

AVG

De Algemene verordening gegevensbescherming (AVG) is van toepassing. Dit betekent dat er dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer. De AVG is ook wel bekend onder de Engelse naam: General Data Protection Regulation (GDPR).

We selecteren de belangrijkste informatie en verwijzen je naar hulpbronnen. Ook hebben we enkele documenten voor je gemaakt, die als voorbeeld kunnen dienen. Dit zijn algemeen opgestelde documenten, die niet altijd precies zullen aansluiten bij jouw specifieke situatie. Het is aan jou om de teksten aan te passen naar jouw situatie.

De overheid heeft toegezegd dat bij de toepassing van de privacyregels rekening wordt gehouden met de omvang van organisaties. Hierdoor moet voorkomen worden dat Nederland onnodige lasten oplegt aan kleine organisaties.

Voor de inhoud en de manier waarop je deze documenten toepast is de vereniging niet aansprakelijk.

[Bron: Autoriteit Persoonsgegevens]

Met de AVG krijgen mensen meer zeggenschap over hun persoonsgegevens. Zij mogen bijvoorbeeld hun gegevens inzien en laten wijzigen of in veel gevallen zelfs volledig laten wissen. Ook krijgen zij het recht bij een organisatie hun persoonsgegevens op te vragen en mee te nemen naar een andere ‘aanbieder’; het recht op dataportabiliteit. En komen ze er met de organisatie niet uit, dan kan iedereen vanaf 25 mei een klacht indienen bij de Autoriteit Persoonsgegevens.

Bedrijven en overheden zijn verplicht om zorgvuldig om te gaan met persoonsgegevens. Zij hebben vanaf 25 mei een verantwoordingsplicht. Dat betekent dat zij een privacy-administratie moeten bijhouden. Welke persoonsgegevens verwerken zij? Met welk doel? En hoe zijn die gegevens beveiligd?

Als bij een bedrijf sprake is van een grootschalige verwerking van persoonsgegevens die een kernactiviteit van de organisatie is, is deze organisatie verplicht een functionaris voor de gegevensbescherming (FG) aan te stellen en een privacy impact assessment (PIA) uit te voeren. De AVG definieert echter niet wat er precies verstaan wordt onder ‘grootschalig’, maar uit voorbeelden blijkt dat een éénpitter hier niet onder valt, wat je ontslaat van deze plicht, als je éénpitter bent. Voor een groepspraktijk zou dit mogelijk anders kunnen liggen.

De onderstaande zaken moeten zijn geregeld en/of zijn vastgelegd.

Gegevensbeperking. Alleen de noodzakelijke gegevens mogen worden verzameld.

Transparantie. De persoon van wie gegevens verwerkt worden, is hier van op de hoogte, heeft hiervoor toestemming gegeven en kent zijn rechten.

Doelbeperking. De persoonsgegevens mogen voor een legaal doel verzameld worden en mogen niet voor andere zaken gebruikt worden.

Juistheid. De persoonsgegevens moeten juist zijn en blijven.

Bewaarbeperking. De persoonsgegevens mogen niet langer bewaard worden dan nodig is.

Integriteit en vertrouwelijkheid. De persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging.

Accounts beveiligen

Met twee-staps-authenticatie kun je eenvoudig je accounts voor Facebook, Google, Twitter en Snapchat een stuk beter beveiligen. Klik [hier](#) voor meer informatie.

Beeldscherm

Je beeldscherm dient automatisch op zwart te gaan als je de computer niet gebruikt. Daarna dient opnieuw te moeten worden ingelogd.

E-mailverkeer

Je maakt wellicht gebruik van e-mail om informatie uit te wisselen met de huisarts of een medebehandelaar. Indien e-mail persoonsgegevens bevat, dan dien je deze via een beveiligde omgeving te versturen. Dit kan bijvoorbeeld met [Zorgmail](#) of [Zivver](#). Voor het versturen van afspraakbevestigingen en facturen per e-mail is extra beveiliging niet verplicht.

Heb je iemand nog nooit een factuur gestuurd? Dan mag dat alleen als iemand daarvoor actief en aantoonbaar toestemming heeft gegeven, door het aanvinken van een vakje of zijn/haar e-mailadres te geven. Je moet daarbij aangeven waarvoor je het e-mailadres gebruikt.

Voeg een disclaimer toe aan uw e-mail, bijvoorbeeld als hieronder.

De inhoud van dit bericht is alleen bestemd voor de geadresseerde en kan vertrouwelijke of persoonlijke informatie bevatten. Als u dit bericht onbedoeld heeft ontvangen verzoeken wij u het te vernietigen en de afzender te informeren. Het is niet toegestaan om een bericht dat niet voor u bestemd is te verspreiden of te kopiëren. Aan dit bericht inclusief de bijlagen kunnen geen rechten ontleend worden, tenzij schriftelijk anders wordt overeengekomen. De <praktijknaam> aanvaardt geen enkele aansprakelijkheid voor schade en/of kosten die voortvloeien uit onvolledige en/of foutieve informatie in e-mailberichten.

BSN

Het Burgerservicenummer (BSN) van je cliënt mag je niet verwerken. Het BSN van de cliënt niet op de factuur te staan.

Datalek-meldplicht

In toenemende mate maken we gebruik van mobiele apparaten en wisselen we ongemerkt allerlei (persoons)gegevens uit. Daarmee is de kans op datalekken van persoonsgegevens toegenomen. Daarom moeten apparaten en accounts goed zijn beveiligd (zie verder onder 'Accounts beveiligen'). Bij diefstal van je mobiele telefoon, laptop of pc, of het verloren gaan van een back-up, heb je een [meldplicht](#). Zorg dat je een datalekprotocol hebt. In het geval van een datalek kun je terecht bij Eerste Hulp bij Data Lekken (EHBD) van [fg-online.nl](#).

(Digitaal) dossier/praktijksoftware

Maak je gebruik van software? Informeer bij je leverancier of het product voldoet aan de AVG. De leverancier dient met jou een zogenaamde verwerkersovereenkomst af te sluiten. Het digitaal dossier dient in ieder geval beveiligd te zijn met een wachtwoord (zie verder onder 'Accounts beveiligen').

Papieren dossiers moeten achter slot en grendel.

Mobiele telefoon/overige mobiele apparaten

Zorg dat er een wachtwoord op je telefoon/overige mobiele apparaten zit en dat deze binnen 20 seconden vergrendelt. De communicatie met WhatsApp is op zich veilig. Alternatieven voor versleutelde chatapps zijn Telegram, Signal of Wire.

Privacy beleid/privacyverklaring

Je dient jouw cliënten te informeren over jouw privacy beleid. Denk er vooral ook aan om op jouw website een privacyverklaring op te nemen, die betrekking heeft op de gegevens die je via je website verzamelt. Op internet zijn tal van voorbeelden te vinden.

De [privacyverklaring van de Kamer van Koophandel](#) is een goed voorbeeld, maar heel uitgebreid. Klik [hier](#) voor een voorbeeld, die je kunt aanpassen aan jouw situatie. De privacyverklaring hoef je niet aan cliënten te sturen. Het is voldoende om de verklaring op je website te hebben (vindbaar en leesbaar).

Register van verwerkingsactiviteiten

Je dient transparant te zijn over welke persoonsgegevens je verwerkt. In een zogenaamd register van verwerkingsactiviteiten leg je vast welke persoonsgegevens je verwerkt en met welke doel. De gegevens die je verzamelt moeten goed beveiligd zijn en ze mogen uitsluitend worden gebruikt voor het verzameldoel.

Voor het opslaan en verwerken van persoonsgegevens heb je toestemming van je cliënt nodig. Je kunt hiervoor gebruik maken van een toestemmingsformulier. Je dient de cliënt de mogelijkheid te bieden zijn/haar toestemming elk moment weer te kunnen intrekken. [Toestemmingsformulier Autoriteit Persoonsgegevens](#) (voorbeeld). Je kunt deze toestemming ook opnemen in de behandelovereenkomst.

Verwerkersovereenkomst

Besteed je het beheer van gegevens uit, dan heb je een [verwerkersovereenkomst](#) nodig. Het enkele feit dat je persoonsgegevens uitwisselt, betekent niet automatisch dat een verwerkersovereenkomst nodig is. Neem als vuistregel: de overeenkomst is niet verplicht als je persoonsgegevens alleen maar (eenmalig) uitwisselt, omdat je iets koopt of een dienst afneemt. De overeenkomst is wel verplicht als de primaire opdracht is de persoonsgegevens te laten bewerken, actualiseren, bewaren, etc. (meestal is dat in de cloud).

Website

Jouw website dient beveiligd te zijn (SSL beveiliging). Je kunt eenvoudig controleren of jouw website iSSL-beveiliging heeft, namelijk er staat dan een slotje voor de url. Doe een [SSLCheck](#).

Wifi

Maak geen gebruik van een open Wifi-verbinding. Hang nooit het wachtwoord van de Wifi-verbinding op in de wachtkamer, als daarmee jouw cliënten op hetzelfde netwerk zitten als jijzelf.

HULP EN INFORMATIE

Je kunt bij de Stichting AVG voor Verenigingen een abonnement afnemen, waarmee je toegang kunt krijgen tot een stappenplan om alle punten die in het kader van de wetgeving van belang zijn door te lopen. Je krijgt hiermee overzicht op wat je moet regelen en al geregeld hebt. Na het doorlopen van het gehele stappenplan kun je een verklaring opvragen en krijg je het OK-vignet, waarmee je laat zien dat je AVG-proof bent.

[Landingspagina VVH-Stichting AVG voor Verenigingen](#)

De Autoriteit Persoonsgegevens heeft een [regelhulp](#) ontwikkeld. Na het doorlopen van de stappen ontvang je de uitslag met actiepunten en tips. Met vragen over de AVG kun je contact

opnemen met de Autoriteit Persoonsgegevens (AP) tijdens het telefonisch spreekuur op maandag, dinsdag, donderdag en vrijdag van 10.00 tot 12.00 uur. De AP is bereikbaar via telefoonnummer 0900-2001201. Het is ook mogelijk vragen per e-mail te stellen via vragenAVG@autoriteitpersoonsgegevens.nl.

De [Stichting AVG voor Verenigingen](#) heeft een handig instrument ontwikkeld hoe je dit kunt aanpakken. De 'tool' heeft een stappenplan om tot een AVG-verklaring te komen. Als lid van de Vereniging Haptonomie kun je deze tool met korting aanvragen. De kortingscode kun je bij ons opvragen.