AVG verklaring

Hierbij verklaart de Stichting AVG voor Verenigingen dat Psychologenpraktijk `De Reiziger' het AVG-programma geheel of gedeeltelijk heeft doorlopen. Psychologenpraktijk `De Reiziger' 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 Psychologenpraktijk `De Reiziger' 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.

Psychologenpraktijk `De Reiziger' 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 Psychologenpraktijk `De Reiziger' 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 Psychologenpraktijk `De Reiziger' zijn te vinden op de volgende pagina('s) van deze verklaring.

Aldus opgemaakt te Gorinchem,

d.d. 23-5-2018,

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

- [x] Naam/ voorletters/ tussenvoegsel
- [ ] Titels
- [x] Adres
- [x] Postcode
- [x] Plaats
- [ ] Provincie
- [x] Land
- [x] Woonplaats
- [x] Telefoonnummer
- [x] Faxnummer
- [x] E-mailadres
- [ ] Website
- [x] Geslacht
- [x] Geboortedatum
- [ ] Geboorteplaats
- [x] Overlijdensdatum
- [x] Burgerlijke staat
- [ ] LinkedIn
- [ ] Facebook
- [ ] Twitter
- [x] Werkzaam bij organisatie
- [x] Bankrekeningnummer
- [ ] Inloggegevens (gebruikersnaam/wachtwoord)
- [ ] Voertuig kentekenplaat
- [ ] Salarisgegevens Salarisgegevens worden niet gezien als bijzondere gegevens.

Andere gewone persoonsgegevens:

- Naam zorgverzekering en polisnummer
- Gegevens huisarts (adres, telefoonnummer, AGB-

Bijzondere persoonsgegevens

- [x] Etnische afkomst
- [x] Politieke opvattingen of voorkeur
- [x] Religieuze opvatting of overtuiging
- [ ] Lidmaatschap van een vakbond
- [ ] Genetische of biometrische gegevens met het oog op unieke identificatie
- [x] Gegevens over gezondheid
- [x] Gegevens over seksuele geaardheid
- [x] Strafrechtelijke gegevens of veroordelingen of daarmee verband houdende veiligheidsmaatregelen
- [ ] Kopie identiteitsbewijs/paspoort, zonder voorlegger gekopieerd
- [x] BSN-nummer Organisaties buiten de overheid mogen het BSN alleen gebruiken als dat wettelijk is bepaald. Dit geldt bijvoorbeeld voor zorgverleners, zoals huisartsen, apotheken en zorgverzekeraars. Ook in het onderwijs en kinderopvang wordt het BSN gebruikt.

Aantekeningen bijzondere persoonsgegevens:

Bovenstaande gegevens alsmede de algemene gegevens (hiernaast) worden verzameld in het kader van de Wet Geneeskundige Behandelovereenkomst (WGBO) en Wet Beroepen In de Gezondheidszorg (Wet B.I.G.) en dienen ter uitvoering van mijn zorgtaak als GZ-psycholoog.

code)
- Gegevens verwijzer (adres, telefoonnummer, AGB-code)
- Gegevens opdrachtgevers (namen, adres, telefoonnummer, AGB-code, bankrekeningnummer, factuurgegevens)
- Gegevens verhuurder praktijkruimte (naam, adres, telefoonnummer, KvK-nummer, B.I.G.-registratienummer, bankrekeningnummer, BTW-nummer)
- Na(a)m(en) contactperso(o)n(en)
- E-mailadres contactperso(o)n(en)
- Telefoonnummer contactperso(o)n(en)
- Type relatie met contactperso(o)n(en)
- Leeftijden en beroep/opleiding personen uit gezin van herkomst
- Overlijdensjaar personen uit gezin van herkomst/huidige gezin
- Leeftijden en beroep/opleiding personen uit huidige gezin
- Naam, type relatie (bijvoorbeeld vriend) en woonplaats huidige belangrijke personen
- Gegevens genoten opleiding(en): periode waarin de opleiding plaatsvond, type/niveau opleiding, wel of geen diploma
- Gegevens werkcarrière: naam werkgever, functie, periode waarin de persoon daar werkzaam was, reden beëindiging contract
- Waaruit de persoon inkomsten ontvangt: loondienst, zelfstandig, (type) uitkering
- Hoogte van eventuele schulden en of er een afbetalingsregeling bestaat

3.1 Inventarisatie doelbinding.

Welke persoonsgegevens verwerk je, met welk doel en heb je ze daar ook voor gekregen? Dat noemen we ‘doelbinding’. Het is belangrijk dat je persoonsgegevens alleen verwerkt (dus opslaat en gebruikt) voor de doeleinden waarvoor je deze hebt verkregen.
Voor de inventarisatie van de vormen van doelbinding binnen de onderneming 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 onderneming nog andere doelbindingen voor, dan kun je deze in de open vorm noteren bij 3.3.

Grondslag: Grondslag is een reden op basis waarvan je de persoonsgegevens mag verwerken. Een reden kan zijn een verkregen toestemming (b.v. het krijgen van een visitekaartje of een inschrijving voor een nieuwsbrief). Een reden kan ook zijn dat je deze persoonsgegevens nodig hebt voor het uitvoeren van een overeenkomst (b.v. een koopcontract of een lidmaatschapsovereenkomst).

LET OP: Het is verstandig zo min mogelijk persoonsgegevens te hanteren. 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:

☐ **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 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:

☐ **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.
Overeenkomst:	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:

☐ **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:

☐ **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: Leveren van psychologische zorg in het kader van de WGBO en wet BIG
Persoonsgegevens: NAWTE+BSN+geboortedatum+ alle relevante gegevens die een goede inschatting van de gezondheid mogelijk maken (waaronder ook contextuele informatie: o.a. religie, ethniciteit, gezin van herkomst, gezinssamenstelling, opleiding, werkcarrière, aanwezigheid schulden, burgerlijke staat).
Grondslag: Het stellen van een diagnose en het verstrekken van psychologische behandelingen op grond van de Wet op de Geneeskundige Behandelovereenkomst (WGBO) en de Wet Individuele beroepen in de Gezondheidszorg (Wet BIG).
Verwerkingen: Openen en bewerken van een Electronisch Patiëntendossier (EPD), correspondentie met verwijzer/huisarts, declaratie van zorgtraject
Verwerkt door: Zorgverlener
Bewaartermijn: minimaal 10 jaar
Toelichting: Voor de uitoefening van mijn taak als zorgverlener (GZ-psycholoog) zijn deze gegevens noodzakelijk om een Electronisch Patiëntendossier (EPD) te openen en alle gegevens die betrekking hebben op de levering (en financiële afhandeling) van zorg ten behoeve van mijn patiënten te kunnen verwerken.

Doel of soort overeenkomst: Supervisie geven
Persoonsgegevens: NAWTE (uitsluitend van de supervisant)+ alle relevante gegevens die een goede inschatting van de gezondheid van de ingebrachte casuïstiek mogelijk maken (waaronder ook contextuele informatie: o.a. religie, ethniciteit, gezin van herkomst, gezinssamenstelling, opleiding, werkcarrière, aanwezigheid schulden, burgerlijke staat).
Grondslag: Het superviseren van het stellen van een juiste diagnose en van het verstrekken van adequate psychologische behandelingen op grond van de Wet op de Geneeskundige Behandelovereenkomst (WGBO) en de Wet Individuele beroepen in de Gezondheidszorg (Wet BIG).
Verwerkingen: Opstellen van een supervisiecontract, beoordelen en bewaren van casusconceptualisaties op een beveiligde computer. evalueren van de supervisies, van supervisanten aan de hand van praktijktoetsen, mailcontact/telefonisch contact met de supervisant, verslaglegging van supervisiesessies
Verwerkt door: Supervisor (zorgverlener)
Bewaartermijn: Gedurende de duur van de periode van het supervisiecontract
Toelichting: In de rol van supervisor is het niet noodzakelijk om te kunnen herleiden wie de patiënten zijn die worden ingebracht. De ingebrachte privacygevoelige informatie (waaronder ook ethniciteit, religie, of er sprake is van een strafblad, en alle relevante gegevens die betrekking hebben op de gezondheidssituatie van de betreffende patiënt) is noodzakelijk om de supervisant professioneel en adequaat te kunnen superviseren.

4.1 Privacy policy vindbaar, verwijzing in documenten.

De privacy policy van de organisatie moet voor iedereen 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.

- [x] 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 te raadplegen op de website

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

- [x] 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 alle correspondentietemplates (behandelovereenkomst, brieven aan verwijzer, brieven aan derden) wordt verwezen naar de privacy policy.

5.1 Werken met verwerkersovereenkomst.

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

- [x] 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:

Praktijk `De Reiziger' maakt gebruik van een webbased Elektronisch Patiëntendossier: Epos van Zilos ZGP Services. Daarnaast is Praktijk `De Reiziger' verplicht vragenlijsten in het kader van Routine Outcome Monitoring (ROM) te verwerken via Telepsy. Met beide organisaties is een verwerkersovereenkomst afgesloten. Daarnaast kunnen nieuwe patiënten zich aanmelden via de website. Met de webhost (Webreus) wordt nog een verwerkersovereenkomst aangegaan.

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.

- [x] 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:

Ik ben de enige medewerker in deze organisatie en ben gebonden aan geheimhoudingsplicht in het kader van de WGBO en de Wet BIG.
De Wachtwoorden van de PC, laptop en ook van het Elektronisch Patiënten Dossier (EPD) worden eens per drie maanden gewijzigd;
- Praktijk `De Reiziger' is gebonden aan zijn beroepsgeheim op grond van de Wet op de Geneeskundige Behandelovereenkomst (WGBO) en de wet Beroepen in de Individuele Gezondheidszorg (wet BIG)
- Alle personen (derden) die namens Praktijk `De Reiziger’ van uw gegevens kennis kunnen nemen, zijn gehouden aan geheimhouding daarvan.
- Praktijk `De Reiziger’ anonimiseert/pseudonimiseert en zorgt voor de encryptie van persoonsgegevens als daar aanleiding toe is;
- Praktijk `De Reiziger’ maakt (Bitlocker encrypted) back-ups van de persoonsgegevens om deze te kunnen herstellen bij fysieke of technische incidenten;
- Automatische schermblokkering na drie minuten van inactiviteit op alle beeldschermen;
- Beeldschermvergrendeling wordt aangezet wanneer de ruimte verlaten wordt terwijl er een derde in de ruimte aanwezig is waar de te verwerken en verwerkte persoonsgegevens zich bevinden;
- De ruimte waarin persoonsgegevens verwerkt worden, wordt afgesloten nadat deze verlaten wordt;
- Praktijk `De Reiziger’ test en evalueert regelmatig de genomen maatregelen;

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.

- [x] 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:

Praktijk `De Reiziger' maakt gebruik van Windows 10 Pro en van Microsoft Office voor de verwerking van alle gegevens op alle computers. De website is gecertificeerd en veilig (https-verbinding).

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 een internationale organisatie, moet je kijken of er een adequaatheidsbesluit van de Europese Commissie bestaat. Je moet ook weten en kunnen aantonen dat er passende of geschikte waarborgen zijn, en hoe er een kopie van kan worden verkregen of waar ze kunnen worden geraadpleegd.

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.

- [x] 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:

Praktijk `De Reiziger' is uitsluitend actief binnen Nederland en werkt uitsluitend samen met verwerkers van persoonsgegevens die in Nederland gegevens opslaan. Met alle verwerkers is een verwerkersovereenkomst afgesloten.

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.

- [x] 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:

Back-ups worden vooralsnog gemaakt op een externe harde schijf die wordt beveiligd met een Bitlockerencryptie en wachtwoord. De harde schijf wordt opgeborgen in een afgesloten kast in een afgesloten ruimte.

10.1 Geautoriseerde medewerkers.

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

- [x] 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:

Praktijk `De Reiziger' is een eenmanszaak. Dhr. T. van der Lee is de enige persoon binnen het bedrijf die toegang heeft tot de persoonsgegevens die verwerkt worden door Praktijk `De Reiziger'

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 in 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.

- [x] Wij als organisatie verklaren dat wij alle persoonsgegevens vernietigen 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:

Op grond van de WGBO ben ik gehouden aan een bewaartermijn van 15 jaar voor gegevens van de patiënten die ik behandel. Daarna worden de gegevens vernietigd tenzij de persoon uitdrukkelijk (schriftelijk) heeft aangegeven dat de gegevens langer bewaard dienen te worden. Voor supervisanten geldt een bewaartermijn die overeenkomt met de looptijd van het supervisiecontract.

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 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.

- [x] Wij als organisatie vragen vooraf altijd toestemming voordat we iemand benaderen via digitale direct markering.

- [ ] Wij als organisatie vragen vooraf geen toestemming voordat we iemand benaderen via digitale direct markering.

- [ ] Wij als organisatie maken geen gebruik van digitale direct markering.

Beschrijf hieronder kort uw situatie:

Bij praktijk `De Reiziger' wordt het eerste contact doorgaans gelegd door de patiënt zelf door middel van een e-mail (al dan niet via de website) of telefonisch contact. Met de provider voor de website is een verwerkersovereenkomst aangegaan en de website is beveiligd (https). In mijn eerste antwoordmail na een aanmelding staat onderstaande tekst waarin toestemming gevraagd wordt voor contact en desgewenst uitwisseling van (persoons)gegevens per e-mail en/of SMS.

Geachte/beste

BELANGRIJK! Lees svp eerst onderstaande informatie goed door alvorens een antwoord op deze mail te sturen!

Praktijk `De Reiziger' hecht veel waarde aan de bescherming van uw persoonsgegevens. Praktijk `De Reiziger' doet er daarom alles aan om uw privacy te waarborgen en gaat daarom zorgvuldig om met uw persoonsgegevens. Praktijk `De Reiziger' houdt zich aan de toepasselijke wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming.

Om (tot u als persoon herleidbare) gegevens te kunnen/mogen uitwisselen via e-mail en/of SMS is uw expliciete toestemming een vereiste. Wilt u hieronder aangeven via welke media wij contact met elkaar mogen hebben om een zo goed mogelijke samenwerking te kunnen bespoedigen?

☐ e-mail
☐ SMS

Bij minderjarigheid (jonger dan 16 jaar).

Als je persoonsgegevens hebt van personen jonger dan 16 jaar, dan moet je daarvoor altijd schriftelijk een handtekening (op papier!) voor akkoord hebben van de ouder, verzorger of wettelijke vertegenwoordiger. Geef hieronder aan dat je organisatie dat ook altijd zo doet.

- [x] Wij als organisatie verklaren dat wij alleen persoonsgegevens van minderjarigen verwerken als daarvoor schriftelijke toestemming is gegeven door de ouder, verzorger of wettelijke vertegenwoordiger.

- [ ] Wij als organisatie verklaren dat wij persoonsgegevens van minderjarigen verwerken zonder dat daarvoor schriftelijke toestemming is gegeven door de ouder, verzorger of wettelijke vertegenwoordiger.

- [ ] Wij als organisatie verklaren dat wij geen persoonsgegevens van minderjarigen verwerken.

Beschrijf hieronder kort uw situatie:

Praktijk `De Reiziger' verwerkt in principe geen persoonsgegevens van minderjarigen, omdat de doelgroep patiënten en supervisanten vanaf 18 jaar betreft.

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.

- [x] 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:

Ik maak, naast een Elektronisch Patiënten Dossier (EPD) ook een papieren dossier aan. Deze dossiers bewaar ik in een afgesloten dossierkast. De sleutel is in beheer van mij als vertegenwoordiger van mijn praktijk.

14.1 Datalekken.

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

- [x] 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:

Als er een datalek kan worden vastgesteld, zal in een standaarddocument worden vastgelegd wanneer het datalek (vermoedelijk) heeft plaatsgevonden, wanneer het is ontdekt en om welk datalek het gaat. Tevens zal worden vastgelegd of de Autoriteit Persoonsgegevens is geïnformeerd of niet en om welke reden dit (niet) gedaan is.

15.1 Medewerkers geïnstrueerd

Wij hebben onze medewerkers als volgt geïnstrueerd:

- [x] Alle medewerkers hebben de video van de Stichting AVG bekeken.
- [ ] We hebben het onderwerp privacy bescherming in alle afdelingsoverleggen besproken.
- [x] 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.
- [x] 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:

Ik ben de enige medewerker van Praktijk `De Reiziger'. Derhalve ben ik degene die het AVG-programma heeft doorgevoerd en alle instructie en uitleg heeft opgezocht en verwerkt in mijn handelen in en namens de praktijk . Ik ben van plan de instructies/video's met enige regelmaat te herhalen opdat ik scherp blijf in mijn handelen.

16.3 Ondertekening.

Met het inzenden van dit stappenplan verklaar ik hierbij dat ik naar eer en geweten dit stappenplan heb ingevuld namens de organisatie.
Aldus verklaard door:

Naam organisatie:	Psychologenpraktijk `De Reiziger'
Naam persoon:	T. van der Lee
Plaats:	Vreeland
Datum:	23-5-2018