ALGEMENE VERORDENING **GEGEVENS-BESCHERMING**

DE GEVOLGEN VAN **AVG** VOOR DE APOTHEEK

MEI 2018

KONINKLIJKE NEDERLANDSE MAATSCHAPPIJ TER BEVORDERING DER PHARMACIE

KNMP

APOTHEKERSORGANISATIE

ALGEMENE VERORDENING **GEGEVENSBESCHERMING**

NIEUWE PRIVACYWETGEVING

PER 25 MEI 2018 IS DE ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG) VAN TOEPASSING. DAT BETEKENT DAT ER VANAF DIE DATUM DEZELFDE PRIVACYWETGEVING GELDT IN DE EUROPESE UNIE (EU). DE WET BESCHERMING PERSOONSGEGEVENS (WBP) GELDT DAN NIET MEER. DEZE BROCHURE LEGT UIT WAT DIT VOOR DE APOTHEEK BETEKENT EN WAT DE APOTHEEK KAN DOEN OM TE VOLDOEN AAN DEZE WETGEVING.

Een van de belangrijkste veranderingen is Functionaris voor de Gegevensbescherming (FG). Het aanstellen van een FG is verplicht als op grote schaal bijzondere persoonsgegevens worden verwerkt. De apotheker kan aan de hand van vier factoren bepalen of het aanwijzen van een FG noodzakelijk is. Op pagina 6 van deze brochure wordt dit verder toegelicht.

Deze brochure is de derde versie. In de komende periode verheldert onder andere de Autoriteit Persoonsgegevens (AP) nog meer onduidelijkheden van de nieuwe wet. De KNMP brengt daarna een volgende versie uit, waarbij de wijzigingen duidelijk zijn weergegeven. Zo heeft u altijd alle informatie over de AVG overzichtelijk bijeen

De praktische hulpmiddelen die de KNMP voor u heeft ontwikkeld, zijn te vinden op de pagina ‘Praktische hulpmiddelen AVG’.

Deze brochure geeft antwoord op de volgende vragen:

1. WAT BLIJFT HETZELFDE ONDER DE AVG?

Inhoudelijk wijzigt met de inwerkingtreding van de AVG de systematiek van de Wbp niet principieel. De AVG is op onderdelen vooral een aanscherping en aanvulling op de Wbp. Daarom volgt eerst uitleg over wat er met de AVG in elk geval niet verandert en welke vereisten ook nu al gelden.

Met de AVG blijft de (inhoud van de) reeds bestaande zorgspecifieke wet- en regelgeving ongewijzigd. Dit betekent onder meer dat 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 (de Wmg) en de Wet op de geneeskundige behandelingsovereenkomst (WGBO) onveranderd blijven. In het Overzicht wetgeving informatieveiligheid en privacy is aanverwante wetgeving kort toegelicht en uitgelicht wat relevant is voor informatieveiligheid en privacy. Naast de AVG is er zorgspecifieke wet- en regelgeving voor de elektronische verwerking en uitwisseling van medische gegevens. Dit betreft de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (voorheen: Wet gebruik burgerservicenummer in de zorg) en het Besluit elektronische gegevensverwerking door zorgaanbieders.

De zorgspecifieke regelgeving kent op een aantal onderdelen een strenger regime voor gegevensbescherming dan de AVG. Daarbij gaat het bijvoorbeeld om regels over het beroepsgeheim, mogelijkheid tot weigering verzoek verwijdering of rectificatie en de mogelijkheden tot het verwerken van het BSN-nummer van patiënten.

Verplichtingen die hetzelfde blijven of minimaal zijn aangescherpt:

- U ziet erop toe dat de leverancier van de 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, informeert of bij het ontwerp van het systeem al rekening is gehouden met de privacyregels (privacy by design). Deze principes waren al van belang en worden expliciet verplicht onder de AVG

- U informeert patiënten over de persoonsgegevens die u verwerkt. Daarvoor heeft u een privacyverklaring van uw apotheek (bijvoorbeeld op de website) beschikbaar. Patiënten hebben het recht op **inzage** in hun persoonsgegevens, deze te laten **aanvullen, corrigeren, verwijderen of af te schermen**. Daarnaast 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 bent verplicht om binnen één maand aan te geven of, dan wel in hoeverre, u aan een dergelijk verzoek gaat voldoen.

- U mag niet zomaar 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 hebben. Zie ook de Praktijkgids Patiëntgegevens in de cloud van de AP (2017).

- Inbreuken op de beveiliging van persoonsgegevens (**datalekken**) meldt u bij de Autoriteit Persoonsgegevens (AP) binnen 72 uur na ontdekking en vaak ook bij patiënten. Zie voor meer informatie de KNMP handreiking meldplicht datalekken. Indien er sprake is van verlies, ongeautoriseerde toegang of diefstal van patiëntgegevens kunt u ervan uitgaan dat u dit datalek hoort te melden bij de AP en patiënt(en). De AVG verplicht dat alle datalekken in uw apotheek vastgelegd zijn, ook als het gaat om kleine kwesties die niet bij de AP gemeld worden.

- Tenslotte behoudt de AP de mogelijkheid om boetes op te leggen. Deze boete mag de AP onder de AVG direct opleggen en het maximum bedrag is verhoogd naar EUR 20.000.000,- of 4% van de wereldwijde jaaromzet.

2. WAT IS VERANDERD ONDER DE AVG?

Er gaat met de inwerkingtreding van de AVG ook wat veranderen. In essentie zijn de nieuwe verplichtingen er vooral op gericht om (1) gegevens beter te beveiligen, (2) patiënten meer controle te geven over hun gegevens en (3) u te stimuleren gericht beleid te maken op het gebruik en de verwerking van persoonsgegevens. De belangrijkste veranderingen zijn:

2.1 Functionaris voor de Gegevensbescherming (FG)

Volgens de AVG is het aanstellen van een Functionaris Gegevensbescherming (FG) verplicht als op grote schaal bijzondere persoonsgegevens worden verwerkt. De apotheker kan aan de hand van vier factoren bepalen of het aanwijzen van een FG noodzakelijk is: (1) het aantal patiënten, (2) de hoeveelheid gegevens, (3) de duur van de gegevensverwerking, (4) de geografische reikwijdte. Een uitgebreidere omschrijving van de vier factoren is beschikbaar op de KNMP-site.

Als de apotheek van mening is dat een FG niet noodzakelijk is, moet de apotheker dit goed uit kunnen leggen. De AP hecht groot belang aan aantoonbare inspanningen. De aanbeveling luidt dan wel om iemand binnen de organisatie verantwoordelijk te maken voor privacy. Het profiel van deze rol kan dan erg lijken op die van de verplichte FG, maar de apotheker heeft dan meer flexibiliteit in de daadwerkelijke invulling van de rol.

De AP kent voorbeelden waarbij geen FG vereist is, zoals voor de individuele arts. Daartoe behoort de apotheek niet. Een individuele arts is namelijk een zorgaanbieder bestaande uit één persoon die persoonsgegevens verwerkt zonder medewerkers.

De FG controleert of de privacywetgeving wordt nagekomen, geeft advies, maakt inventarisaties van de gegevensverwerkingen en houdt deze bij. Daarnaast is de FG contactpersoon voor de AP en patiënten. De FG brengt verslag uit aan de apotheekeigenaar.

De FG mag een personeelslid zijn of op basis van een servicecontract met een persoon of organisatie (met een team van FG's) worden ingehuurd. Het is van belang dat de FG onafhankelijk kan handelen en deskundig is op het gebied van de wetgeving en de praktijk inzake gegevensbescherming. Eén FG kan door meerdere organisaties worden ingeschakeld, waardoor apotheken of andere zorgaanbieders ook een FG kunnen delen. Het is wel van belang dat deze makkelijk bereikbaar is en voldoende betrokken blijft iedere apotheek. Het profiel van een FG en de verschillende mogelijkheden bij het aanstellen van een gedeelde FG staat nader toegelicht op de KNMP-site.

2.2 Privacy Impact Assessment (PIA)[1]

Met een PIA worden vooraf de privacyrisico's van gegevensverwerking (bijvoorbeeld het opnemen van medische dossiers in een informatiesysteem) in kaart gebracht. Om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

De apotheek is verplicht om een PIA uit te voeren bij wijzigingen in gegevensverwerking als dit waarschijnlijk een verhoogd risico met zich meebrengt. Dit kan bepaald worden aan de hand van een lijst met criteria, die door de Europese werkgroep (WP29) zijn opgesteld. Bijvoorbeeld bij het gebruik van nieuwe technologieën.

1) In de wet wordt de term data protection impact assessment (DPIA) gebruikt of, in de Nederlandse vertaling, gegevensbeschermingseffectbeoordeling (GEB)

De apotheek kan ervoor kiezen om de uitvoering van de PIA uit te besteden, maar blijft wel verantwoordelijk. Als de apotheek dit zelf uitvoert, kan zij dit samen met de FG doen of de FG vragen voor advies en toe te zien op de uitvoering. Als een verwerker (bv. een AIS/IT-leverancier, zie paragraaf 2.4) betrokken is bij de verwerking, dan dient de leverancier daarbij te voorzien in relevantie informatie, zoals de gebruikte technieken en mogelijke risico's daarvan. Hoe een PIA er in de praktijk uit hoort te zien is niet vastgelegd. Wel zijn er criteria opgesteld door de Europese Werkgroep (WP29) voor de AVG om te voldoen aan de vereisten die zijn gesteld (Bijlage 2, Nederlandse vertaling guidelines DPIA, AP). Een handreiking voor het uitvoeren van een PIA is beschikbaar op de KNMP-site.

Bij het uitvoeren van een PIA is het handig om alle relevante informatie over de huidige situatie te gebruiken en waar nodig aan te passen aan de toekomstige situatie. Denk bijvoorbeeld aan het verwerkingsregister (zie paragraaf 2.3), beschrijving van gebruikte technologie/software, en onderzoeken en richtlijnen van de AP.

Blijkt uit de PIA dat de (gewijzigde) verwerking een hoog risico oplevert voor de patiënt en kunt u dat risico niet beperken, dan is een voorafgaande raadpleging benodigd. Voordat u met de voorgenomen verwerking start, raadpleegt u zelf of uw FG de AP. De AP beoordeelt dan of de verwerking in strijd is met de privacywetgeving en adviseert hierover schriftelijk.

2.3 Verwerkingsregister

De apotheek is verantwoordelijk voor de naleving van de AVG en behoort dit aan te kunnen tonen ('verantwoordingsplicht'). Dat doet de apotheek door een register bij te houden van de verwerking van patiëntgegevens. De FG kan daarbij adviseren en/of mee helpen. Kan de apotheek niet voldoen aan de verantwoordingsplicht, dan kan de AP een boete opleggen aan de apotheek.

In het register documenteert u onder meer welke categorie persoonsgegevens (bijvoorbeeld medische gegevens) u verwerkt, met welk doel (bijvoorbeeld behandeling van de patiënt of het opstellen van een factuur), wie (bijvoorbeeld patiënten of andere zorgverleners) de gegevens aan u heeft gegeven en met wie u de gegevens deelt (bijvoorbeeld andere zorgverleners of factoring bedrijf). In het register staat ook steeds vermeld waarom u de gegevens mag gebruiken op grond van de AVG (bijvoorbeeld omdat u wettelijk verplicht bent de gegevens te verwerken of de verwerking noodzakelijk is met het oog op de behandeling van de patiënt). Het is van belang dat u dit goed kunt onderbouwen. De AP kan deze administratie bij u opvragen. Het register bevat dus geen namen van patiënten en andere zorgverleners, de benoeming van een categorie is voldoende.

Een samenvatting van het register kunt u gebruiken voor de privacyverklaring, om de patiënt te informeren over de wijze waarop u omgaat met de gegevens. Ook kunt u het overzicht gebruiken indien de patiënt inzage wil in zijn gegevens of u vraagt bepaalde soort gegevens te corrigeren, te verwijderen, aan te vullen, te beperken of door te geven aan een andere zorgaanbieder.

De KNMP heeft een voorbeeld register (inclusief toelichting) opgesteld en beschikbaar gesteld op de KNMP-site dat u kunt aanvullen met de informatie specifiek voor uw apotheek.

2.4 Verwerkersovereenkomst

Wanneer de apotheek persoonsgegevens (op uw instructie) laat verwerken door andere verwerkers (voorheen bewerkers), dan dient de apotheek hierover afspraken vast te leggen. Denk bijvoorbeeld aan uw AIS/IT-leverancier of salarisadministratie (indien deze is uitbesteed aan een derde partij). Dus met een ieder, anders dan de medewerkers of ingehuurd personeel, die toegang heeft tot de persoonsgegevens. Deze specifieke afspraken kunnen in een aparte overeenkomst, zogenoemde verwerkersovereenkomst (voorheen bewerkersovereenkomst), of in een bestaande overeenkomst worden opgenomen. De mondelinge of schriftelijke afspraken die nu al gemaakt met destijds de bewerker om aan de wetgeving te voldoen, neemt u ook op in de overeenkomst. Heeft u nu al een goede overeenkomst waarin alle afspraken zijn vastgelegd, dan gaat die inhoudelijk niet sterk verschillen met de verwerkersovereenkomst. Controleert u wel of in uw huidige overeenkomsten de verplichtingen uit de AVG voldoende zijn beschreven.

Let op: Het is niet nodig om een verwerkersovereenkomst af te sluiten met partijen die niet onder uw verantwoordelijkheid vallen. Denk aan ziekenhuizen of andere zorgaanbieders in de eerste lijn waar u medicatiegegevens mee uitwisselt. Dat geldt ook voor de Vereniging van zorgaanbieders voor zorgcommunicatie (VZVZ) voor gebruik van het LSP. Het is wel aan te raden om dan afspraken te maken over de verdeling van verantwoordelijkheid, wie de betrokkene (bijvoorbeeld over een datalek of ingediend verzoek van de betrokkene) informeert of beveiligingsmaatregelen met betrekking tot de uitwisseling, zodat u zeker weet dat aan de wet

wordt voldaan. Deze afspraken kunt u in een gewone overeenkomst vastleggen. Indien u twijfelt of een partij verantwoordelijke of verwerker is, beoordeel dan samen met de betreffende organisatie wat de verdeling van de verantwoordelijkheid is.

Op de KNMP-site is een beslisboom beschikbaar die helpt beoordelen met welke partij een verwerkersovereenkomst nodig is. Daarbij is ook een modelovereenkomst beschikbaar gesteld.

2.5 Nieuwe rechten voor patiënten

Op verzoek van de patiënt draagt u het dossier over aan een andere zorgaanbieder. Dit geldt ook onder de WGBO, waarbij tevens de patiënt recht heeft op inzage in zijn medisch dossier en het recht heeft eventueel een afschrift te ontvangen. Onder de AVG mogen hier geen kosten voor in rekening gebracht worden. Daarnaast bent u verplicht om een deel van het medisch dossier digitaal over te dragen aan de patiënt ('recht op dataportabiliteit'). Dat geldt voor de persoonsgegevens die uw patiënt zelf actief en bewust heeft verstrekt en voor de gegevens die de patiënt indirect heeft verstrekt door het gebruik van een dienst of een apparaat. Bijvoorbeeld de gegevens die een pacemaker of een bloedrukmeter genereert.

Daarnaast krijgen patiënten onder de AVG het recht om u te verzoeken de verwerking te beperken (alleen voor bepaalde doeleinden te gebruiken) indien (1) de juistheid van de gegevens wordt betwist, (2) de gegevens niet mogen worden verwerkt, (3) de gegevens niet meer nodig zijn of (4) de patiënt bezwaar heeft gemaakt.

De WGBO en AVG kennen beide rechten met betrekking tot patiënten. Deze wetten gelden naast elkaar. Wanneer er verschil is tussen de wetten, volgt u altijd de striktste wetgeving.

	VOORBEELDEN
WGBO strikter dan AVG	- Mogelijkheid tot afwijzen verzoek tot verwijdering, bijvoorbeeld wanneer dit goed hulpverlenerschap in de weg staat. - Informatieplicht van de patiënt - Bewaartermijn, zoals van recepten (20 jaar) en declaraties (7 jaar).
AVG strikter dan WGBO	- Recht op overdraagbaarheid, zodat gegevens gestructureerd, gangbaar en digitaal overgedragen kunnen worden ('dataportabiliteit'). - De AP kan bestuurlijke boetes direct opleggen. - Kennisgevingsplicht aan iedere ontvanger van persoonsgegevens inzake wissing, beperking, vergetelheid

3. ONDUIDELIJKHEDEN

De AVG kent nog veel onduidelijkheden en grijze gebieden. Voorbeelden daarvan zijn (1) 'kennisgevingsplicht' binnen de zorg en verhouding met WGBO, (2) verwerkingen waarvoor een PIA verplicht is en waar de AP nog een lijst voor opstelt, (3) wanneer verwerking noodzakelijk is in verband met een algemeen belang op het gebied van de volksgezondheid, en (4) wat precies onder 'grootschalig' wordt verstaan. In de Tweede Kamer is in maart 2018 een motie aangenomen waarin wordt gevraagd om verduidelijking van het begrip 'grootschalige verwerking'. Uitleg van dit begrip moet in heel Europa gelijk zijn, daarom zal de AP met andere toezichthouders in Europa overeenstemming moeten bereiken. Een duidelijk 'afkappunt' is dus nog niet te geven. Op sommige punten zullen richtsnoeren worden opgesteld door de AP of de gezamenlijke Europese toezichthouders. Andere punten zullen pas duidelijk worden nadat er over is geprocedeerd. De KNMP houdt de ontwikkelingen in het oog en past deze brochure aan wanneer praktische informatie beschikbaar komt.

4. ALGEMENE BEPALINGEN EN BEGRIPPEN

De Wbp en de AVG bevatten regels voor de verwerking van persoonsgegevens. De begrippen 'persoonsgegevens', 'verwerken' en 'verantwoordelijke 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) 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.

Verwerken: elke handeling met betrekking tot persoonsgegevens. Daaronder vallen 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 natuurlijk 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 zijn.

Aanleiding

In de basis blijven de regels met betrekking tot de verwerking van persoonsgegevens hetzelfde. De hoofdregel dat er altijd een aanleiding moet zijn voor de verwerking van persoonsgegevens verandert niet. Medische gegevens vallen onder de categorie bijzondere persoonsgegevens en mag u van uw patiënten verwerken indien:

- de verwerking voor een **goede behandeling** of verzorging van de patiënt, dan wel voor het **beheer van uw praktijk**, noodzakelijk is;

- de patiënt mondeling of schriftelijk **toestemming** heeft gegeven voor het verwerken van een dossier. Toestemming voor uitwisseling met andere zorgverleners (opt-in) vereist een actieve handeling van de patiënt nadat de patiënt is voorzien van voldoende informatie;

- toestemming geven niet mogelijk is, maar er sprake is van een **kwestie van leven of dood** waarvoor de gegevens verwerkt moeten worden. Dat geldt echter niet voor uitwisseling met andere zorgverleners. Daarvoor is alsnog toestemming van de patiënt nodig;

- de verwerking noodzakelijk is voor de uitvoering van een **wettelijke verplichting**, zoals de dossierplicht, waarvoor ook een wettelijke bewaartermijn van 20 jaar geldt;

- de verwerking noodzakelijk is in verband met een **algemeen belang** op het gebied van de volksgezondheid (bijvoorbeeld bij de uitbraak van een gevaarlijke infectieziekte);

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

Let op: zoals aangegeven gelden er in een aantal gevallen **strengere regels** op grond van zorgspecifieke regelgeving. 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 (bijvoorbeeld meldplicht kindermishandeling) wordt voldaan. Zie KNMG-richtlijn ‘Omgaan met medische gegevens’.

- 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 als aan een aantal beginselen wordt voldaan:

- **Rechtmatigheid, behoorlijkheid** en **transparantie**: u bent verplicht om aan de wet te voldoen bij de verwerking van persoonsgegevens en u dient patiënten proactief te 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**: enkel de gegevens die noodzakelijk zijn om de vastgestelde doeleinden te bereiken, mogen worden verwerkt.

- **Juistheid**: er dienen redelijke maatregelen te worden genomen om de juistheid van de persoonsgegevens te controleren en zo nodig te actualiseren. Onjuiste gegevens behoren te worden gewist of gerectificeerd.

- **Opslagbeperking**: gegevens mogen niet langer worden opgeslagen dan noodzakelijk om de vastgestelde doeleinden te bereiken.

- **Integriteit en vertrouwelijkheid**: een informatieveiligheidsbeleid dient aanwezig te zijn. Hierin dienen passende beveiligingsmaatregelen voor bescherming van persoonsgegevens opgenomen en toegepast te zijn. Het ministerie van VWS stelt de **NEN-normen 7510**, **7512** en **7513** kosteloos beschikbaar om te bewerkstelligen dat de gegevens beter worden beschermd, met name het BSN. Implementatie van NEN-norm 7510 is verplicht.

Als apotheekeigenaar bent u ervoor verantwoordelijk dat uw medewerkers en (IT) leveranciers deze beginselen nakomen (accountability). Zie in dat kader ook de toelichting op de verwerkersovereenkomst onder 2.4.

5. AFKORTINGEN

AIS	Apotheek Informatie Systeem
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BSN	Burgerservicenummer
FG	Functionaris voor de gegevensbescherming
GEB	Gegevensbeschermingseffectbeoordeling
IT	Informatie Technologie
LSP	Landelijk Schakelpunt
NEN	NEderlandse Norm
PIA	Privacy Impact Assessment
VZVZ	Vereniging van Zorgaanbieders voor Zorgcommunicatie
Wbp	Wet bescherming persoonsgegevens
Wet BIG	Wet op de beroepen in de individuele gezondheidszorg
WGBO	Wet op de geneeskundige behandelingsovereenkomst
Wkkgz	Wet kwaliteit klachten en geschillen zorg
Wmg	Wet marktordening gezondheidszorg
WTZi	Wet toelating Zorginstellingen

6 COLOFON

Dit is een productie van de KNMP
Advies: Van Benthem & Keulen, advocaten & notariaat

Bronnen:
Website en richtlijnen van de AP
Richtlijnen WP29, onafhankelijke advies -en overlegorgaan van Europese privacytoezichthouders.
Handreiking Privacy Impact Analyse (PIA) van NOREA

Uitgave Mei 2018, versie 1.2

Wilt u meer informatie over de AVG? Zie ook de website van de Autoriteit Persoonsgegevens hier.

Versie	Wijzigingen
v1.0	• Eerste versie
v1.1	• Algemeen: verwijzing naar alle praktische hulpmiddelen die ontwikkeld zijn • Algemeen: verwijzing naar overzicht wet- en regelgeving Informatieveiligheid en Privacy • FG: extra toelichting over de criteria voor (gezamenlijk) instellen van een FG met verwijzing naar de KNMP-site • Nieuwe rechten patiënt: toelichting over 'recht op dataportabiliteit' • WGBO strikter dan AVG: mogelijkheid tot afwijzen verzoek tot verwijdering toegevoegd. • PIA: toelichting over de uitvoering van een PIA en aan welke criteria dit aan moet voldoen. • Aanleiding: toevoeging van voorwaarde waaronder gegevens verwerkt mogen worden. Indien toestemming geven niet mogelijk is, maar er sprake is van een kwestie van leven of dood. • Algemene beginselen: toegelicht dat een informatiebeveiligingsbeleid aanwezig dient te zijn.
v1.2	• Aangepast advies waar op te letten bij aanstellen FG voor apotheken

KNMP
Alexanderstraat 11
2514 JLDen Haag
T 070 373 73 73
F 070 310 65 30