Privacy wetgeving mei 2018

Dit document is alleen voor jou.

De wet A.V.G.

Op dit moment zijn er twee wetten, de oude wet met de afkorting WBP en de nieuwe wet met de afkorting AVG:

1. Wet bescherming Persoonsgegevens – WBP. Deze wet is geldig tot 25 mei 2018.
2. Wet Algemene Verordening Gegevensbescherming – AVG. Deze wet is geldig vanaf mei 2018.
3. Daaraan ten grondslag ligt de Europese wet GDPR (General Data Protection Regulation).

De regels voor het omgaan met persoonsgegevens zijn afkomstig van de wet WBP aangevuld met de veranderde wetgeving van de nieuwe wet, de AVG. Overal in de tekst van deze les gaan we uit van de nieuwe wet; Wet Algemene Verordening Gegevensbescherming – AVG.

Wat zijn persoonsgegevens?

*Een persoonsgegeven is elk gegeven is over een geïdentificeerde of identificeerbare natuurlijke persoo*n. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van overleden personen of van organisaties geen persoonsgegevens (meer) zijn.

Er zijn vele soorten (klassen) persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers en

postcodes met huisnummers zijn *persoonsgegevens*. Gevoelige gegevens als iemands ras, afkomst, godsdienst of gezondheid worden ook wel *bijzondere persoonsgegevens* genoemd. Deze zijn door de wetgever extra beschermd.

Als het personen in Europa betreft

De nieuwe wet dekt heel Europa. En sinds deze nieuwe wet AVG dient elk bedrijf (of instantie) dat zich richt op inwoners van Europa zich aan de wet AVG te houden. Dus ook als de zetel van het bedrijf buiten de EU ligt, of de hosting-provider van bijvoorbeeld de database zich buiten de EU bevindt.

Wat is verwerken van persoonsgegevens

Elke handeling die een organisatie kan uitvoeren met persoonsgegevens, van verzamelen tot en met vernietigen.
Dit is een zeer ruim begrip. Handelingen die er in ieder geval onder vallen, zijn:
Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

Overzicht verwerkingen

- Breng de gegevensverwerkingen in kaart.
- Documenteer welke persoonsgegevens je verwerkt en met welk doel je dit doet, waar deze gegevens vandaan komen en met wie je ze deelt.
- Onder de AVG heb je een verantwoordingsplicht, wat inhoudt dat je moet kunnen aantonen dat jouw organisatie in overeenstemming met de AVG handelt.
- Je kunt het overzicht ook nodig hebben als betrokkenen hun privacy-rechten uitoefenen. Als zij vragen hun gegevens te corrigeren of verwijderen, moet je dit doorgeven aan de organisaties waarmee je ooit hun gegevens hebt gedeeld.
- Vermeld in het overzicht ook per categorie van gegevens op basis van welke wettelijke grondslag je deze gegevens verwerkt. Beroep je je bijvoorbeeld op een gerechtvaardigd belang of vraag je toestemming aan de betrokkenen?

Welke gegevens mag je verwerken (waaronder bijhouden)

Een organisatie mag alleen persoonsgegevens verwerken als dat *noodzakelijk is voor een bepaald doel*. Ook kan de organisatie deze gegevens niet zomaar voor een ander doel gebruiken. Organisaties hebben de verplichting om persoonsgegevens goed te beveiligen.
Bij elk gebruik van persoonsgegevens geldt dat de inbreuk op iemands persoonlijke levenssfeer zo klein mogelijk moet zijn. Niet elke verwerking van persoonsgegevens hoeft overigens een inbreuk op de privacy te zijn. Of dat zo is, hangt af van het soort gegevens en hoe een organisatie deze gebruikt.
Hoe specifieker de informatie, hoe groter de kans dat je gegevens gaat bijhouden die vallen onder *Bijzondere* Persoonsgegevens.

Wat zijn bijzondere persoonsgegevens

Dat zijn gegevens over iemands:

- godsdienst of levensovertuiging;
- ras;
- afkomst (anders dan ras);
- politieke voorkeur;
- gezondheid;
- seksuele leven;
- lidmaatschap van een vakbond;
- strafrechtelijk verleden.

In de nieuwe wet is het burgerservicenummer (BSN) geen bijzonder persoonsgegeven.

Wat hou je bijvoorbeeld bij over je clienten

Een therapeut mag verschillende gegevens over een cliënt bewaren in een dossier. Dit dossier bestaat uit administratieve gegevens en informatie die nodig is voor de therapie aan en de begeleiding van de cliënt.

Het cliëntendossier kan de volgende gegevens bevatten:

- gegevens over data en tijden van afspraken
- gegevens over afwezigheid;
- adresgegevens;
- gegevens die nodig zijn om te berekenen hoeveel geld de therapeut krijgt;
- voortgangsrapportage;
- gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen;
- de resultaten van eventueel psychologisch onderzoek.

Wat hou je bijvoorbeeld bij over je cursisten

Een school mag verschillende gegevens over een leerling bewaren in het zogeheten leerlingdossier. Dit dossier bestaat uit administratieve gegevens en informatie, nodig voor het onderwijs aan en de begeleiding van de leerling.

Het leerlingdossier kan de volgende gegevens over een leerling bevatten:

- gegevens over in- en uitschrijving;
- gegevens over afwezigheid;
- adresgegevens;

- gegevens die nodig zijn om te berekenen hoeveel geld de school krijgt;
- het onderwijskundig rapport;
- gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen;
- gegevens over de vorderingen en de resultaten van de leerling;
- verslagen van gesprekken met de ouders;
- de resultaten van eventueel psychologisch onderzoek.

Identiteitsbewijs

Soms is het nodig voor een organisatie om iemands identiteit vast te stellen, zoals van een cliënt, student, medewerker of ZZP'er. Bijvoorbeeld om fraude te voorkomen.
Een organisatie kan dit op verschillende manieren doen. Welke manier is toegestaan, hangt af van de toepasselijke wet en van de noodzaak.

Identiteitsbewijs tonen

Vaak is het genoeg als mensen hun identiteitsbewijs, zoals hun paspoort of identiteitskaart, laten zien. Dit wordt ook wel 'legitimeren' of 'identificeren' genoemd. Dan zet je in de clienten dossier: gelegitimeerd: ja, met de datum er bij.

Gegevens overnemen

De organisatie kan na het tonen eventueel noteren om welk identiteitsbewijs het ging en het nummer

hiervan. In enkele gevallen zijn organisaties wettelijk verplicht om bepaalde persoonsgegevens van iemands identiteitsbewijs over te nemen.

Kopie of scan identiteitsbewijs

Een organisatie mag alleen in uitzonderlijke gevallen een kopie of scan maken van iemands identiteitsbewijs. Dit geldt onder meer als het in de wet staat. Dit is bij clienten van je praktijk of cursisten niet nodig. (Een uitzondering daarop zou kunnen zijn het verstrekken van medicijnen die alleen op heel strenge voorwaarden of aan een bepaalde doelgroep dient te worden verstrekt).
Als je daarentegen een collega toegang zou geven tot de persoonsgegevens van je clienten, dan is een kopie maken van het legitimatiebewijs van deze collega geen overbodige luxe.

Regels bij identificatie

Bij het laten tonen of tijdelijk innemen van een identiteitsbewijs verwerkt een organisatie geen persoonsgegevens. Daarom vallen deze situaties niet onder de privacywetgeving. Maar er kunnen wel andere (wettelijke) regels gelden. Zo moeten mensen op grond van de Wet op de identificatieplicht in bepaalde situaties hun identiteitsbewijs laten zien en blijft een identiteitsbewijs altijd eigendom van de staat.

Wie is de verantwoordelijke bij het verwerken van persoonsgegevens?

De *verantwoordelijke* is de persoon of organisatie die het doel *van* en de middelen *voor* het gebruik van persoonsgegevens bepaalt. De verantwoordelijke kan dit alleen doen, of samen met anderen. Het houdt in dat de verantwoordelijke uiteindelijk beslist of een organisatie persoonsgegevens verwerkt, en zo ja:

- Om welke verwerking het gaat;
- Welke persoonsgegevens de organisatie hierbij verwerkt;
- Voor welk doel de organisatie dit doet;
- Op welke manier de organisatie dit doet.

Wie is de betrokkene bij het verwerken van persoonsgegevens?

- De *betrokkene* is degene van wie een organisatie persoonsgegevens verwerkt.
- Dit is dus degene op wie de persoonsgegevens betrekking hebben, zoals de cliënt of de student.

Wie is de verwerker/bewerker bij het verwerken van persoonsgegevens?

- Een *verwerker* / *bewerker* is een persoon of organisatie aan wie de verantwoordelijke de gegevensverwerking heeft uitbesteed. Bijvoorbeeld een administratiekantoor.

- Een bewerker is niet zelfstandig verantwoordelijk voor de verwerking van de persoonsgegevens.
- De bewerker heeft wel een aantal afgeleide verplichtingen, voor onder meer beveiliging en geheimhouding van de gegevens.

Er dus sprake van een:

- Verantwoordelijke
- Betrokkene
- Verwerker / bewerker

Bewaren van persoonsgegevens

De inhoud van een digitaal of papieren dossier bevat veel informatie over een persoon. De huisarts weet bijvoorbeeld welke medicijnen zijn patiënt gebruikt. En de werkgever kan zien wanneer het salaris van een werknemer voor de laatste keer is verhoogd. Om een goede administratie bij te kunnen houden, moet een organisatie bepaalde persoonsgegevens een tijd bewaren. Maar organisaties mogen die gegevens niet langer bewaren dan noodzakelijk is. Er is op grond van de Wet bescherming persoonsgegevens (Wbp) geen concrete bewaartermijn voor persoonsgegevens. Organisaties bepalen zelf hoe lang zij persoonsgegevens bewaren. Hierbij kijken zij naar hoe lang de gegevens nodig zijn voor het doel waarvoor deze zijn verzameld of worden gebruikt.
Wel zijn er concrete bewaartermijnen in andere wetten waar organisaties zich aan moeten houden. Bijvoorbeeld op grond van belastingwetgeving.

Vernietigen of archiveren

Is de bewaartermijn van persoonsgegevens voorbij of zijn de gegevens niet meer noodzakelijk? Dan moeten organisaties de gegevens vernietigen. Organisaties mogen persoonsgegevens in een archief bewaren als dit bestemd is voor historische, statistische of wetenschappelijke doeleinden. Tenzij de Archiefwet of een andere wet van toepassing is, geldt voor persoonsgegevens in een

archief geen bewaartermijn. De organisatie moet de gegevens vernietigen als ze niet meer nodig zijn voor het doel van het archief.

Toestemming

Je mag persoonsgegevens bijhouden zonder daar toestemming voor gevraagd te hebben aan de betrokkene(n). Daarbij gaat de wet er wel vanuit dat je alleen die gegevens verzamelt en bewaart die je nodig hebt voor het doel.

Foto toestemming

Je mag een foto van de client of student zonder toestemming gebruiken en bewaren als deel van je persoonsgegevens. Elke publicatie of ander gebruik daarvan op bijvoorbeeld sociale media mag daarentegen alleen met toestemming van de betrokkene.

Verstrekken van persoonsgegevens

Een organisatie mag niet zomaar persoonsgegevens doorgeven aan personen of andere organisaties. De algemene regel is dat verstrekken van persoonsgegevens alleen mag als dat verenigbaar is met het doel waarvoor de gegevens zijn verzameld. Of dit het geval is, hangt af van de concrete omstandigheden. Dat kan dus per situatie verschillen.

Verenigbaar met doel

Bij de vraag of een verstrekking verenigbaar is, spelen verschillende factoren een rol, waaronder:

- de verwantschap met het doel van verzamelen;
- de aard van de gegevens;
- de gevolgen van een verstrekking;
- de waarborgen die zijn getroffen;
- de verwachtingen van de betrokkene (degene van wie een organisatie persoonsgegevens gebruikt).

Gronden voor verstrekking

Naast de algemene regel van verenigbaarheid geldt dat het verstrekken van gegevens gebaseerd moet zijn op één van de 6 gronden (ook wel grondslagen genoemd)

Dat zijn:

- toestemming van de betrokkene;
- uitvoeren van een overeenkomst;
- wettelijke verplichting;
- vitaal belang van de betrokkene;
- uitvoeren van een publiekrechtelijke taak;
- gerechtvaardigd belang van de organisatie.

Doorgeven van gegevens en toestemming

Organisaties moeten kunnen bewijzen dat zij geldige toestemming hebben gekregen om gegevens van een betrokkene door te geven. En het moet voor mensen net zo makkelijk zijn om hun toestemming in te trekken als om die te geven. Vanaf dat moment van intrekking mag de organisatie de persoonsgegevens niet meer verstrekken.

Belangrijke regels van deze wet:

Gedragscode
Een branche, sector of instantie/onderneming kan een gedragscode gebruiken voor de omgang met persoonsgegevens. Dit is een vorm van zelfregulering. Door een gedragscode op te stellen, is het voor jouw instantie / onderneming duidelijk hoe een ieder om dient te gaan met de persoonsgegevens.

Bijhouden wie inziet
Elke keer dat een medewerker, leraar of wie dan ook een dossier inziet, dient er een aantekening gemaakt te worden wie en wanneer de gegevens heeft ingezien.

Bijhouden aan wie doorgegeven
Elke keer dat persoonsgegevens worden verstrekt of doorgegeven, dient er een aantekening gemaakt te worden aan wie en wanneer de gegevens zijn verstrekt.

Recht op inzage
Mensen hebben recht op inzage in hun persoonsgegevens. Dat houdt in dat zij een organisatie mogen vragen of deze persoonsgegevens van hen heeft vastgelegd en zo ja, welke. Zij hoeven geen reden te geven voor een inzageverzoek.

Vraagt iemand om inzage, dan moet de organisatie diegene op een duidelijke en begrijpelijke manier laten weten:

- of de organisatie zijn persoonsgegevens gebruikt, en zo ja:
- om welke gegevens het gaat;
- wat het doel is van het gebruik;
- aan wie de organisatie de gegevens eventueel heeft verstrekt;
- wat de herkomst is van de gegevens, als deze bekend is.

Reikwijdte inzagerecht

Het recht op inzage betreft alleen inzage in iemands eigen gegevens. Mensen hebben dus geen recht op informatie over anderen.

Werk-aantekeningen door therapeut of leraar:

Gebruikt een organisatie persoonlijke werkaantekeningen als geheugensteuntje? Dan vallen deze aantekeningen niet onder het inzagerecht. Maar slaat de organisatie de aantekeningen vervolgens op in een dossier of verstrekt de organisatie deze aan anderen? Dan heeft degene over wie het gaat ook recht op inzage in deze aantekeningen.

Recht op correctie en verwijdering

Mensen hebben het recht om correctie van hun persoonsgegevens te vragen. Dat houdt in dat zij een organisatie mogen vragen hun

persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen.

Iemand kan om correctie vragen als zijn persoonsgegevens:

- feitelijk onjuist zijn;
- onvolledig zijn of niet ter zake doen voor het doel waarvoor ze zijn verzameld;
- op een andere manier in strijd met een wet worden gebruikt.

Reikwijdte correctierecht

Het correctierecht is niet bedoeld voor het corrigeren van professionele indrukken, meningen en conclusies waarmee iemand het niet eens is, voor zover deze ter zake doen. Wel mag diegene van de organisatie verwachten dat deze in ieder geval zijn schriftelijke mening toevoegt aan het dossier. Dat kan vooral een oplossing bieden bij situaties waarbij het om niet objectief vast te stellen feiten gaat. Gecorrigeerde gegevens dienen ook door te worden doorgegeven aan alle organisaties waar je de gegevens mee gedeeld heeft.

Recht van verzet

Mensen hebben het recht aan een organisatie te vragen hun persoonsgegevens niet meer te gebruiken. Dit heet het recht van verzet. Iemand kan bijvoorbeeld om bijzondere persoonlijke redenen van het recht van verzet gebruikmaken.

Recht van verzet bij bijzondere persoonlijke omstandigheden

Iemand kan verzet aantekenen vanwege bijzondere persoonlijke omstandigheden. Bijvoorbeeld als diegene als patiënt mee heeft gedaan aan een medisch onderzoek en er later achter komt dat een bekende als onderzoeker bij dat centrum werkt. Deze persoon kan er dan belang bij hebben dat zijn gegevens worden verwijderd of niet meer tot hem zijn te herleiden.

Hoe kan een organisatie voldoen aan een correctieverzoek?

Een organisatie is verplicht binnen 4 weken schriftelijk of per e-mail te reageren op een correctieverzoek. Besluit de organisatie de gegevens te corrigeren, dan moet dit zo snel mogelijk gebeuren.

Is het technisch gezien niet mogelijk om gegevens te verbeteren? Bijvoorbeeld doordat deze zijn opgeslagen op een cd-rom? Dan kan de organisatie een bestand met aanvullingen en verbeteringen aanleggen.

Andere organisaties informeren

Heeft de organisatie in het voorafgaande jaar (onjuiste) gegevens aan andere organisaties doorgegeven? Dan moet de organisatie ook zo snel mogelijk deze andere organisaties van de wijzigingen op de hoogte stellen. Maar dit hoeft niet als het onmogelijk is om die organisaties op te

sporen. Bijvoorbeeld als de organisatie niet meer beschikt over de daarvoor benodigde informatie. Het hoeft ook niet als het een onevenredige inspanning zou zijn. Bijvoorbeeld als een persoonsnaam verkeerd gespeld staat in een landelijk verspreid telefoonboek. De betrokkene kan dan niet van de uitgever verlangen om iedereen die het telefoonboek heeft ontvangen van de wijziging op de hoogte stellen.

Identiteit controleren

Voordat de organisatie een correctieverzoek in behandeling neemt, kan deze controleren of de betrokkene daadwerkelijk is wie hij of zij zegt te zijn. De organisatie kan daartoe vragen om een identiteitsbewijs te laten zien of om een kopie daarvan op te sturen.

is het de mening dat een kopie noodzakelijk is? Dan mag de betrokkene de pasfoto en burgerservicenummer (BSN) onzichtbaar maken, tenzij een van de twee juist nodig zijn voor het doel.

Bijhouden welke externe data bij een verwerker gebruikt wordt

Als een deel van de persoonsgegevens door een externe verwerker ingezien dus verwerkt wordt, bijvoorbeeld om mailings samen te stellen of voor het maken van statistieken, dien je bij te houden welke gegevens je aan wie hebt doorgegeven, en voor welk doel.

Register van datalekken

Als er onverhoopt door een inbraak, fysiek of in de cloud of anderszins, iemand toegang heeft gekregen tot persoonsgegevens, dien je dit bij te houden; datum, soort inbraak, mogelijke data ingezien en van wie.

Datalekken doorgeven

Als er onverhoopt door een inbraak, fysiek of in de cloud of anderszins, iemand toegang heeft gekregen tot persoonsgegevens, dien je dit door te geven aan de Autoriteit Persoonsgegevens. Minimaal vereist voor het doorgeven: datum, soort inbraak, mogelijke data ingezien en van wie.

Recht op data-portabiliteit

(in leesbare vorm verstreken aan client / student)

De Algemene verordening gegevensbescherming (AVG) geeft betrokkenen (degenen van wie persoonsgegevens worden verwerkt) het recht op dataportabiliteit, oftewel overdraagbaarheid van persoonsgegevens. Het houdt in dat betrokkenen het recht hebben om de persoonsgegevens te ontvangen die een organisatie van hen heeft. Vervolgens kunnen betrokkenen deze gegevens zelf opslaan voor persoonlijk (her)gebruik. Ook kunnen ze de gegevens doorgeven aan een andere organisatie. Bijvoorbeeld als ze willen overstappen naar een andere telecomprovider of als ze een

dienst van een andere organisatie willen gebruiken, zoals een online huishoudboekje.
De organisatie die de gegevens verstrekt, mag betrokkenen hierin niet tegenwerken. En moet ervoor zorgen dat de betrokkenen hun gegevens makkelijk kunnen krijgen en doorgeven.

Acceptabele vormen en voorwaarden:

- niet encrypted
- leesbaar door de betrokkene
- bestandsformaat dat ‘algemeen leesbaar’ is zoals CSV, XML, TXT, PDF

Regels die voor jou niet gelden:

Register van verwerkingsactiviteiten

Bedrijven of instanties met meer dan 250 medewerkers dienen een register van verwerkingsactiviteiten bij te houden.
Bedrijven of instanties met minder dan 250 medewerkers hoeven dat register van verwerkingsactiviteiten alleen bij te houden indien

- er gegevens die een hoog risico inhouden voor de rechten en vrijheden van de personen van wie u persoonsgegevens verwerkt bijhoudt en/of;
- waarvan de verwerking niet incidenteel is en/of;
- die vallen onder de categorie bijzondere persoonsgegevens. Zoals gegevens over godsdienst, gezondheid en politieke voorkeur of strafrechtelijke gegevens.

Bent u verplicht om een register van verwerkingsactiviteiten op te stellen? Dan moet u dit register kunnen verstrekken wanneer de Autoriteit Persoonsgegevens daar om vraagt.
Noot: tenzij je wel heel veel details bij gaat houden over je clienten en/of studenten is dit niet nodig.

Functionaris voor de gegevensbescherming (FG)

Alleen bij:

– Overheden en publieke organisaties

Ten eerste zijn overheidsinstanties en publieke organisaties altijd verplicht om een FG aan te stellen, ongeacht het type gegevens dat ze verwerken. Het kan gaan om de rijksoverheid, gemeenten en provincies, maar ook om bijvoorbeeld zorg- en onderwijsinstellingen. Voor rechtbanken geldt de verplichte aanstelling van een FG niet.

– Observatie

Ten tweede geldt de verplichting om een FG aan te stellen voor organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen. Het kan hierbij gaan om bijvoorbeeld profilering van mensen voor het maken van risico-inschattingen, cameratoezicht en monitoring van iemands gezondheid via wearables.

Relevant hierbij zijn onder meer het aantal mensen dat een organisatie volgt, de hoeveelheid gegevens die deze organisatie verwerkt en hoe lang de organisatie mensen volgt.

– Bijzondere persoonsgegevens

Ten derde zijn organisaties verplicht een FG te benoemen als ze op grote schaal bijzondere persoonsgegevens verwerken en dit een kernactiviteit is. Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over iemands gezondheid, ras, politieke opvatting, geloofsovertuiging of strafrechtelijke verleden.

Klacht en Handhaving:

Klacht over gebruik persoonsgegevens

Heeft een betrokkene een klacht over het gebruik van zijn of haar persoonsgegevens? Bijvoorbeeld omdat de betrokkene vindt dat een organisatie niet zorgvuldig omgaat met de persoonsgegevens? Of omdat deze inzage of correctie heeft gevraagd van de persoonsgegevens, maar niet tevreden is met de reactie? De betrokken dient dan eerst naar de organisatie zelf te gaan. Komen de betrokkene en de organisatie er samen niet uit, dan kan de betrokkene alsnog naar de rechter gaan.

Handhaving en boete door Autoriteit Persoonsgegevens

Het houden aan deze wet en regels is niet optioneel, maar verplicht.

Bedenk dat de AP (Autoriteit Persoonsgegevens) jouw organisatie sancties kan opleggen van maximaal 20 miljoen euro of 4% van de omzet als jouw praktijk niet aan de nieuwe privacywetgeving houdt.

Hoe geef je invulling aan deze wet:

Gegevens voor één doel

Het is niet toegestaan gegevens die je hebt te gebruiken voor een ander doel dan waarvoor de cliënt je die gegevens heeft verstrekt. Dat betekent dat een spiritueel centrum of een beroepsorganisatie bijvoorbeeld geen gegevens van de bij haar aangesloten beoefenaars verstrekt aan een groothandel van behandeltafels of aan een uitgever van boeken. Zij zouden deze gegevens echter wèl kunnen verstrekken aan een organisatie die bijvoorbeeld een website onder haar beheer heeft waar Nederlandse erkende healers op staan. Dat mag omdat de activiteiten in de belangensfeer van de aangesloten beoefenaars liggen. Als de wet gegevens verlangt of indien de persoon over wiens gegevens het gaat er zelf om verzoekt, is het uiteraard een andere zaak.

Gegevens in verhouding tot het doel

Elke houder van een persoonsregistratie wordt geacht alleen die gegevens bij te houden die voor dat doel van belang zijn. Het salaris en het type auto van de cliënt is voor een behandeling bijvoorbeeld minder van belang. Zodra je korting geeft aan cliënten met een minimum inkomen zou je dat wel eens op de klantenkaart kunnen vermelden. Dan is dat weliswaar nodig, maar ook zeer privacy gevoelige informatie.

Laat client of student weten dat hun persoonsgegevens bewaard worden

Op een moment dient de client, student (of medewerker indien van toepassing) te worden medegedeeld dat je hun gegevens bij gaat houden. Bij voorkeur met een indicatie van het hoe en waarom of met een verwijzing naar een inhoudelijke tekst.
Het verdiend dan ook de voorkeur om de client of student in de gelegenheid te stellen om ergens te lezen wat je bijhoudt en voor welk doel en wat zij, volgens de wettelijke regelingen, mogen qua recht op inzagen, aanpassing, verwijdering etc.
Voorbeeld:
http://www.nederlofcentrum.nl/privacy-en-gerelateerd/

Termijn van behandeling

Indien een cliënt een verzoek indient om gegevens in te zien, te wijzigen of te laten verwijderen, dient de organisatie (jij) te reageren binnen een termijn van vier weken na aanvraag.

Legitimatie bij elke aanvraag door geregistreerde

Het recht op informatie mag niet ten koste gaan van de privacy. Om zeker te weten dat de informatieaanvraag van de geregistreerde zelf is, dient elke aanvraag te gebeuren onder vermelding

van naam, volledig adres en als bijlage een kopie van paspoort of rijbewijs.

Wat kan zonder problemen

Zonder problemen kan je gebruik maken van de volgende gegevens;
Naam, voornamen, titulatuur, geslacht, geboortedatum, adres, woonplaats, telefoonnummers, bankgegevens en een administratie-nummer. Verder kun je bepaalde gegevens noteren als huisarts, specialist, medicijnen, klachten, klachtenverloop en dergelijke.

Wijze van verzamelen van gegevens

Het verzamelen van gegevens kan bijvoorbeeld mondeling, middels een papieren formulier (zoals een intake bij een behandelaar) of een formulier op een website.

Mondeling

Het mondeling verzamelen van gegevens dient, indien er sprake is van persoonsgegevens, te gebeuren onder omstandigheden die de privacy van de betrokkene intact laten. Dus zonder dat anderen erbij zijn, teksten zouden kunnen overhoren of notities zouden kunnen maken.

Papier

Het verzamelen van gegevens middels een papieren drager, zoals een intake formulier, dient indien er sprake is van persoonsgegevens, te gebeuren onder omstandigheden die de privacy van de betrokkene

intact laten. Dus het invullen en later lezen en verwerken ervan dient te gebeuren zonder dat onbevoegden erbij zijn, teksten zouden kunnen lezen of notities zouden kunnen maken.

Digitaal

Het verzamelen van gegevens middels een digitaal (website) formulier, dient indien er sprake is van persoonsgegevens, te gebeuren onder omstandigheden die de privacy van de betrokkene intact laten.

Dat wil zeggen dat:

– Het formulier verstuurt moet worden middels een beveiligde verbinding (SSL / HTTPS)

– Dat het lezen en verwerken ervan dient te gebeuren zonder dat onbevoegden erbij zijn of deze teksten zouden kunnen lezen of notities zouden kunnen maken.

Extra informatie over verzamelen

- Ook een email die je ontvangt met daarin informatie is ‘verzamelen’.
- Een email adres gebruiken van bijvoorbeeld Google (Gmail) of Hotmail (Microsoft) betekent dat alle informatie in de email door deze organisaties wordt gelezen.
- Gebruik dus een email provider die de emails van hun gebruikers niet leest. (Elders in deze module staan handige adressen).
- Cookies die ‘door een website’ geplaatst worden op de computer of smartphone etc valt ook onder de privacy wetgeving. De bezoeker

van jouw website dient op de hoogte te worden gesteld dat je een cookie plaatst en de bezoeker dient ook akkoord te gaan. Belangrijk in de nieuwe wet is dat de bezoeker ook het recht heeft om een cookie te weigeren en dan nog steeds het recht heeft de website te bezoeken, met zoveel mogelijk behoud van de functionaliteit. Er bestaan verschillende soorten cookies:

- – **Gewone functionele cookies**. Deze worden altijd geplaatst anders zou bijvoorbeeld de browser de site niet goed kunnen vergeven en zou je steeds opnieuw moeten aangeven in welke taal je de website wilt lezen.
- – **Performance cookies**. Hiermee kan worden gemeten of bijvoorbeeld een advertentie leidt tot een aankoop of aanmelding of dat een bezoek leidt tot een vervolg bezoek.
- – **Analytische cookies**. Hiermee kunnen website-eigenaren de statistieken van hun site bijhouden. In Google Analytics bijvoorbeeld kunnen de aantallen bezoekers, locatie van bezoekers en gebruikte browser worden gemeten.
- – **Profilerings cookies**. Dit zijn cookies die er voor kunnen zorgen dat je ineens advertenties te zien krijgt met producten die je net hebt bekeken op bv. bol.com Daarnaast gebruikt Facebook dit soort cookies wanneer je op de

'vind ik leuk' knop hebt geklikt. Daarom zie je soms wie van je vrienden een bepaald product wel of niet heeft 'geliked'.

- Mocht je denken 'Ik plaats geen cookies'; jouw website doet dit vaak zonder dat je het weet. Als jij of je webbouwer bijvoorbeeld gebruik maakt van Google analytics of je werkt met Google search of je hebt een filmpje van Youtube op je site staan; deze plaatsen alle cookies.

Gebruik van gegevens buiten jouw kantoor

Als je buiten je kantoor omgeving gebruik maakt van persoonsgegevens, zoals een cliëntenformulier of een lijst van deelnemers, dienen deze gegevens niet rond te slingeren en na afloop weer meegenomen te worden of op verantwoorde wijze vernietigd te worden.

Veiligheid gegevens

De gegevens dienen veilig te zijn opgeborgen en er dient voorkomen te worden dat deze gegevens per ongeluk op straat of elders terecht komen. Het is de bedoeling dat de gegevens niet voor iedereen in dezelfde ruimte toegankelijk zijn. Een kast met een slot, een computer met een wachtwoord zijn normale maatregelen.
Als je bijvoorbeeld een dossier in gebruik hebt en iemand komt binnen hoort de bezoeker geen 'blik te

kunnen werpen' op het dossier en/of de persoonsgegevens.

Vernietiging

Indien een cliëntenformulier of een gehele administratie wordt vernietigd, dient dit op een manier te gebeuren die de privacy waarborgt. Dat wil zeggen dat je een dossier niet in de prullenbak gooit, maar vernietigt middels een goede papierversnipperaar of door dit door een erkend vernietigingsbedrijf te laten uitvoeren. Ook als je een papierbak hebt die in zijn geheel later door de papierversnipperaar gaat, dient deze bak middels een deksel afgesloten te zijn.
Een digitaal bestand dient ook op een correcte manier te worden verwijderd en indien een computer, back-up of online backup of opslag wordt afgedankt of opgezegd dienden de gegevens grondig te worden verwijderd.

In verband met klachten of terugkoppeling

Wij adviseren om de aanwezige cliënten-gegevens minimaal vijf jaar na het afsluiten van het dossier (veilig) te bewaren. Dit is mede in het belang van de behandelaar of leraar zelf bij de behandeling van eventuele klachten en geschillen.

Hoe hou je de gegevens bij:

Papier

- Een ouderwetse kaartenbak of ordner voldoet nog steeds maar heeft qua privacy een aantal nadelen waarbij beveiliging een groot nadeel is. Als je kiest voor de papieren versie dient het opgeborgen te worden in een afsluitbare kaartenbak of ordner in een afsluitbare kast.
- Waarbij belangrijk is dat niet iedereen in die kast kan.

Elektronische kaartenboek – adresboek

- Elke computer of smartphone heeft een adresboek.
- Dit kan over het algemeen voldoende informatie bevatten om functioneel te zijn.
- Nadeel is dat niet elk systeem echt de privacy van de client of student kan garanderen; de meeste Android systemen bijvoorbeeld zijn besmet (85%) met een vorm van malware waardoor anderen toegang hebben tot jouw telefoon of tablet. Ook Windows systemen zijn heel vaak besmet en is het is waarschijnlijk alleen kwestie van tijd voordat Apple systemen soortgelijke problemen hebben.

Als je persoonsgegevens bewaart op een computer of tablet of smartphone

- Apparaat dient beveiligd te zijn met een wachtwoord

- Het bestand waar de persoonsgegevens in staan, zoals een database of spreadsheet dient ook beveiligd te zijn met een wachtwoord.
- Als je een adresboek kiest bij een extern bedrijf, bijvoorbeeld online via internet, dient de toegang ook beveiligd te zijn met een wachtwoord.

Adresboek in facturering- of boekhoud programma

- Elk facturering- of boekhoudprogramma heeft de mogelijkheid crediteuren in te voeren. Voordeel daarvan is dat je dan meteen ook een factuur op hun naam kunt maken en versturen. Ook een boekhoudprogramma dient beveiligd te zijn met een wachtwoord.

Combinatie van 2 locaties

- Natuurlijk hoeven niet alle gegevens op een centrale plek opgeslagen te zijn.

Voorbeeld:

- In je adresboek of boekhoudprogramma bewaar je de contactgegevens van je clienten of studenten. Elke persoon geef je een klant nummer.
- Op je praktijk of laptop of tablet bewaar je een dossier voor elke client of student.

(dat kan ook gewoon een MS Word bestand zijn) met data sessies, notities etc. Als je het heel veilig

wil doen zet je daar alleen hun klantennummer op en hun voornaam.

Wachtwoord – beveiliging

- Het wachtwoord waarmee de computer, laptop of smartphone is beveiligd mag niet ergens worden opgeschreven of vindbaar te zijn of een telefoon, tablet of smartphone. Daarvoor wordt een wachtwoord App voor je smartphone aangeraden; daar kan je al je wachtwoorden en pincodes in bewaren en je hoeft dan nog maar één wachtwoord te onthouden; het wachtwoord van de wachtwoord app zelf.
- Als je een wachtwoord app uitzoekt kan je zoeken met trefwoord *password* of *wachtwoord.*
- Als je gebruik maakt van een wachtwoord app zorg dat dat je regelmatig een back-up maakt daarvan of dat de app de wachtwoorden ergens versleuteld in de cloud opslaat. Anders zou je bij een nieuwe of gestolen telefoon al je wachtwoorden kwijt zijn.
- Geschikte apps zijn bijvoorbeeld:
- – 1Password (nadeel duur)
- – Securesafe (gratis tot 50 wachtwoorden)

Tot slot: data is business

Er zijn steeds meer bedrijven die het verzamelen, bewaren en verkopen van persoonsgegevens, al dan niet anoniem gemaakt, tot hun kern-bedrijfsactiviteit gemaakt hebben.

Denk aan:

- Google
- Gmail (eigendom van Google / Alphabet)
- WhatsApp (eigendom van Google / Alphabet)
- Hotmail (eigendom van Microsoft / Windows)
- En er zijn er nog veel meer met wat minder bekende namen.

Er zijn ook veel diensten die je misschien onder een andere naam kent maar ook eigendom zijn van Google (Alphabet) of een ander groot bedrijf. De enige reden dat ze deze diensten gratis of heel goedkoop kunnen aanbieden is dat ze geld verdienen aan de verkoop van jouw data.
Daar is op zich niets mis mee, als jij je daar als gebruiker maar heel bewust van bent zodat je daar rekening mee kunt houden. In dit geval, het beheer van gegevens van personen, is het niet verstandig gebruik te maken van een van deze (veelal gratis) diensten. Het is in een aantal landen niet voor niets verboden om in bijvoorbeeld de gezondheidszorg gebruik te maken van WhatsApp als communicatiemiddel met of over patiënten.
Eigenlijk bestaat er in principe geen gratis dienst of service die de data die je daar opslaat niet gebruikt voor eigen doeleinden of het verkopen aan andere

bedrijven. Betalen voor een service is daarom soms een directere manier om een dienst af te nemen. Dan weet je tevoren wat de energie uitwisseling (betaling) is.