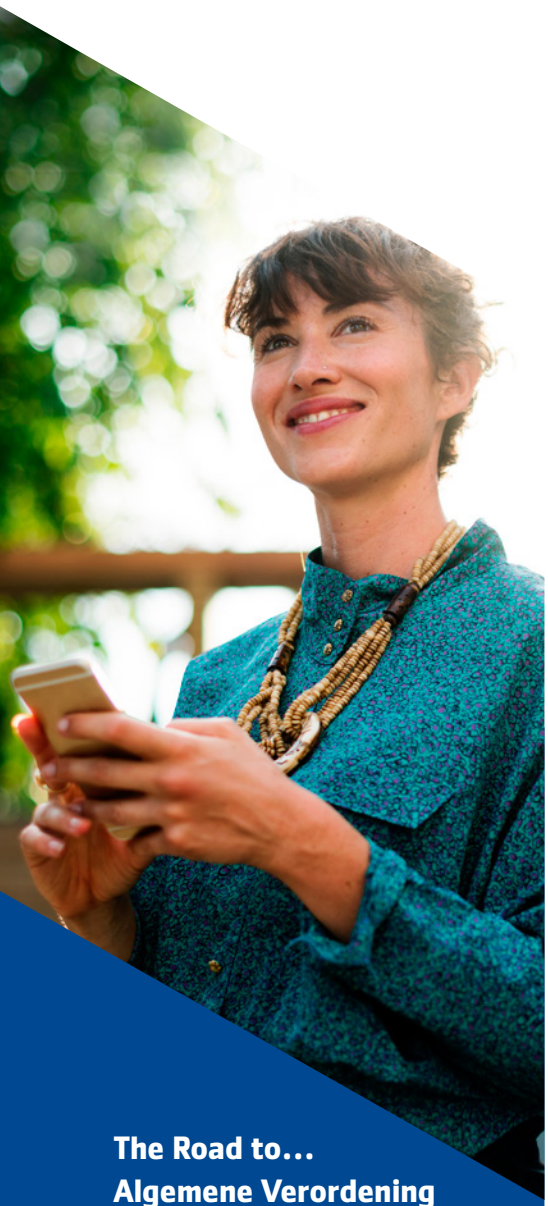
The Road to...

Algemene Verordening Gegevensbescherming

Whitepaper | PharmaPartners



The Road to...
Algemene Verordening Gegevensbescherming

Meer informatie:
www.pharmapartners.nl/wetgeving
voor vragen:
privacy@pharmapartners.nl

De Algemene Verordening Gegevensbescherming (AVG) is er al! Vanaf mei 2016 is de AVG ingevoerd. Op 25 mei 2018 gaat de Autoriteit Persoonsgegevens (AP) handhaven. En dat gaan ze zeker doen: ze investeren fors om extra controleurs aan te stellen. En omdat de AVG er feitelijk al is, zal er geen coulance zijn voor organisaties die meer tijd nodig hebben.

Iedere organisatie moet eigenlijk al concrete stappen hebben gezet op het gebied van privacy, de rechten van cliënten en de bescherming van persoonsgegevens. Nog niet begonnen? Of al in het proces maar behoefte aan een checklist? PharmaPartners helpt u graag op weg met dit stappenplan: The Road to... Algemene Verordening Gegevensbescherming.

Wat zijn de stappen?

1. **Ga na of uw praktijk of apotheek een Functionaris Gegevensbescherming moet aanstellen.**
2. **Zorg voor een kennisbasis over beleid en protocol.**
3. **Bewustwording binnen de organisatie.**
4. **Start met een Privacy Impact Assesment.**
5. **Leg datastromen vast in modellen en processen.**
6. **Maak afspraken met externe verwerkers.**
7. **24/7 let op datalekken en processen.**
8. **Maak altijd een privacy belangenafweging.**
9. **Informeer de patiënten.**
10. **Ga terug naar stap 2.**

Stap 1: ga na of uw praktijk of apotheek een Functionaris Gegevensbescherming moet aanstellen.

Een Functionaris Gegevensbescherming (FG) is verantwoordelijk voor de controle op gegevensverwerking binnen de zorgorganisatie. Onder de Wet bescherming persoonsgegevens (Wbp) was het hebben van een FG optioneel. Na de invoering van de AVG is dit verplicht.

Tip: U hoeft een FG niet in dienst te nemen, deze kunt u inhuren en/of delen met andere zorgorganisaties. Het is wel verstandig om daarbij aansluiting te zoeken bij bestaande samenwerkingsverbanden.

Op grond van artikel 37 van de AVG is een FG in drie situaties verplicht. Eerstelijnszorgorganisatie voldoen aan alle drie deze situaties.
(bron: Autoriteit Persoonsgegevens).

1. 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.

2. 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.

1

The Road to…
Algemene Verordening Gegevensbescherming

Meer informatie:
www.pharmapartners.nl/wetgeving
voor vragen:
privacy@pharmapartners.nl

1

The Road to…
Algemene Verordening Gegevensbescherming

Meer informatie:
www.pharmapartners.nl/wetgeving
voor vragen:
privacy@pharmapartners.nl

3. 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.

Een FG controleert. Daarom is het belangrijk dat hij of zij onafhankelijk kan opereren en verder geen invloed heeft in de gegevensverwerking. Creëer deze onafhankelijkheid dan ook binnen het organogram van de zorgorganisatie. Alleen dan kan een FG zijn werk goed doen. Aan de andere kant van de tafel zit de uitvoerder van het privacybeleid: de Privacy Officer (PO) en/of Chief Information Security Officer (CISO). Hij of zij is verantwoordelijk voor de uitvoer van privacy regelgeving en degene die de organisatie adviseert over het veilig verwerken van persoonsgegevens. Binnen dit traject is het ook goed om korte lijnen te hebben richting de systeembeheerders binnen de organisatie. Zij zijn namelijk hands-on bezig met informatieverwerking.

Verplicht vanaf 25 mei 2018

Een Functionaris Gegevensbescherming die datastromen controleert. Het is een functie waarin strategisch organisatie advies, management, bestuurszaken, communicatie, juridische kennis over privacyrecht, data-beveiliging en IT in samen komen. Daarnaast moet u richting de AP en de Raad uw mannetje kunnen staan. Daarom kan een FG het beste in schaal 12 worden geplaatst.

Tip: Voor kleine en middelgrote organisaties is de verleiding groot om CISO- en FG-taken bij één persoon te leggen. Dit komt de onafhankelijkheid echter niet ten goede. Er zijn twee opties om de onafhankelijkheid toch te waarborgen:

- *Zoek samenwerking met andere organisaties. Vraag een CISO van een andere organisatie om de FG rol in te vullen. Zo kan diegene zich volledig specialiseren op het persoonsgegevens- en privacyvraagstuk.*

- *Laat de FG zijn of haar werk parttime doen. De overgebleven uren kunnen worden ingevuld op een andere positie binnen de zorgorganisatie, mits deze werkzaamheden niet conflicteren met de taken van de FG.*

2

Stap 2: zorg voor een kennisbasis.

Een FG en een CISO hebben een centrale rol binnen de implementatie van de AVG. Logischerwijs is het belangrijk dat zij goed beslagen ten ijs komen.

Kerntaken zijn het maken en controleren van privacybeleid, protocollen en reglementen. Op de website van de Autoriteit Persoonsgegevens staat veel informatie die kan helpen met AVG. Daarnaast staat op de websites van de LHV en de KNMP relevante informatie voor eerstelijnszorgorganisaties.
Ook juridische kennis is belangrijk.

Daarvoor is het goed om de centrale personen binnen dit traject daarin ook te sterken. Er zijn diverse cursussen die daarvoor gevolgd kunnen worden.

U kunt op verschillende manieren de staat van privacybeleid toetsen. Eén manier lichten we toe: de PMP Privacy Kompas. Benieuwd? Klik dan hier om alles te weten te komen over deze methodiek.

Belangrijke bronnen: Cursus voor FG

iapp.org/certify/cippe/

euroforum.nl/juridisch/opleiding-data-protection-officer/

duthleracademy.nl/nl/leergang-fg

Zie stap 7 voor meer informatie over datalekken.

3

Stap 3: bewustwording binnen de organisatie.

Eigenlijk geen stap, maar eerder een continu proces, is het creëren van bewustwording binnen de organisatie. Een goed middel om bewustwording te creëren binnen een organisatie is de meldplicht datalekken. Mocht u nog nooit te maken heb ben gehad met een datalek, dan bent u waarschijnlijk niet goed op de hoogte van deze verplichting.

Door de meldplicht datalekken te gebruiken als insteek van een bewustwordingscampagne, kan privacybeleid ook heel praktisch worden gemaakt voor medewerkers. De AVG is toch wat abstracter en richt zich op de grote lijnen.

Stap 4: start met een Privacy Impact Assesment.

4

Verandert er iets in de manier waarop u persoonsgegevens verwerkt, zoals het aanschaffen van een nieuw informatie systeem of een nieuwe datakoppeling met een derde partij, dan verlangt de AVG dat u in dergelijke gevallen een analyse uitvoert om te bepalen of deze nieuwe diensten, producten en/of koppelingen een verhoogd (cyber)risico opleveren voor de cliënt, diens persoonsgegevens. Om die vragen te kunnen beantwoorden, moet een Privacy Impact Assesment (PIA) worden gedaan.

Een PIA stimuleert u om op tijd na te denken over vragen als:

- wat de impact is van het beoogde product, dienst of koppeling (project) op de privacy van de betrokkenen (de mensen van wie u persoonsgegevens verwerkt);

- wat de risico's zijn voor de betrokkenen en voor de organisatie;

- of er, gegeven de doelstellingen, ook een aanpak mogelijk is die minder gevolgen heeft voor de privacy.

Een PIA is niet zelf te ontwikkelen: deze worden door specialistische bureaus vormgegeven en uitgevoerd. Waar een goede PIA aan moet voldoen en waar u als inkoper op moet letten is te lezen op de website van NOREA.

Uit een PIA komen procesplannen en taken. Deze zijn, als ze SMART zijn geformuleerd, te vangen in dashboards. Dit maakt het voor een FG maar ook voor portefeuillehouders inzichtelijk wat de staat van het privacybeleid binnen de organisatie is. Voor draagvlak en overzicht: neem afscheid van spreadsheets en pak deze kans om te switchen naar dashboards.

5

Stap 5: leg datastromen vast in modellen.

Het voelt heel natuurlijk om het vastleggen van datastromen als één van de allereerste stappen te zien. Maar uit de praktijk blijkt dat veel stromen in grote lijnen al zijn gedocumenteerd, door bijvoorbeeld de gegevensbeheerder. Een PIA zorgt ervoor dat u ook goed weet hoe alles binnen een organisatie loopt. Het vastleggen van deze stromen in modellen of een register blijft natuurlijk wel essentieel en voor sommige organisatie zelfs verplicht.

Tip: Begin bij de start van een registratie en werk vanuit daar verder met de informatie die er al is en uit de PIA is verkregen.

Sla twee vliegen in één klap: informatiebeveiliging is prima te combineren met privacy. Kijk goed naar de datakwalificaties van de bronnen. Ga daarom goed in gesprek met de verantwoordelijke systeembeheerders en eigenaren van de data. Vraag ze het hemd van hun lijf en investeer in de relatie. Het zijn namelijk uw ogen en oren binnen de organisatie.

6

Stap 6: maak afspraken met externe verwerkers.

Externe verwerkers zijn er in alle soorten en maten. In deze stap gaan we in op de drie belangrijkste soorten verwerkers: huidige verwerkers, nieuwe verwerkers en organisaties die dossiers geleverd krijgen van de zorg-organisatie.

Bij huidige verwerkers kunnen twee dingen aan de hand zijn: privacy is al onderdeel van de overeen-komst óf dat is het niet. In het eerste geval is het een kwestie van controleren of de overeenkomst voldoet aan de nieuwe rechten en plichten van de AVG. Zijn er nog geen hel-dere afspraken gemaakt, dan is het uitermate belangrijk dat u dit snel oppakt met uw leverancier. Denk daarbij onder andere aan beveiligingseisen, communicatie rond datalekken, oplostijden bij incidenten, etc.

Hetzelfde geldt natuurlijk voor nieuwe verwerkers. Let op: U als verantwoordelijke bent verplicht om dit te re-gelen, leun dus niet te lang achterover en benader actief uw leverancier hierover.

PharmaPartners stelt een standaard verwerkersover-eenkomst op. Deze kan worden gebruikt om andere overeenkomsten te toetsen. Meer informatie daarover vindt u op de pagina 'Wetgeving' op mijn.pharmapartners.nl.

The Road to…
Algemene Verordening Gegevensbescherming

Meer informatie:
www.pharmapartners.nl/wetgeving
voor vragen:
privacy@pharmapartners.nl

7

The Road to…
Algemene Verordening Gegevensbescherming

Meer informatie:
www.pharmapartners.nl/wetgeving
voor vragen:
privacy@pharmapartners.nl

Stap 7: 24/7 let op datalekken.

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven, zorginstellingen als overheden) direct, uiterlijk binnen 72 uur, een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Het is belangrijk om bij een datalek zo snel mogelijk te acteren zodat de schade voor de cliënt wordt beperkt en diens privacy wordt geborgd.

Vraag 1: Heeft zich een beveiligingsincident voorgedaan?
In de meeste gevallen (zoals bekend bij de AP) gaat het bij beveiligingsincidenten in de meeste gevallen om databestanden die bij een verkeerde adressant belanden, al kan een gestolen of misplaatst printje evengoed een beveiligingsincident vormen. Andere voorbeelden zijn: cyberaanvallen (incl. DDos), e-mail verzonden naar verkeerde adressen, medische gegevens versturen via Gmail, gestolen laptops, afgedankte niet-schoongemaakte computers en verloren onbeveiligde usb-sticks.

Vraag 2: Is er sprake van een datalek?

Er is sprake van een datalek als zich een beveiligingsincident heeft voorgedaan wat gevolgen kan hebben voor (de beschikbaarheid of integriteit van) persoonsgegevens en dit mogelijk (ernstige) nadelige gevolgen kan hebben voor de betrokkene. Zijn bij een beveiligingsincident gegevens over iemands gezondheid betrokken, dan gaat dit protocol, in overeenstemming met de beleidsregels van de Autoriteit Persoonsgegevens, er in principe bijna altijd vanuit dat het een datalek betreft.

Vraag 3: Moet ik het ook melden bij de autoriteit?

Heeft u een datalek geconstateerd en betreft het persoonsgegevens waar u verantwoordelijke voor bent (uw clienten), dan moet u melden bij de autoriteit persoonsgegevens. PharmaPartners kan u hierin ondersteunen en waar mogelijk van extra informatie voorzien. Heeft u dus een vermoedelijk datalek, neem dan direct contact op met één van onze Customer Support specialisten.

De meldplicht datalekken heeft tot doel datalekken te voorkomen. Daarnaast moet het ook de gevolgen voor de betrokkene beperken indien een datalek zich toch voordoet. Ook moet de meldplicht bijdragen aan het herstel van vertrouwen in de omgang met persoonsgegevens door organisaties.

7

The Road to…
Algemene Verordening Gegevensbescherming

Meer informatie:
www.pharmapartners.nl/wetgeving

voor vragen:
privacy@pharmapartners.nl

8

Stap 8: Maak altijd een privacy belangenafweging (uw belang vs. die van de cliënt)

Gegevens verwerken voor declaratie-, management informatie- en/of wetenschappelijke doeleinde mag in de meeste gevallen gewoon, alleen wil de nieuwe verordening dat u bij dergelijke koppelingen of verwerkingen wel kritisch blijft nadenken en rekening houdt met de privacy van de patiënt.

De eerste 17 jaar van het nieuwe millennium, stonden in het teken van de koppeldrift. Data werd op grote schaal verzameld, zonder dat men zich afvroeg of het verzamelen ook daadwerkelijk een gerechtvaardigd doel diende.

2018 gaat in het teken staan van dataminimalisatie: Oftewel, is deze verwerking (of hoeveelheid data) absoluut noodzakelijk voor het doel dat ik nastreef? In het geval van de zorgaanbieder: wat is absoluut noodzakelijk voor het leveren van goede zorg?

Stap 9: informeer de patiënten.

9

Nederland heeft 17 miljoen toezichthouders. Iedere patiënt kan namelijk zijn of haar gegevens opvragen bij een huisarts of apotheek.

Logischerwijs is het dus belangrijk om te laten weten dat de informatie van de patient in goede handen is. Sterker nog, u bent verplicht om ervoor te zorgen dat de patiënt goed begrijpt wat u allemaal met zijn persoonsgegevens gaat doen, voor welke doeleinde en op welke manier u deze (laat) beveiligen. Gebruik de AVG dan ook als gelegenheid om de patiënt hier uitgebreid over te informeren en laat zien dat u zijn privacy hoog in het vaandel hebt staan.

Stap 10: begin weer bij stap 2

Zoals zoveel dingen is privacy niet iets dat u afvinkt en dat het dan voor jaren geregeld is. Alles ontwikkelt zich/verandert. Kijk bijvoorbeeld hoe hackers te werk gaan en naar de samenstelling van het Nederlandse zorglandschap.

Blijf dus op de bal en laat hem niet lopen. Als aan de voorwaarden van de AVG is voldaan, is het goed om weer naar stap 2 te gaan. Kijk naar de trends op het gebied van privacy, informatiebeveiliging en gegevensbescherming en controleer doorlopend of het privacybeleid nog steeds voldoende bescherming biedt.

En nu aan de slag!

We hopen dat PharmaPartners u via dit stappenplan genoeg handvatten heeft gegeven om met goede moed aan de slag te gaan met de Algemene Verordening Gegevensbescherming.

We kunnen ons voorstellen dat sommige organisaties extra stappen inbouwen. Dit horen we graag! Mail ons daarom als u vindt dat belangrijke informatie ontbreekt. Of als u tips hebt waarvan u denkt dat ze collega's kunnen helpen!

Meer informatie:

www.pharmapartners.nl/wetgeving

voor vragen:

privacy@pharmapartners.nl

PharmaPartners
Wilhelminakanaal Zuid 110A
4903 RA Oosterhout

088 - 688 88 88
www.pharmapartners.nl