Inhoudsopgave

[Veilig digitaal werken 2](#_Toc516487477)

[Privacy risico omlaag in 8 simpele stappen 3](#_Toc516487478)

[Privacy en datalekken 5](#_Toc516487479)

[Phishing en cybercriminaliteit 6](#_Toc516487480)

[Incidenten melden 7](#_Toc516487481)

[Tools & tips voor veilig digitaal werken 8](#_Toc516487482)

[(Eigen) mobiele apparaten 9](#_Toc516487483)

[Algemene Verordening Gegevensbescherming (AVG) 11](#_Toc516487484)

[Verwerkersovereenkomst 12](#_Toc516487485)

[Verwerkingsregister 13](#_Toc516487486)

[Data Protection Impact Assessment (DPIA) 14](#_Toc516487487)

[Functionaris gegevensbescherming 15](#_Toc516487488)

[Privacyverklaring 16](#_Toc516487489)

[Persoonsgegevens 17](#_Toc516487490)

[Rechten van betrokkenen m.b.t. persoonsgegevens 19](#_Toc516487491)

[Medische gegevens 20](#_Toc516487492)

[Personeelsdossiers 20](#_Toc516487493)

[Documenten 22](#_Toc516487494)

[FAQ 23](#_Toc516487495)

# Veilig digitaal werken

Als medewerker van een gezondheidsinstelling werk je met (bijzondere) persoonsgegevens. Hoe zorg je ervoor dat onbevoegden geen toegang hebben tot deze informatie?

**In 8 simpele stappen het privacyrisico verlagen**

Het beschermen van privacy is de verantwoordelijkheid van ons allemaal. Het is ook jouw taak om zo zorgvuldig mogelijk met persoonsgegevens om te gaan. [Hier lees je hoe je in 8 simpele stappen het privacyrisico](#_Tools_&_tips) flink kunt verlagen. Ook de poster (zie documenten) de “10 geboden informatiebeveiliging” geeft inzicht hoe hier mee om te gaan. Deze kun je ophangen in je organisatie/praktijk, zodat iedereen bekend raakt met de afspraken om veilig digitaal te werken.

**Datalekken, phishing/cybercriminaliteit en incident melding**

Ieder verlies van controle over opgeslagen persoonsgegevens is[een potentieel datalek](https://www.medewerkers.universiteitleiden.nl/ict/privacy-en-gegevensbescherming/veilig-digitaal-werken/datalekken). Het gaat in de meeste gevallen om gestolen (of verloren) digitale bestanden, maar een gestolen (of verloren) geprinte lijst met persoonsgegevens is ook een datalek. Meld een datalek altijd aan de organisatie/praktijkverantwoordelijke. Ook als er sprake is van [phishing of andere vormen van cybercriminaliteit.](#_Phishing_en_cybercriminaliteit)Wordt er al gewerkt met een VIM systeem dan kun je het melden van beveiligingsincidenten hierin ook registreren. Indien dit ontbreekt, registreer het desnoods op een andere manier, als ze maar geregistreerd worden.

**Tools & tips voor veilig werken**

[In de tools & tips voor veilig digitaal werken](#_Tools_&_tips)vind je informatie over hoe je bestanden versleutelt, welke programma’s veilig zijn en dat je bijvoorbeeld beter een wachtzin dan een wachtwoord kunt gebruiken.

**Smartphones en tablets beveiligen**

Heb je een eigen smartphone of tablet die je ook zakelijk gebruikt? [Hier lees je hoe je bestanden veilig opslaat op je mobiele apparaat en vertrouwelijke informatie beschermt](#_(Eigen)_mobiele_apparaten).

## Privacy risico omlaag in 8 simpele stappen

Als medewerker werk je hoogstwaarschijnlijk met (bijzondere) persoonsgegevens. Het is ook jouw taak om zo zorgvuldig mogelijk met deze informatie om te gaan. In de volgende 8 simpele stappen kun je het privacy risico flink verlagen.

**Stap 1. Herken (bijzondere) persoonsgegevens**

Persoonsgegevens zijn alle informatie over een persoon. Daaronder vallen niet alleen namen en adressen, maar ook BSN- bankrekeningnummers, IP-adressen, medische gegevens etc. Wees je bewust van de waarde en gevoeligheid van deze informatie voor de betrokkenen en voor kwaadwillende derden. Bijzondere persoonsgegevens, ras, afkomst en geaardheid, en medische gegvens mogen we niet zomaar verwerken. Onder de wet WGBO mogen we bijzondere gegevens zoals medische gegevens wel verwerken, alleen indien? noodzakelijk.

**Stap 2. Houd je bureau opgeruimd**

Ruim je bureau/ werkplek regelmatig op. Het klinkt simpel, maar het is een belangrijke actie die je kunt nemen om persoonsgegevens te beschermen. We hebben dagelijks te maken met allerlei persoonsgegevens. We printen ze uit, nemen ze mee naar huis of laten ze op ons bureau liggen. Iedereen die jouw kamer/ werkplek binnenkomt kan de persoonsgegevens zien. Door je bureau opgeruimd te houden, verklein je deze kans. Handiger en veiliger: niet uitprinten of onmiddellijk vernietigen na gebruik.

**Stap 3. Vergrendel je PC**

Het vergrendelen van je PC. Het is weer een simpele handeling, maar toch ontzettend belangrijk. Als je je PC niet vergrendelt is er een kans dat persoonsgegevens zichtbaar zijn voor iemand die langsloopt. Er is dan al sprake van een [datalek.](#_Privacy_en_datalekken)

**Stap 4. Verzamel zo min mogelijk persoonsgegevens**

Verzamel niet meer gegevens dan puur noodzakelijk. Door zo min mogelijk gegevens te verwerken, verkleinen we het privacy risico. Daarmee loopt je ook minder kans op een onnodige [Data Privacy Impact Assessment (DPIA).](#_Data_Protection_Impact)

**Stap 5. Opschonen verkenner: -schijf**

Op veel verkenners (schijven) staan veel persoonsgegevens die niet meer gebruikt worden. Denk aan namenlijsten van een oud evenement. Gegevens van oud sollicitanten. Deze gegevens mogen niet bewaard worden, dus verwijder ze van de -schijf. Naast het feit dat we hiermee veiliger met persoonsgegevens omgaan, levert het ook nog eens een overzichtelijkere schijf op.

**Stap 6. BCC in plaats van CC**

Als je e-mailadressen verspreidt, deel je persoonsgegevens. Maak daarom gebruik van BCC (Blind Carbon Copy) in plaats van CC. Zo verspreidt je niet onnodig e-mailadressen onder de geadresseerden.

**Stap 7. Maak gebruik van een beveiligd netwerk**

Probeer altijd alleen met een beveiligd netwerk verbinding te maken. Zoals het praktijknetwerk of je netwerk thuis, als dat goed beveiligd is. De beveiliging maakt het haast onmogelijk voor derden om het netwerkverkeer te onderscheppen. Deze kans is aanzienlijk groter wanneer je verbinding maakt met onbeveiligde, vaak vrij toegankelijke, netwerken in bijvoorbeeld cafe’s, restaurants, hotels of openbare ruimtes. Het wordt daarom sterk afgeraden om een verbinding te maken met deze netwerken. Wanneer een verbinding met het praktijknetwerk of beveiligd netwerk thuis niet mogelijk is, dan is het verbinden met een eigen mobiele hotspot een veilig alternatief.

**Stap 8. Verstuur werkmail via de organisatie/praktijk mail**

Een werkmail heeft  (als het goed is) een beveiligde mailverbinding met een eigen server. Verstuur je werkmail daarom altijd via je werk e-mailaccount. We raden af om mailservers van bijvoorbeeld Hotmail, Gmail of Yahoo te gebruiken.

## Privacy en datalekken

Ieder verlies van controle over opgeslagen persoonsgegevens is een potentieel datalek. Het gaat in de meeste gevallen om gestolen (of verloren) digitale bestanden, maar een gestolen (of verloren) geprinte lijst met persoonsgegevens is ook een datalek. Het is belangrijk dat je een datalek meld en registreert.

**Wat is een datalek?**

Ieder verlies van controle over opgeslagen persoonsgegevens is een potentieel datalek. Het gaat in de meeste gevallen om gestolen digitale bestanden, maar een gestolen geprinte lijst met persoonsgegevens is ook een datalek. Voorbeelden van datalekken zijn:

* het verlies van een USB-stick met medische gegevens of persoonsgegevens
* het verlies van het briefje met je wachtwoord dat onder je toetsenbord geplakt zit
* een gestolen laptop
* het kwijtraken van persoonsgegevens zonder dat er een back-up van aanwezig is
* brieven/ e-mails die naar de verkeerde persoon verstuurd zijn

Neem bij twijfel contact op met de [functionaris gegevensbescherming](#_Functionaris_gegevensbescherming).

**Het melden van een datalek**

Mochten persoonsgegevens onverhoopt in handen van onbevoegde derden terechtkomen? Organisaties/praktijken zijn bij wet verplicht datalekken binnen 72 uur te melden bij de Autoriteit Persoonsgegevens. Mocht er sprake zijn van een datalek, meld dit dan zo spoedig mogelijk bij je organisatieverantwoordelijke en registreer in een eventueel VIM systeem. De organisatie/praktijk verantwoordelijke kan in overleg met de [functionaris gegevensbescherming](#_Functionaris_gegevensbescherming) een melding doen.

## Phishing en cybercriminaliteit

Het is je vast weleens overkomen: je ontvangt een vreemde mail of een onduidelijk telefoontje, waarin je wordt gevraagd je persoonlijke gegevens af te geven. Klik niet op verdachte links en voer je inloggegevens niet in op verzoek van een mail: mogelijk is er sprake van phishing. Meld (mogelijke) phishing en cybercriminaliteit bij de organisatie/praktijk verantwoordelijke en registreer in een eventueel VIM systeem.

**Phishing**

Phishing is een vorm van oplichting, waarbij je per e-mail of via de telefoon gevraagd wordt om informatie. Of je klikt op een link en installeert daarmee een kwaadaardig programma (malware, virussen) op je computer.

Cybercriminelen kunnen zich voordoen als collega’s of patiënten van ons, of ze doen zich voor als betrouwbare instanties zoals Microsoft, een bank of EPD leverancier. Zij vragen jou om je inloggegevens te geven, of andere persoonlijke informatie. Vaak is het taalgebruik ook dwingend en wordt er gedreigd met blokkeren van accounts of afschrijvingen.

**Hoe kun je phishing voorkomen?**

Gelukkig kun je cybercriminelen een stap voor zijn:

* Reageer niet op e-mails waarin om persoonlijke gegevens wordt gevraagd. Open nooit zomaar bijlages of links.
* Geef nooit zo maar patiëntgegevens als daar om gevraagd wordt, denk hier goed over na.
* Geef nooit zomaar persoonsgegevens als een ogenschijnlijk betrouwbare instantie hierom vraagt. Wees hier alert op.
* Geef nooit zomaar gegevens af in een telefoongesprek dat je niet zelf begonnen bent.
* Controleer het certificaat van de website en controleer bij twijfel alle gegevens. Als de adresbalk of de tekst in de adresbalk groen is, kunt je zien of er van een beveiligde verbinding gebruik gemaakt wordt.
* Meld een phishing e-mail altijd bij de organisatie/praktijkverantwoordelijk en registreer in een eventueel VIM systeem.
* Vraagt een bekend persoon of instantie je iets ongewoons of afwijkends, wees dan alert.
* Biedt een onbekende afzender je iets aan dat te mooi is om waar te zijn, wees dan alert.
* De werkplekken binnen een organisatie/praktijk dienen voorzien te zijn van antivirussoftware. Maak ook thuis of op onbeheerde werkplekken gebruik van antivirussoftware.

**Meld phishing**

Denk je dat je te maken hebt met cybercriminaliteit? Meld dit dan bij de organisatie/praktijk verantwoordelijke en meld in een eventueel VIM systeem!

**Meld zwakke plekken in systemen**

Besteed veel aandacht aan de beveiliging van de systemen! Maar ook dan kan het toch gebeuren dat er een zwakke plek aanwezig is. Als je zo’n plek ontdekt in één van de systemen, dan is het belangrijk dit zo snel mogelijk te melden aan de organisatie/praktijkverantwoordelijke.

## Incidenten melden

Heeft er al een veiligheidsincident plaatsgevonden? Bijvoorbeeld wanneer jij of een collega van je te maken heeft gehad met een datalek, malware of phishing? Neem dan zo spoedig mogelijk contact op met de organisatie/praktijk verantwoordelijk en meld in een eventueel VIM systeem. Neem bij twijfel eerst contact op met de [functionaris gegevensbescherming](#_Functionaris_gegevensbescherming).

## Tools & tips voor veilig digitaal werken

Als medewerker werk je waarschijnlijk met persoonsgegevens. Hoe kun je ervoor zorgen dat je die zo goed mogelijk beschermt?

**E-mail sturen aan grote groep mensen**

Als je een e-mail verstuurt aan een grote groep mensen is het in het kader van de privacy belangrijk om de e-mailadressen in het bcc-veld (blind copy) te plaatsen. Hierdoor kunnen de ontvangers niet zien wie de mail nog meer heeft gekregen. Het voorkomt bovendien dat iemand per ongeluk een antwoord verstuurt naar alle geadresseerden met de ‘reply all’ optie.

**Thuiswerken**

Als je thuiswerkt gebruik dan altijd een veilige omgeving om in te loggen. Sla geen bestanden op met persoonsgegevens op een eigen/privé netwerk. Gebruik ook geen dropbox.

**Versleutel bestanden**

Het is mogelijk om bestanden met vertrouwelijke data deels of volledig te versleutelen, zodat ze alleen toegankelijk zijn met een wachtwoord. Het stappenplan hiervoor kun je vinden in het document [Handleiding omgaan met vertrouwelijke data (pdf).](#_Documenten)

**Verdachte zaken melden**

Internetcriminelen proberen soms via e-mailberichten aan je accountgegevens te komen (phishing). Bijvoorbeeld met mails die door hun lay-out een bekende organisatie/praktijk (je eigen organisatie/praktijk) als afzender lijken te hebben. Soms krijg je de vraag je accountgegevens te mailen of in te loggen op een scherm dat lijkt op een voor jou bekend inlogscherm. Beantwoord dergelijke mailberichten nooit, maar verwijder ze direct uit je mailbox.

Wil je je wachtwoord wijzigen? Klik dan nooit op een link uit een mail.

Meld verlies van vertrouwelijke gegevens altijd eerst aan de organisatie/praktijkverantwoordelijke.

**Vertrouwelijke informatie**

Digitale vertrouwelijke informatie kan worden versleuteld. Fysieke vertrouwelijke documenten horen in een afgesloten kast. Als een niet bevoegde medewerker inzage nodig heeft, mag dit alleen onder toezicht van de verantwoordelijke beheerder.

**Gebruik een 'wachtzin' in plaats van een wachtwoord**

Een simpele zin is moeilijker te kraken (en vaak makkelijker te onthouden) dan een wachtwoord, zeker als de zin ook een bijzonder teken en een getal bevat. Een wachtwoord dat een combinatie van vreemde tekens, letters en cijfers bevat, is lastig te kraken. Hieronder volgen een aantal tips voor een goed wachtwoord:

* Zorg voor een combinatie van cijfers, letters en vreemde tekens.
* Hoe langer het wachtwoord, hoe beter.
* Gebruik meerdere hoofdletters.
* Zorg dat het wachtwoord geen relatie heeft met de applicatie.
* Gebruik geen bekende uitspraken, gezegden of spreuken.
* Gebruik geen persoonlijke informatie zoals namen, geboortedatum of lijfspreuk.

**Je mobiele apparaat**

Heb je je e-mail en agenda gesynchroniseerd met je eigen smartphone of tablet? Of gebruikt je je telefoon of tablet op een andere manier zakelijk? Beveilig dit apparaat dan goed. Zorg bijvoorbeeld dat je het apparaat op afstand kunt wissen in geval van diefstal of verlies. [Meer tips lees je op de pagina over mobiele apparaten.](#_(Eigen)_mobiele_apparaten)

**Veiligheidsupdates**

Installeer op alle apparaten de nieuwste veiligheidsupdates.

Bewaar gegevens niet op losse geheugenunits zoals usb-sticks of externe harde schijven.

**Wat kun je nog meer doen?**

Je kunt zelf ook bijdragen aan het voorkomen van datalekken en een veilige werkomgeving:

* Deel je account nooit met derden.
* Houd wachtwoorden geheim en gebruik je organisatie wachtwoord niet op andere websites.
* Reageer niet op SPAM en phishing mails.
* Vergrendel je computer als je werkplek wegloopt.
* Verlies USB-sticks en externe harde schijven met vertrouwelijke informatie niet uit het oog.
* Wees alert op ransomware: open geen emailbijlages van onbekenden. Ransomware is een virus dat bestanden versleutelt en vervolgens losgeld vraagt voor de sleutel om de bestanden weer beschikbaar te maken.

## (Eigen) mobiele apparaten

Heb je een mobiel apparaat zoals een smartphone of tablet die je privé hebt aangeschaft, maar ook zakelijk gebruikt? Dan is het belangrijk om je bestanden veilig op te slaan en goed om te gaan met vertrouwelijke informatie.

**Bring Your Own Device (BYOD)**

Werken medewerkers met een eigen mobiel apparaat, zoals een laptop, smartphone of tablet. En hebben ze toegang tot informatie van de organisatie/praktijk via dat apparaat en wisselen ze informatie uit via het apparaat? Dan zijn ze verantwoordelijk voor het correct beheren van de informatie.

Het is belangrijk om bepaalde richtlijnen op te stellen. Zie hieronder:

* Je moet je apparaat op afstand kunnen wissen. Stel daarom remote wipe in. Een iPhone, iPad of MacBook kun je op afstand wissen via 'Find my iPhone'.
* Kies een sterk wachtwoord of niet eenvoudige pincode.
* Als iemand maximaal 10 keer een fout wachtwoord invoert, moet het apparaat automatisch worden gewist.
* Gebruik altijd een beveiligde omgeving voor inloggen.
* Sla niets op, op de harde schijf van het apparaat.
* Laat je apparaat nooit onbeheerd achter.
* Maak geen gebruik van bijvoorbeeld Gmail of Hotmail voor het uitwisselen van bedrijfsinformatie.
* Sla vertrouwelijke informatie niet op je apparaat, tenzij die goed genoeg is versleuteld.
* Installeer altijd de veiligheidsupdates en installeer als dat technisch mogelijk is ook antivirus- en malwaresoftware.
* Installeer geen jailbreak / root.
* Wijzig bij verlies of diefstal de betreffende wachtwoorden onmiddellijk en doe melding de organisatie/praktijkverantwoordelijke en via bijvoorbeeld een VIM systeem.

**Choose your own device (CYOD)**

Werken medewerkers met een mobiel apparaat dat voor de organisatie/praktijk is aangeschaft? Ook dan moeten ze zich aan een aantal richtlijnen te houden:

* Gebruik altijd een beveiligde omgeving om in te loggen.
* Zorg dat je apparaat geregistreerd staat bij de organisatie/praktijk (IT), zodat zij het op afstand kunnen wissen.
* Lever het apparaat in als je uit dienst gaat.
* Stel een wachtwoord of pincode in op het apparaat.
* Zorg ervoor dat er altijd een kopie van bedrijfsinformatie op de organisatie/praktijk systeem staat.
* Laat je apparaat niet onbeheerd achter.
* Wil je het apparaat meenemen op vakantie? Vraag eerst toestemming aan de organisatieverantwoordelijke.
* Gebruik geen gmail of hotmail voor het uitwisselen van bedrijfsinformatie.
* Sla geen bedrijfsinformatie met een hoog risico op, op het apparaat, tenzij het voldoende is versleuteld.
* Zorg dat je steeds de nieuwste versies van het besturingssysteem installeert.
* Installeer geen jailbreak of root.
* Meld het aan de organisatie/praktijk verantwoordelijke als het apparaat gestolen is en doe aangifte.

# Algemene Verordening Gegevensbescherming (AVG)

Vanaf 25 mei 2018 moet elke Europese organisatie/praktijk voldoen aan een nieuwe wet: de Algemene Verordening Gegevensbescherming (AVG). Of wellicht ken je de wet onder Engelse naam General Data Protection Regulation (GDPR). Wanneer je met persoonsgegevens werkt, moet je vastleggen wat er met deze data gebeurt.

**Persoonsgegevens**

Het centrale begrip van de nieuwe wet is “[persoonsgegevens](#_Persoonsgegevens)”. Wanneer je met persoonsgegevens werkt, moet je in simpel taalgebruik duidelijk en volledig kunnen uitleggen wat er binnen een organisatie/praktijk met de persoonlijke gegevens en de verwerkingen ervan gebeurt. Dat moet worden vastgelegd in het [verwerkingsregister](#_Verwerkingsregister).

**Werken met de AVG**

Op de volgende pagina's lees je meer over:

* Wat je moet doen als onbevoegden toegang hebben tot gegevens.
* Hoe je weet of je gegevens met een hoog privacyrisico verwerkt.
* Wanneer je een verwerkersovereenkomst moet opstellen.
* Of je persoonsgegevens in het verwerkingsregister moet vastleggen.

**Meer verantwoordelijkheid voor de organisatie/praktijk**

Onder de AVG krijgt je als organisatie/praktijk meer verantwoordelijkheid. Je moet zorgen voor technische en organisatorische maatregelen die veilig werken mogelijk maken.

**Meer verantwoordelijkheid voor de medewerkers**

Het beschermen van privacy is de verantwoordelijkheid van ons allemaal. Het is dus ook de taak van de medewerkers om zo zorgvuldig mogelijk met persoonsgegevens om te gaan. [Kijk welke stappen je kunt nemen om privacyrisico's te verminderen.](#_Privacyrisico_omlaag_in)

## Verwerkersovereenkomst

Schakel je een (nieuwe) partij in die voor jou persoonsgegevens verwerkt? Dan mag deze partij de gegevens niet voor eigen doeleinden gebruiken. Dat leg je vast in een verwerkersovereenkomst. In de meeste gevallen  is er inmiddels al een verwerkersovereenkomst afgesloten. Is dubbel op met stuk hieronder, misschien dit stuk weg en onderstaande alinea laten staan?

**Wanneer heb je een verwerkersovereenkomst nodig?**

Als je een andere partij inschakelt die voor jou persoonsgegevens verwerkt, bijvoorbeeld een nieuwe EPD leverancier, moet er een verwerkersovereenkomst zijn. Daarin staat dat de andere partij de persoonsgegevens niet voor eigen doeleinden mag gebruiken en een [datalek](#_Privacy_en_datalekken) direct moet melden.

Voor standaardapplicaties die persoonsgegevens verwerken heb je inmiddels al een verwerkersovereenkomst afgesloten. Schakel je een nieuwe partij in of twijfel je of er al een verwerkersovereenkomst is met een partij? Neem contact op met [de functionaris gegevens bescherming.](#_Functionaris_gegevensbescherming)

**Wat moet er in een verwerkersovereenkomst staan?**

Je kunt gebruik maken van het standaard model verwerkersovereenkomst (BOZ), dat onder [documenten](#_Documenten) te vinden is. Leg het BOZ model naast de toegestuurde overeenkomst.

##

## Verwerkingsregister

Als organisatie/praktijk moet je een centrale administratie van verwerkingen van persoonsgegevens onderhouden. Die administratie is het verwerkingsregister.

**Verwerkingsregister**

Als organisatie/ praktijk moet je een centrale administratie van verwerkingen van persoonsgegevens onderhouden. Dan kun je aantonen dat je de technische en organisatorische maatregelen neemt om persoonsgegevens te beschermen. Dat gebeurt in het verwerkingsregister. Daarin wordt vastgelegd:

* welke persoonsgegevens worden verwerkt
* met welk doel deze persoonsgegevens worden verwerkt
* waar de gegevens vandaan komen
* met wie de gegevens worden gedeeld
* risicovolle verwerking van persoonsgegevens

In sommige gevallen levert gegevensverwerking een hoog privacyrisico op voor de betrokkenen. Dat is in ieder geval zo als:

* je op grote schaal gegevens verwerkt
* je [gevoelige persoonsgegevens](https://www.medewerkers.universiteitleiden.nl/ict/privacy-en-gegevensbescherming/persoonsgegevens/persoonsgegevens) verwerkt
* de verwerking een hoog risico voor de betrokkenen met zich meebrengt

Om te bepalen of de verwerking een verhoogd risico heeft, is een formulier met 9 vragen ontwikkeld. Vraag  [de functionaris gegevensbescherming](#_Functionaris_gegevensbescherming)om dit formulier en ondersteuning hierbij.

## Data Protection Impact Assessment (DPIA)

Wanneer er een hoog privacyrisico is, moet je vooraf onderzoek doen naar de (mogelijke) risico’s. Zo’n onderzoek heet een Data Protection Impact Assessment (DPIA), ook wel gegevensbeschermingseffectbeoordeling genoemd. Een DPIA moet schriftelijk worden vastgelegd en in ieder geval de volgende elementen bevatten:

* Een systematische beschrijving van de verwerkingen en hun doelen.
* Een beoordeling van de proportionaliteit van de verwerkingen.
* Een inventarisatie van de risico’s voor betrokkenen.
* Een opsomming van de genomen maatregelen om de geconstateerde risico’s te matigen.
* Wat doen wij met risicovolle verwerkingen?
* Wanneer moet ik iets doen met risicovolle verwerkingen?

Een DPIA hoeft alleen plaats te vinden voor nieuwe verwerkingen na 25 mei 2018. Verwerkingen die dus al plaatsvonden voor deze datum daarvoor hoeft heen DPIA uitgevoerd te worden. Raadpleeg voor een DPIA je functionaris gegevensbescherming. Die kan hierin ondersteunen.

## Functionaris gegevensbescherming

De zorggroep heeft een functionaris gegevensbescherming (FG) aangesteld. Dat is een onafhankelijke privacy expert, die toezicht houdt op de toepassing en naleving van de privacywet. Alle huisartsenpraktijken binnen de regio kunnen na aanmelding gebruik maken van deze functionaris gegevensbescherming.

Deze functionaris:

* Houdt toezicht op de naleving van de wettelijke regels.
* Initieert en laat risico-analyses en privacy-audits uitvoeren.
* Adviseert de organisatie/praktijkverantwoordelijke.
* Handelt vragen en klachten van mensen binnen en buiten de organisatie/praktijk af.

De functionaris voor gegevensbescherming is Vanessa van Vliet, telefoonnummer 06-52611212 e-mail FG@gezondrivierenland.nl.

Als je gebruik wilt maken van de functionaris gegevensbescherming kun je contact opnemen met Vanessa van Vliet. Grotere organisaties die verplicht zijn om een FG te hebben, kunnen dit vervolgens melden aan de Autoriteit Persoonsgegevens via onderstaande link.

<https://www.autoriteitpersoonsgegevens.nl/nl/aanmeldenfg>

##

## Privacyverklaring

Als organisatie/praktijk ben je wettelijk verplicht patiënten duidelijk te informeren over welke privacygevoelige gegevens je verzamelt en met welk doel. Ook als dat doel alleen maar het vastleggen van hun gegevens in het EPD is. Dit volgt uit AVG. In de privacyverklaring staat dit beschreven. Onder [documenten](#_Documenten) vind je het LHV voorbeeld van een privacyverklaring welke je kunt gebruiken.

## Persoonsgegevens

Als medewerker werk je waarschijnlijk met persoonsgegevens. Persoonsgegevens zijn niet alleen namen en telefoonnummers, maar bijvoorbeeld ook cookies. Hoe kun je ervoor zorgen dat je als organisatie/ praktijk privacy proof werkt?

**Persoonsgegevens**

Persoonsgegevens zijn alle gegevens die terug te leiden zijn tot een persoon. Het gaat bijvoorbeeld om, naam, adres en woonplaats, maar ook om BSN- en bankrekeningnummers, telefoonnummers en postcodes met huisnummers.

Per 25 mei 2018 zijn ook cookies, gegevens gekoppeld aan IP-adressen en MAC-adressen, persoonsgegevens. Houd er dus rekening mee dat data sneller privacygevoelig is. Mocht je op je website gebruik maken van cookies, dan moet je hier op je website toestemming voor vragen.

**Bijzondere (gevoelige) persoonsgegevens**

Gevoelige gegevens zoals iemands ras, godsdienst of gezondheid worden bijzondere persoonsgegevens genoemd. Die zijn door de wetgever extra beschermd.

**4 tips voor gebruik van persoonsgegevens**

**Tip 1. Verzamel zo min mogelijk persoonsgegevens**

Bedenk bij het vragen naar persoonsgegevens welke er precies nodig zijn. Is het bijvoorbeeld nodig om persoonsgegevens te verzamelen die te herleiden zijn naar een natuurlijk persoon? Regel is: hoe minder, hoe beter. En des te minder kans op een onnodige? [Data Privacy Impact Assessment (DPIA) en/of datalek.](#_Data_Protection_Impact)

**Tip 2. Vraag toestemming**

Het vastleggen van medische gegevens voor het uitvoeren van een behandeling is geregeld via de WBGO. Hiervoor hoef je geen toestemming te vragen. Maar voor gegevens die niet gebruikt worden voor de zorgverlening daarvoor moet je wel toestemming vragen. Zoals bijvoorbeeld het vastleggen van persoonsgegevens van personeelsgegevens op een intranet site. Ook voor het vastleggen van foto’s moet wel toestemming gevraagd worden.

**Tip 3. Werk veilig**

Zorg dat persoonsgegevens niet in handen komen van onbevoegde derden. [Lees hoe je makkelijk persoonsgegevens kunt beschermen.](#_Privacyrisico_omlaag_in)

**Tip 4. Vernietig of anonimiseer persoonsgegevens als die niet meer nodig zijn.**

**Toestemming voor het werken met persoonsgegevens**

Is het voor je werkzaamheden noodzakelijk dat er persoonsgegevens worden verzameld? In de wet vind je een aantal grondslagen waarop dat kan:

* Je hebt [toestemming van de betrokken persoon](https://www.medewerkers.universiteitleiden.nl/ict/privacy-en-gegevensbescherming/persoonsgegevens/informed-consent).
* De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst.
* De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting bijvoorbeeld WGBO medische gegevens
* De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen.
* De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
* De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

Eén van bovenstaande grondslagen is voldoende grondslag voor het gebruik van persoonsgegevens. Voor het werken met bijzondere (gevoelige) persoonsgegevens moet je je ook nog kunnen beroepen op een wettelijke uitzondering.

**Een datalek. Wat nu?**

Mochten persoonsgegevens onverhoopt toch in handen van onbevoegde derden terechtkomen? Doordat je laptop bijvoorbeeld gestolen is? Je moet [datalekken](https://www.medewerkers.universiteitleiden.nl/ict/privacy-en-gegevensbescherming/veilig-digitaal-werken/datalekken) zo spoedig mogelijk melden bij de organisatie/praktijk verantwoordelijk. Neem bij twijfel contact op met de [functionaris gegevensbeschermin](#_Functionaris_gegevensbescherming)g.

## Rechten van betrokkenen m.b.t. persoonsgegevens

Onder de Algemene verordening gegevensbescherming (AVG) krijgen mensen meer mogelijkheden om voor zichzelf op te komen als hun persoonsgegevens worden verwerkt. Hun bestaande privacy rechten worden uitgebreid en er gelden 2 nieuwe rechten. Je moet klaar zijn voor verzoeken van personen die hun rechten willen uitoefenen.

**De AVG-privacy rechten**

* Het recht op dataportabiliteit. Het recht om persoonsgegevens over te dragen (NIEUW).
* Het recht op vergetelheid. Het recht om ‘vergeten’ te worden (NIEUW).
* Recht op inzage. Dat is het recht van mensen om de persoonsgegevens die je van hen verwerkt in te zien.
* Recht op rectificatie en aanvulling. Het recht om de persoonsgegevens die je verwerkt te wijzigen.
* Het recht op beperking van de verwerking: Het recht om minder gegevens te laten verwerken.
* Het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij besluiten.
* Het recht om bezwaar te maken tegen de gegevensverwerking.

Ten slotte hebben mensen recht op duidelijke informatie over wat je met hun persoonsgegevens doet. Dit kan in een privacyverklaring (zie onder [documenten](#_Privacyverklaring)) worden toegelicht. Onder de AVG moet je aan een aantal specifieke eisen voldoen.

**Gehoor aan verzoek geven**

Je moet je systemen, processen en interne organisatie op deze rechten inrichten zodat je op de juiste manier gehoor kunt geven aan verzoeken van mensen die hun rechten uitoefenen. Hieronder vind je meer informatie over de verschillende rechten. En wanneer en hoe je daar gehoor aan moet geven.

**Recht op vergetelheid**

Mensen hebben in een aantal gevallen het recht om hun persoonsgegevens/ medische gegevens te laten wissen. Dat noemen we het 'recht op vergetelheid'.

**In welke gevallen kan ik persoonsgegevens gegevens laten wissen?**

Als een betrokkene bij je meldt dat informatie objectief onjuist, onvolledig of niet ter zake doende is, kun je die altijd laten verwijderen.

Per mei 2018 kunt je ook persoonsgegevens laten verwijderen waar sprake is van:

* Niet meer nodig. De organisatie/praktijk heeft de persoonsgegevens niet meer nodig voor de doeleinden waarvoor de organisatie/praktijk ze heeft verzameld of waarvoor de organisatie/praktijk ze verwerkt. Denk hierbij aan personeelsgegevens die verzameld zijn voor een jaarlijks uitje.
* Intrekken toestemming . De betrokkene heeft eerder (uitdrukkelijke) toestemming gegeven aan de organisatie/praktijk voor het gebruik van zijn gegevens, maar trekt die toestemming nu in.

**Bezwaar**

De betrokkene maakt bezwaar tegen de verwerking. Er geldt op grond van artikel 21 van de AVG een absoluut recht van bezwaar tegen direct marketing. En een relatief recht van bezwaar als de rechten van de betrokkene zwaarder wegen dan het belang van de organisatie/praktijk om de persoonsgegevens te verwerken.

**Onrechtmatige verwerking**

* De organisatie/praktijk verwerkt de persoonsgegevens onrechtmatig. Bijvoorbeeld omdat er geen wettelijke grondslag is voor de verwerking.
* Wettelijk bepaalde bewaartermijn
* De organisatie/praktijk is wettelijk verplicht om de gegevens na bepaalde tijd te wissen.

## Medische gegevens

**Medisch dossier**

Zorgverleners, zoals huisartsen, tandartsen en specialisten, leggen de medische gegevens van hun patiënten vast in een medisch dossier. De rechten van patiënten en plichten van zorgverleners daarbij zijn wettelijk vastgelegd.

**Dossierplicht**

Op grond van de Wet op de geneeskundige behandelingsovereenkomst (WGBO) zijn zorgverleners verplicht een medisch dossier bij te houden.

**Beveiliging**

De Algemene verordening gegevensbescherming (AVG) schrijft voor dat zorgverleners medische dossiers goed beveiligen. Zij moeten er bijvoorbeeld voor zorgen dat alleen bevoegde personen toegang hebben tot het dossier van een patiënt.

**Bewaartermijn**

De hoofdregel voor het bewaren van medische dossiers staat in de WGBO. In die wet is bepaald dat de zorgverlener het medisch dossier in principe 15 jaar moet bewaren.

Maar ook de AVG en andere specifieke wetten kunnen van toepassing zijn om te bepalen hoe lang een zorgverlener een medisch dossier moet bewaren.

## Personeelsdossiers

Als organisatie/praktijk verwerk je ook veel persoonsgegevens van je werknemers. Deze zijn vaak opgeslagen in een personeelsdossier. Werkgevers mogen alleen een personeelsdossier aanleggen als dat noodzakelijk is om een arbeidsovereenkomst uit te voeren. En zij moeten daarbij rekening houden met de privacy van hun werknemers.

**Voorwaarden personeelsdossier**

De Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) geven de voorwaarden voor het aanleggen van personeelsdossiers.

Werkgevers:

* zijn verantwoordelijk voor de juistheid en nauwkeurigheid van de gegevens in het personeelsdossier;
* mogen niet meer gegevens in het personeelsdossier vastleggen dan nodig is, en de gegevens moeten ter zake doen;
* moeten de werknemers informeren, onder andere over welke gegevens zij verzamelen, voor welke doeleinden en op basis van welke rechtsgrond;
* moeten de persoonsgegevens passend beveiligen, zodat ze niet verloren raken of in verkeerde handen terechtkomen;
* mogen de persoonsgegevens niet langer bewaren dan noodzakelijk is;
* moeten werknemers de mogelijkheid bieden hun gegevens in te zien - dit geldt in principe voor het gehele personeelsdossier - en eventueel te corrigeren, te beperken of te verwijderen;
* moeten werknemers afzonderlijk wijzen op het recht van bezwaar bij de verwerking van gegevens op grond van het gerechtvaardigd belang;
* moeten werknemers in voorkomende gevallen de mogelijkheid bieden hun recht op dataportabiliteit uit te oefenen.

#

# Documenten

* Modelverwerkingsovereenkomst BOZ
* Voorbeeld privacyverklaring LHV
* Voorbeeld procedure datalekken
* Voorbeeld verwerkingsregisters
* Voorbeeld procedure beheer verwerkingsregister
* Handleiding veilig mailen en bestanden beveiligen
* Tien geboden informatiebeveiliging

#

# FAQ

Hieronder de vragen die tot nu toe zijn gesteld.

**Moet ik een FG aanstellen?**

Een van de onduidelijkheden was nog de vraag wat onder ‘grootschalige gegevensverwerking’ moet worden verstaan. Dit om te kunnen bepalen of een zorgaanbieder een Functionaris voor de Gegevensbescherming (FG) moet aanstellen. De Autoriteit Persoonsgegevens (AP) heeft nu een duidelijk antwoord gegeven: minder dan 10.000 patiënten wordt als niet grootschalig beschouwd. Voorwaarde is wel dat er slechts één informatiesysteem wordt gebruikt. Dit betekent waarschijnlijk dat het merendeel van de huisartsenpraktijken niet verplicht is om een FG aan te stellen. Voor de gezondheidscentra moet het van geval tot geval worden bekeken. Overigens kan ook op vrijwillige basis een (gedeelde) FG worden ingezet. Deze kan helpen de organisatie AVG-proof in te richten. Voor alle duidelijkheid: de AP beschouwt de verwerking van patiëntgegevens door huisartsenposten en zorggroepen altijd  als grootschalig. Deze zorgaanbieders zijn dus zonder meer verplicht een FG aan te stellen, zelfstandig of gezamenlijk.

**Moet ik toestemming vragen voor foto’s die ik plaats van medewerkers op een beschermde intranetsite? Bijvoorbeeld van een personeelsuitje.**

Ja. Daar moet je toestemming voor vragen.

**Moet ik toestemming vragen aan de patiënt als ik zijn/haar medicatie aan een iemand anders mee geef? Of bijvoorbeeld een uitslag door geef aan de vrouw van…?**

Deze vraag heb ik meerdere keren gesteld gekregen. Je moet hier wel toestemming voor vragen. Maar dit zou ik zo praktisch mogelijk doen. Je zou tijdens het consult kunnen vragen “Is het goed dat wij de uitslag doorgeven aan uw vrouw”? Is het antwoord “ja”. Dan kun je in het dossier noteren; uitslag of medicatie mag door/ meegegeven worden aan de partner/echtgenoot.

**Verder merk ik dat het verwerkingsregister soms lastig is. Wat moet je hierover weten?**

Het verwerkingsregister is niet iets wat je eenmalig opstelt, maar een dynamische document. De AVG geeft aan wat er verplicht in moet staan. Ik zou ook niet meer dan dat registeren. Het makkelijkst is om te bedenken wat en waar je allemaal persoonsgegevens hebt opgeslagen. Dat kan een systeem zijn (het EPD, Salarisverwerkingssysteem etc). Maar het kan ook een verwerking op papier zijn, bijvoorbeeld een map met personeelsdossiers of inschrijvingen nieuwe patiënten. En ook kun je persoonsgegevens opgeslagen hebben in mapjes op de verkenner. Als je dit inventariseert ben je al een heel eind. De volgende stap is dan te bepalen of je deze gegevens allemaal nodig hebt. Soms kom je erachter dat je bepaalde gegevens (bijv CV’s) hebt opgeslagen op verschillende plekken (een map, verkenner en mail). Het verwerkingsregister moet ook bijgehouden worden en hiervoor heb je een procedure nodig.