Versie 2
16-05-2018

De Algemene Verordening Gegevensbescherming in de huisartsenpraktijk

Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming ('AVG') van toepassing. De AVG vervangt de huidige Wet bescherming persoonsgegevens ('Wbp'). In deze handleiding leggen wij uit wat dit voor u, als huisarts/praktijkhouder, en uw medewerkers betekent en wat u kunt doen om aan deze wetgeving te voldoen.

In deze handleiding geven we antwoord op de volgende vragen:

Met dank aan Van Benthem & Keulen, advocaten & notariaat voor hun advisering.

>>

1 Waar moet ik aan voldoen?

Iedereen die in zijn/haar beroepsuitoefening werkt met persoonsgegevens van anderen moet zich houden aan de privacywetgeving. Dat geldt natuurlijk ook voor u als huisarts. Zeker in het geval van gevoelige informatie zoals gezondheidsgegevens is het erg belangrijk dat er zorgvuldig wordt omgegaan met deze data.
Tot 25 mei 2018 geldt daarvoor de Wet bescherming persoonsgegevens (Wbp). Na die datum geldt de Algemene Verordening Gegevensbescherming (AVG). De AVG is op onderdelen vooral een aanscherping en aanvulling op de Wbp. Enkele onderdelen zijn geheel nieuw. De Autoriteit Persoonsgegevens (AP) is de instantie die in Nederland toeziet op naleving van de privacywetgeving.

1.1 Welke eisen blijven hetzelfde?

Hieronder volgt eerst een uitleg over wat er met inwerkingtreding van de AVG hetzelfde blijft als onder de Wbp en waar u dus nu ook al aan moet voldoen.
Daarnaast heeft u als huisarts ook nog met andere, zorgspecifieke wet- en regelgeving van doen. Deze wetten blijven ongewijzigd gelden: de Wet op de geneeskundige behandelingsovereenkomst ('WGBO'), de Wet kwaliteit klachten en geschillen zorg ('Wkkgz'), de Wet op de beroepen in de individuele gezondheidszorg ('Wet BIG'), de Wet Toelating Zorginstellingen ('WTZi'), de Wet marktordening gezondheidszorg ('Wmg') en de Zorgverzekeringswet ('Zvw').

Verplichtingen die hetzelfde blijven (of minimaal zijn aangescherpt):

- U moet patiënten **informeren** over de persoonsgegevens die u verwerkt. Daarnaast hebben patiënten het recht om u te verzoeken om **inzage** te geven in hun persoonsgegevens (medisch dossier), deze te laten **aanvullen**, **te corrigeren, te verwijderen of af te schermen**. Ook hebben patiënten het recht **bezwaar** te maken tegen de verwerking van bepaalde gegevens. Aan dit lijstje zijn twee nieuwe rechten toegevoegd die onder paragraaf 2.5 zijn beschreven.

- U mag alleen met toestemming van de patiënt elektronisch gegevens delen. Deze verplichting is onder de AVG aangescherpt, in die zin dat u de AP moet kunnen laten zien dat u die toestemming daadwerkelijk heeft. Twee van de eisen die de AVG stelt aan 'toestemming' zijn namelijk dat deze 'geïnformeerd' en 'uitdrukkelijk' gegeven is. Om geldige toestemming aan te tonen moet u dan ook kunnen laten zien op basis van welke informatie de betrokken personen de toestemming hebben gegeven. Het is dus onvoldoende om alleen de toestemming zelf vast te leggen.

- U mag niet zonder meer persoonsgegevens doorsturen naar landen **buiten de Europese Unie**. Dat geldt ook voor het toegang geven aan een persoon of rechtspersoon buiten de Europese Unie tot de door u verwerkte persoonsgegevens. Zet uw gegevens dan ook niet zomaar in de 'cloud' en overleg goed met uw IT-leverancier over wie wanneer toegang heeft.

- De meldplicht **datalekken** blijft onder de AVG grotendeels hetzelfde. Inbreuken op de beveiliging van persoonsgegevens moet u binnen 72 uur na ontdekking en onverwijld bij patiënten melden. Wel stelt de AVG strengere eisen aan de registratie die u zelf moet doen van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie kan de AP controleren of u aan de meldplicht heeft voldaan.
  Raadpleeg voor meer informatie de Handreiking Meldplicht datalekken in de eerstelijnszorg, via www.lhv.nl.

- De AP heeft de mogelijkheid om **boetes** op te leggen. Deze boete mag de AP onder de AVG zelfs direct opleggen. De boete is bovendien verhoogd naar maximaal EUR 20.000.000,- of 4% van de jaaromzet van de betreffende organisatie.

2 Wat gaat er veranderen onder de AVG?

Er gaat met de inwerkingtreding van de AVG ook wat veranderen.
De nieuwe verplichtingen zijn er vooral op gericht om:

- gegevens nog beter te beveiligen,
- patiënten meer controle te geven over hun gegevens,
- u te stimuleren om te kunnen aantonen dat u zich aan de privacywet houdt.

De belangrijkste veranderingen zijn:

2.1 De Functionaris Gegevensbescherming (FG)

In de AVG staat dat bij 'grootschalige gegevensverwerking' van bijzondere persoonsgegevens zoals gezondheidsgegevens het aanstellen van de Functionaris Gegevensbescherming ('FG') verplicht is.

Een FG controleert binnen een organisatie of de privacywetgeving wordt nagekomen, geeft advies over (verbetering van de) informatiebeveiliging & privacy en beoordeelt beveiligingsincidenten/datalekken. Daarnaast is de FG contactpersoon voor de AP en voor patiënten. De FG brengt verslag uit aan de hoogste leidinggevende binnen de organisatie. In de huisartsenpraktijk zal dat dus over het algemeen de praktijkhouder(s) zijn.

Voor een preciezere omschrijving van wat de FG behoort te weten en doen, verwijzen wij u naar het Functieprofiel FG.

De FG mag een personeelslid zijn of mag worden ingehuurd. Het is wel van belang dat de FG onafhankelijk kan handelen en deskundig is op het gebied van de wetgeving en de praktijk inzake gegevensbescherming. Dezelfde FG kan door meerdere organisaties worden ingeschakeld, waardoor zorgaanbieders een FG kunnen delen. Het is van belang dat deze in dat geval voldoende betrokken blijft bij elke organisatie, dus niet op te grote afstand staat. De FG moet immers gemakkelijk benaderbaar zijn voor patiënten.

Een FG is dus verplicht als er op grote schaal bijzondere gegevens verwerkt worden. Er is echter (op dit moment – 2018) geen duidelijke definitie van wat 'grootschalig' inhoudt. Of er sprake is van grootschalige verwerking is afhankelijk van de concrete omstandigheden, zoals het aantal betrokkenen, de hoeveelheid persoonsgegevens, de duur van de gegevensverwerking en de geografische reikwijdte van de verwerking.

Op dit moment kunnen we alleen met zekerheid stellen dat een FG niet verplicht is voor een eenmanspraktijk en wel voor ziekenhuizen. Ergens tussen deze twee uitersten ligt het kantelpunt van wel of niet 'op grote schaal' verwerken van persoonsgegevens, maar tot op heden kan niemand (ook de AP niet) aangeven waar dit kantelpunt precies ligt. Wanneer we kijken naar het aantal patiënten dat een gemiddelde huisartsenpraktijk heeft, ligt dit aantal veel dichter bij dat van een eenmanspraktijk dan bij dat van ziekenhuizen.

<< >>

Zolang geen invulling wordt gegeven aan het begrip grootschaligheid, kunt u het standpunt innemen dat uw huisartsenpraktijk geen FG hoeft aan te stellen.

2.2 Het uitvoeren van een Data Protection Impact Assessment (DPIA)

Volgens de AVG moet er in bepaalde gevallen een DPIA worden uitgevoerd. Met een DPIA worden vooraf de privacyrisico's van gegevensverwerking in kaart gebracht, bijvoorbeeld het opnemen van medische dossiers in een informatiesysteem. Om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.
U bent alleen verplicht een DPIA uit te voeren als u de manier waarop u gegevens verwerkt wijzigt. Bijvoorbeeld wanneer u een nieuw HIS aanschaft. Verder adviseert de AP voor het in kaart brengen van bestaande grootschalige gegevensverwerkingen periodiek (bijv. eens per 3 jaar) een DPIA uit te voeren

Hoe een DPIA er in de praktijk uit moet zien, is niet vastgelegd. De DPIA moet in elk geval systematisch een beschrijving bevatten van:

- de beoogde verwerkingen en de doeleinden van de verwerking (zie in dat verband ook paragraaf 2.3 over het verwerkingsregister)
- een beoordeling van de noodzaak en de evenredigheid van de verwerking in samenhang met de doeleinden;
- een beoordeling van de risico's voor de rechten en vrijheden van de patiënt;
- de maatregelen die overwogen worden om deze risico's te beheren.

De FG geeft advies over de DPIA en kan deze ook helpen uitvoeren. Blijkt uit de DPIA dat de verwerking een hoog risico oplevert voor de patiënt en kunt u dat risico niet beperken, dan dient u de AP te raadplegen voordat u met de voorgenomen verwerking start. Dit wordt een voorafgaande raadpleging genoemd. De AP beoordeelt dan of de verwerking in strijd is met de privacywetgeving en zal u schriftelijk adviseren.

2.3 Verwerkingsregister

Naast de DPIA moet u een register bijhouden van de verwerking van persoonsgegevens (van patiënten én medewerkers). De LHV heeft een Voorbeeld verwerkingsregister ontwikkeld dat u hiervoor kunt gebruiken. Dit voorbeeld vindt u in het webdossier Privacywet AVG.
In het register moet u onder meer documenteren welke persoonsgegevens u verwerkt, met welk doel u dit doet (bijv. behandeling van de patiënt of het opstellen van een factuur), wie de gegevens aan u heeft gegeven en met wie u de gegevens deelt. De AP kan deze administratie bij u opvragen.

Een samenvatting van het register kunt u gebruiken om de patiënt te informeren over de wijze waarop u omgaat met de gegevens. Het overzicht kan bovendien behulpzaam zijn bij het behandelen van inzageverzoeken van patiënten.
Als u een FG heeft aangesteld, dan kan de FG u helpen en adviseren over het invullen en bijhouden van het verwerkingsregister.

2.4 Verwerkersovereenkomst

Wanneer u persoonsgegevens (op uw instructie) laat verwerken door andere bewerkers (verwerkers) dient u een zogenaamde verwerkersovereenkomst te sluiten. Bij verwerkers moet u bijvoorbeeld denken aan uw IT-leverancier of salarisadministratie (indien deze is uitbesteed aan een derde). Dus met een ieder, anders dan uw medewerkers of ingehuurd personeel, die de toegang heeft tot de persoonsgegevens.
Om na te gaan of u in een bepaalde situatie een verwerkersovereenkomst moet afsluiten met de verwerker, kunt u gebruik maken van het Beslisschema Verwerkersovereenkomst.

Deze specifieke afspraken kunnen in een aparte overeenkomst, een verwerkersovereenkomst, worden opgenomen. De afspraken die nu al in de praktijk moeten zijn overeengekomen met de verwerker om aan de wetgeving te kunnen voldoen, moeten straks verplicht zijn opgenomen in de overeenkomst. Een goede overeenkomst die nu wordt gebruikt zal om die reden inhoudelijk niet sterk verschillen met de toekomstige verwerkersovereenkomst. Het verdient wel aanbeveling om te beoordelen of uw huidige overeenkomsten al naar de AVG verwijzen en aan de verplichtingen onder de AVG voldoen. Om dat te beoordelen, kunt u gebruik maken van de Checklist Verwerkersovereenkomst.
Een voorbeeld van een verwerkersovereenkomst die u kunt gebruiken kunt u hier vinden.

Let op: het is niet nodig een verwerkersovereenkomst te sluiten met personen die zelf bepalen hoe ze met de gegevens omgaan. U hoeft bijvoorbeeld geen verwerkersovereenkomst met ziekenhuizen, andere zorgaanbieders of huisartsen te sluiten. Zij werken namelijk niet op uw instructie. Het is wel aan te raden om afspraken te maken met deze personen, bijvoorbeeld over de verdeling van verantwoordelijkheid, wie de betrokkene informeert of beveiligingsmaatregelen met betrekking tot de uitwisseling, zodat u zeker weet dat de uitwisseling van gegevens aan de wet voldoet. Deze afspraken kunt u in een gewone overeenkomst vastleggen. Als u twijfelt of een organisatie verantwoordelijke of verwerker is, is het altijd goed om in overleg te treden met de andere organisatie om te beoordelen of zij slechts gegevens op uw instructie verwerken of dat zij zelf het doel en de middelen van de gegevensverwerking bepalen.

<< >>

2.5 Nieuwe rechten voor patiënten

De WGBO en AVG hebben beide betrekking op de privacy van patiënten. Deze wetten gelden naast elkaar en aan beide dient te worden voldaan. De WGBO is op bepaalde punten strenger dan de AVG (bijvoorbeeld met betrekking tot verwijdering van gegevens). U moet zich in een dergelijk geval aan de WGBO houden. Indien de AVG strenger is dan de WGBO en/of de bepalingen in de WGBO en de AVG strijdig zijn met elkaar, dient u hetgeen in de AVG is bepaald te volgen.

In de AVG staat dat patiënten het recht hebben om hun persoonsgegevens te verkrijgen en de gegevens aan een andere verwerkingsverantwoordelijke over te dragen. Onder de WGBO hadden patiënten al het recht om hun medisch dossier op hun verzoek over te laten dragen aan een andere huisarts. Dat verandert dus niet.
Daarnaast krijgen patiënten onder de AVG het recht om u te verzoeken de verwerking te beperken (alleen voor bepaalde doeleinden te gebruiken) indien:

- de juistheid van de gegevens wordt betwist;
- de gegevens niet mogen worden verwerkt;
- de gegevens niet meer nodig zijn of;
- de patiënt bezwaar heeft gemaakt.

Patiënten hebben ook recht op (een) kopie(ën) van hun medische gegevens. Hiervoor mag u onder de AVG geen kosten (meer) in rekening brengen. Onder de huidige Wbp mocht dit wel. Maar als een patiënt verzoekt om meer dan één kopie van alle gegevens, dan mag u hiervoor wel een redelijke vergoeding vragen.

3 Welke onduidelijkheden zijn er nog?

De AVG kent nog veel onduidelijkheden en grijze gebieden. Voorbeelden daarvan zijn:

- de definitie van grootschalige verwerking van gegevens (ofwel: wanneer het aanstellen van een FG verplicht is);
- de precieze inhoud van de taken van de FG;
- wanneer verwerking noodzakelijk is in verband met een algemeen belang op het gebied van de volksgezondheid
- wie een FG moet aanstellen.

De LHV volgt de ontwikkelingen op dit gebied op de voet en voert hier gesprekken over met de AP, zodra er meer over bekend is, informeren we u hierover via het webdossier www.lhv.nl/wet-avg.

4 Wat moet ik doen?

In deze handleiding staan veel verplichtingen. Wat moet u nu precies doen om te voldoen aan al die verplichtingen? Dit zijn volgens ons de belangrijkste stappen:

1. **Sluit verwerkersovereenkomsten af.**
2. **Houd een verwerkingsregister bij.**
3. **Voer een DPIA uit bij wijziging in de gegevensverwerking (zoals een nieuw HIS).**
4. **Publiceer een privacyverklaring (op uw praktijkwebsite).**
5. **Maak een afweging over het aanstellen van een FG.**

Over al deze stappen vindt u meer informatie in het webdossier van de LHV over de AVG.

Ook kunt u terecht bij de AP voor meer informatie en voor advies. De AP biedt op haar website informatie aan die speciaal gericht is op zorgverleners onder de noemer 'Zorgaanbieders en de AVG:

De publieksvoorlichters van de AP zijn ook telefonisch bereikbaar op telefoonnummer 0900-2001201.

BIJLAGE

Algemene bepalingen en begrippen

De AVG bevat regels voor de verwerking van persoonsgegevens. De begrippen 'persoonsgegevens' en 'verwerken' vormen ook onder de AVG de belangrijkste begrippen. Mede aan de hand van de definities van deze begrippen kunt u beoordelen of de privacyregels van de AVG op uw organisatie van toepassing zijn. De definities van deze begrippen blijven onder de AVG hetzelfde als onder de Wbp.

Persoonsgegevens: alle informatie (dat kan tekst zijn, maar mag ook een voorwerp of een foto zijn) waarmee direct of indirect een levend persoon kan worden geïdentificeerd. Enkele voorbeelden van persoonsgegevens zijn een naam, adres, een e-mailadres, een telefoonnummer, een unieke patiëntcode of een foto. Het begrip persoonsgegeven wordt ruim uitgelegd. U kunt er daarom van uitgaan dat alle gegevens die u over uw patiënten registreert in uw patiëntinformatiesysteem of administratiesysteem persoonsgegevens zijn. Daarbij geldt dat medische gegevens worden beschouwd als 'bijzondere persoonsgegevens'.

Verwerken: elke handeling met betrekking tot persoonsgegevens. Daaronder valt onder meer het verzamelen, bewaren, in de cloud plaatsen, wijzigen, raadplegen, gebruiken, verstrekken, afschermen en vernietigen van persoonsgegevens. Ook dit begrip wordt ruim uitgelegd en in principe kunt u ervan uitgaan dat alle (geautomatiseerde) handelingen onder de reikwijdte van dit begrip vallen.

Verantwoordelijke: (onder de AVG: verwerkingsverantwoordelijke) een natuurlijke of rechtspersoon die het doel van en de middelen voor de verwerking van persoonsgegevens (bijvoorbeeld medische gegevens) vaststelt. Dit kan alleen of samen met andere partijen zijn.

Grondslagen

In de basis blijven de regels met betrekking tot de verwerking van persoonsgegevens hetzelfde. De hoofdregel dat er altijd een grondslag moet zijn voor de verwerking van persoonsgegevens verandert niet.
U mag medische gegevens verwerken van uw patiënten als:

- de verwerking met het oog op een **goede behandeling** of verzorging van de patiënt, dan wel voor het **beheer van uw praktijk** noodzakelijk is; of
- de patiënt **toestemming** heeft gegeven. Toestemming (opt-in) vereist een actieve handeling van de patiënt nadat de patiënt is voorzien van voldoende informatie; of
- toestemming geven niet mogelijk is, maar er sprake is van een **kwestie van leven of dood** waarvoor de gegevens verwerkt moeten worden; of
- de verwerking noodzakelijk is voor de uitvoering van een **wettelijke verplichting**, zoals de dossierplicht waarvoor ook een wettelijke bewaartermijn van 15 jaar geldt; of
- de verwerking noodzakelijk is in verband met een **algemeen belang** op het gebied van de volksgezondheid (bijvoorbeeld bij de uitbraak van een gevaarlijke infectieziekte); of

- de verwerking noodzakelijk is voor wetenschappelijk of historisch **onderzoek** of statistische doeleinden en toestemming niet mogelijk is.

Let op: in een aantal gevallen gelden er ook **strengere regels** op grond van zorgspecifieke regelgeving. Hieronder treft u een paar voorbeelden.

- Het **beroepsgeheim**: behalve met de patiënt en personen die rechtstreeks bij de behandeling zijn betrokken, mag u de inhoud van het medisch dossier niet met anderen delen, tenzij aan een aantal strenge voorwaarden wordt voldaan.
- het **burgerservicenummer (BSN)**: het BSN van een patiënt mag alleen verwerkt worden indien u een wettelijke plicht heeft om dit te doen. Als zorgaanbieder bent u wettelijk verplicht om het BSN van een patiënt op te nemen in uw administratie, te gebruiken bij onderlinge communicatie over patiënten met andere zorgaanbieders en voor het declaratieverkeer met patiënten.

Algemene beginselen

Zowel onder de Wbp als de AVG mogen persoonsgegevens alleen worden verwerkt, indien er aan een aantal beginselen wordt voldaan. Deze worden hieronder toegelicht.

- **Rechtmatigheid, behoorlijkheid** en **transparantie**: u moet aan de wet voldoen bij de verwerking van persoonsgegevens en u moet patiënten proactief informeren over de gegevensverwerking.
- **Doelbinding**: u mag persoonsgegevens alleen verzamelen voor vooraf bepaalde en gespecificeerde doeleinden en u mag persoonsgegevens niet verder verwerken voor andere doeleinden.
- **Minimale gegevensverwerking**: alleen die gegevens die noodzakelijk zijn om de vastgestelde doeleinden te bereiken, mogen worden verwerkt.
- **Juistheid**: er moeten redelijke maatregelen worden genomen om de juistheid van de persoonsgegevens te controleren en zo nodig te actualiseren. Onjuiste gegevens moeten worden gewist of gerectificeerd.
- **Opslagbeperking**: gegevens mogen niet langer worden opgeslagen dan noodzakelijk om de vastgestelde doeleinden te bereiken.
- **Integriteit** en **vertrouwelijkheid**: er dienen passende beveiligingsmaatregelen genomen te worden. Implementatie van NEN-norm 7510 ten aanzien van informatiebeveiliging in de zorgsector is verplicht. Zorg er ook voor dat uw IT leverancier uw systemen en andere middelen waarmee u persoonsgegevens verwerkt standaard privacyvriendelijk inricht (*privacy by default*) en dat u bij de selectie van nieuwe patiëntinformatiesystemen, administratiesystemen of andere middelen waarmee u gegevens verwerkt bij de leverancier informeert of bij het ontwerp van het systeem al rekening is gehouden met de privacyregels (*privacy by design*). Deze principes waren al van belang onder de huidige wetgeving, maar worden verplicht onder de AVG.

<< >>

Als zorgaanbieder bent u ervoor verantwoordelijk dat uw medewerkers en (IT)-leveranciers deze beginselen nakomen en dient u dit te kunnen aantonen *(accountability)*. Zie in dat kader ook de toelichting op de verwerkersovereenkomst onder 2.4.