niet binnen de aard van onze bedrijfsvoering.

### 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:**

Sanimind behandelt in het kader van een medische diagnosticering en/of medische behandeling geen personen onder de leeftijd van 18 jaar. Er worden derhalve geen persoonsgegevens verzameld van patiënten onder de 18 jaar als het gaat om een medische diagnosticering en/of medische behandeling.

Sanimind behandelt/begeleidt wél personen onder de leeftijd van 16 jaar in het kader van gezinstherapie/systeemtherapie en indien voorkomend ook in het kader van mediation en/of coaching. Deze behandelingen/begeleidingen vinden altijd plaats nadat daar schriftelijk toestemming voor is gegeven door ouders c.q. voogden c.q. wettelijke vertegenwoordigers van deze personen onder de leeftijd van 16 jaar.



## 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:**

Sanimind heeft geen patiëntgegevens op papier. Alle persoonsgegevens van patiënten worden elektronisch bewaard en opgeslagen, waarbij de dataveiligheid daarvan gewaarborgd is.

Sanimind heeft wél papieren documenten van cliënten (dus voor relatie/systeemtherapie, mediation, coaching), alhoewel die papieren gegevens zo veel mogelijk worden beperkt. Deze papieren gegevens worden óf in een met code afgeschermd kluis bewaard waarvan alleen geautoriseerden de code hebben, óf ze worden bewaard in afsluitbare archiefkasten die in ruimten staan die zijn afgesloten. De betreffende sleutels zijn alleen in handen van de geautoriseerden bij Sanimind.

## 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:**

Sanimind heeft aan de behandelaren duidelijk gemaakt wat een data lek is en hoe daarmee moet worden omgegaan. Duidelijk is gemaakt dat een data lek altijd moet worden gemeld aan de verwerkersverantwoordelijke bij Sanimind. Dat is mw A. de Groot-Achterkamp.

Bij Sanimind wordt niet gewerkt met externe datadragers zoals USB sticks, externe harddisks waarop persoonsgegevens worden gezet. Er wordt wel, sporadisch, gebruik gemaakt van video opnames van sessies of delen van sessies. Deze opnames komen tijdelijk terecht op een geheugenkaart maar worden zsm overgezet naar een laptop van Sanimind, waarna de gegevens op de geheugenkaart worden gewist.

Het maken van opnames gebeurt altijd pas na schriftelijke toestemming van degenen die worden opgenomen. In het toestemmingsformulier wordt duidelijk aangegeven wat het doel is van de opname, wat er met de opnames kan gebeuren en hoe er mee wordt omgegaan.

De opnames worden zodra dat mogelijk is gewist/vernietigd.

Er is toezicht op de geheugenkaart zolang daar gegevens op staan.

## 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:**

Sanimind heeft 2 eigenaren/behandelaren die de elkaar op de hoogte hebben gebracht van de AVG en die onderling de benodigde veranderingen uitgevoerd en besproken hebben. De gehele procedure om aan de AVG richtlijnen en eisen te voldoen hebben zij samen gedaan en uitgevoerd waardoor zij goed op de hoogte zijn van de eisen en de strekking van de AVG. Zij houden periodiek overleg met elkaar over de AVG en de effecten daarvan op de organisatie en de bedrijfsvoering.

## 16.3 Afronding.

Naam organisatie:	Sanimind
Plaats:	Uden
Datum:	29-8-2020

De AVG-verklaring is een automatische samenvatting van alle vragen en antwoorden in het stappenplan. 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. Wij zien in de praktijk dat sommige gebruikers de AVG-verklaring regelmatig opvragen en gebruiken als een todo lijst. Je kunt de AVG-verklaring zo vaak opvragen als je wilt.