Branchevereniging BTN in zorg thuis

Algemene verordening gegevensbescherming

FEBRUARI, 2018

Algemene informatie AVG

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

Wat verandert er?
De AVG zorgt onder meer voor:

- Versterking en uitbreiding van privacyrechten;

- Meer verantwoordelijkheden voor organisaties;

- Dezelfde, stevige bevoegdheden voor alle Europese privacytoezichthouders, zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen.

In deze informatiefolder vindt u de belangrijkste wijzigingen voor organisaties.

Overgangsperiode tussen Wbp en AVG
Op 4 mei 2016 is de AVG gepubliceerd. De AVG is 20 dagen na deze publicatie in werking getreden. Maar de AVG is pas vanaf 25 mei 2018 van toepassing.

Er zit dus een periode van 2 jaar tussen de inwerkingtreding van de AVG en het moment dat deze daadwerkelijk van toepassing is. Deze tijd is nodig om organisaties en toezichthouders zich goed te laten voorbereiden op de AVG.

BTN biedt een aantal diensten ter voorbereiding op de AVG. Deze zullen ook benoemd worden in deze informatiefolder. Daarnaast ook een stappenplan om u voor te bereiden.

Veel informatie kunt u ook terug vinden op de website van de Autoriteit Persoonsgegevens:

www.autoriteitpersoonsgegevens.nl.

AUTORITEIT PERSOONSGEGEVENS

Algemene vragen over de AVG

Waarom is er nieuwe Europese privacywetgeving?
In de EU heeft nu nog elke lidstaat een eigen privacywet. Deze nationale wetten zijn wel allemaal gebaseerd op de Europese privacyrichtijn uit 1995. In Nederland is de nationale uitvoering van deze richtlijn de Wet bescherming persoonsgegevens (Wbp).

De Europese privacyrichtlijn werd vastgesteld toen internet nog in de kinderschoenen stond. Daarom is de Europese privacywetgeving herzien.

Wat merken mensen van wie persoonsgegevens worden verwerkt van de AVG?
Door de algemene verordening gegevensbescherming (AVG) krijgen meer mensen meer mogelijkheden om voor zichzelf op te komen bij de verwerking van hun gegevens. Hun privacyrechten worden namelijk versterkt en uitgebreid.

Wat levert de AVG mij als organisatie op?
Als de AVG van toepassing is, geldt er nog maar één privacywet in de hele EU in plaats van 28 verschillende nationale wetten. Ook is de AVG meer toegespitst op de gedigitaliseerde samenleving.

Blijft de NEN 7510 gelden voor zorgaanbieders onder de AVG? Norm voor informatiebeveiliging in de zorg.
Ja, de NEN 7510 blijft ook onder de AVG een belangrijke norm voor informatiebeveiliging in de zorg.

Certificeren volgens de NEN 7510 is op grond van de AVG niet verplicht. Ongeacht de rechtsvorm en de omvang van de organisatie.

Hoewel een NEN 7510-certificaat niet verplicht is, heeft u wel een verantwoordingsplicht onder de AVG.

Voorbereid in 10 stappen

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Organisaties die persoonsgegevens verwerken krijgen dan meer verplichtingen. De nadruk ligt—meer dan nu—op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden. Dat vergt een gedegen voorbereiding.

Als organisatie kunt u nu al stappen ondernemen om straks klaar te zijn voor de AVG. Onderzoek alvast of u uw huidige processen, diensten en goederen op bepaalde punten moeten aanpassen om te voldoen aan de AVG.

Om u op weg te helpen heeft de Autoriteit Persoonsgegevens (AP) de 10 belangrijkste stappen voor u op een rijtje gezet. Dat zijn:

1. Bewustwording
2. Rechten van betrokkenen
3. Overzicht verwerkingen
4. Data protection impact assessment
5. Privacy by design & privacy by default
6. Functionaris gegevensbescherming
7. Meldplicht datalekken
8. Bewerkersovereenkomsten
9. Leidende toezichthouder
10. Toestemming

Stap 1: Bewustwording

Zorg ervoor dat de relevante mensen in de organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op de huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen.

Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en begin er daarom op tijd mee.

Bedenk dat de AP uw organisatie sancties op kan leggen van maximaal 20 miljoen euro of 4% van de omzet als u zich niet aan de privacywetgeving houdt.

BTN heeft voor haar leden een e-learning beschikbaar gesteld over bewustwording onder de medewerkers van uw organisatie.

Meer informatie over deze e-learning vindt u op de ledensite, wanneer u bent ingelogd kiest u voor ‘onderwerpen a-z’. En vervolgens kiest u voor AVG.

Stap 2: Rechten van betrokkenen

Onder de AVG krijgen betrokkenen (de mensen van wie u persoonsgegevens verwerkt) meer en verbeterde privacyrechten. Zorg er daarom voor dat zij hun privacyrechten goed kunnen uitoefenen.

Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet u ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.

Ook kunnen mensen een klacht indienen bij de AP over de manier waarop organisaties omgaan met gegevens. De AP is verplicht deze klachten te behandelen.

Stap 3: Overzicht verwerkingen

Breng uw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt. Onder de AVG heeft u een verantwoordingsplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt. Het bijhouden van een register van verwerkingsactiviteiten is onderdeel van de verantwoordingsplicht.

Informatie behorend bij stap 3:

Ben ik verplicht om een register van verwerkingsactiviteiten op te stellen?
In de AVG staan een aantal verplichte maatregelen genoemd. Of u zo’n verwerkingsregister moet opstellen, hangt af van de omvang van de organisatie en type gegevens.

Organisatie met meer dan 250 medewerkers. Dan bent u verplicht om een verwerkingsregister bij te houden

Organisatie met minder dan 250 medewerkers. Dan moet u over een verwerkingsregister beschikken wanneer u persoonsgegevens verwerkt:

- Die een hoog risico inhouden voor de rechten en vrijheden van de personen van wie u persoonsgegevens verwerkt en/of;

- Waarvan de verwerking niet incidenteel is en/of;

- Die vallen onder de categorie bijzondere gegevens, zoals gegevens over gezondheid.

Bent u verplicht? Dan moet u dit register kunnen vertrekken wanneer

Stap 4: Data protection impact assessment (DPIA)

Onder de AVG kunt u verplicht zijn een DPIA uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

U moet een DPIA uitvoeren als uw beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. U kunt nu alvast inschatten of u straks DPIA's moet uitvoeren en hoe u dit dan gaat aanpakken.

Komt uit een DPIA naar voren dat de beoogde verwerking een hoog risico oplevert, dan dient u de AP te raadplegen.

Op welke manier moet een DPIA uitgevoerd worden?
Er zijn verschillende methodes om een DPIA uit te voeren. U kunt er zelf een kiezen, als u maar voldoet aan de basisvereisten:

- Een systematische beschrijving van de beoogde gegevensverwerkingen en de doeleinden hiervan.
- Een beoordeling van de noodzaak en de proportionaliteit van de verwerkingen. Dat houdt in: is het verwerken van persoonsgegevens op deze manier noodzakelijk om uw doel te bereiken? En is de inbreuk op de privacy van de betrokkenen niet onevenredig in verhouding tot dit doel?
- Een beoordeling van de privacyrisico's voor de betrokkenen.
- De beoogde maatregelen om de risico's aan te pakken en aan te tonen dat u aan de AVG voldoet.

De verantwoordelijke moet een DPIA uitvoeren wanneer de gegevensverwerking waarschijnlijk een hoog privacy risico oplevert. De AP heeft 9 criteria opgesteld om deze inschatting te maken. Als vuistregel kunt u hanteren dat u een DPIA moet uitvoeren als uw verwerkingen aan 2 of meer van de 9 criteria voldoet. De criteria vindt u terug op de website van de AP.

Stap 5: Privacy by design & privacy

Maak uw organisatie nu al vertrouwd met de onder de AVG verplichte uitgangspunten van *privacy by design & privacy by default* en ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat u niet meer gegevens verzameld dan noodzakelijk voor het doel van de verwerking. En dat u de gegevens niet langer bewaart dan nodig.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alleen persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken.

Op de website van de AP staat een handreiking voor het uitvoeren van een DPIA.

Stap 6: Functionaris voor gegevensbescherming

Onder de AVG kunnen organisaties verplicht zijn om een functionaris gegevensbescherming (FG) aan te stellen. Een FG is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG.

Een FG is in drie verschillende situaties verplicht:

1. Overheden en publieke organisaties

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

2. Observatie

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

3. Bijzondere persoonsgegevens

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

BTN heeft ……

Wat moet ik regelen zodat de FG zijn werk goed kan doen?

Volgens artikel 38 van de AVG heeft de FG voldoende middelen nodig om zijn taak te kunnen uitvoeren. En moet hij toegang hebben tot de persoonsgegevens en de verwerkingen van de gegevens in de organisatie. Daarnaast moet een FG zijn kennisniveau op peil kunnen houden.

Actieve steun, voldoende tijd, en praktische ondersteuning maar ook duidelijkheid richting het personeel over de FG en scholing.

Stap 7: Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in de organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan.

Dit gaat verder dan de huidige protocolplicht uit de Wet bescherming persoonsgegevens, die alleen betrekking heeft op de gemelde datalekken.

Datalek
Er is sprake van een datalek als er een inbreuk plaatsvindt op de beveiliging van persoonsgegevens. Dat is bijvoorbeeld het geval wanneer onbedoeld toegang wordt geboden tot persoonsgegevens of als sprake is van vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie. Niet alleen het vrijkomen of lekken van gegevens resulteert in een datalek, ook wanneer onrechtmatig gegevens worden verwerkt is hiervan sprake. Om een voorval te kunnen kwalificeren als een datalek, moet sprake zijn van een daadwerkelijk beveiligingsincident. Dit is niet alleen het geval bij inbraak in een databestand, ook een kwijtgeraakte usb-stick, een gestolen laptop, een laptop die in de trein is blijven liggen of een brand in een datacentrum zijn datalekken.

Modelverwerkersovereenkomst voor de zorgsector
Brancheorganisaties Zorg (BoZ) hebben in het kader van de inwerkingtreding van de AVG een standaard modelverwerkersovereenkomst ontwikkeld.

De verwerkersovereenkomst is een bijlage bij iedere (af te sluiten) overeenkomst waarin een derde in opdracht van de zorgorganisatie persoonsgegevens verwerkt. Het model dat is gemaakt is werkt als standaard voor de gehele zorgsector. Zorgorganisaties kunnen het model binnen de grenzen van de Wbp en AVG aanpassen.

De modellen kunt u downloaden van de ledensite van BTN, via 'Onderwerpen A-Z' en dan kiest u voor 'AVG'.

Stap 8: Verwerkersovereenkomsten

Heeft u de gegevensverwerking uitbesteed aan een verwerker? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn. En of deze nog voldoen aan de eisen van AVG.

Verwerker
Een verwerker is een persoon of een organisatie aan wie de verantwoordelijke de gegevensverwerking heeft uitbesteed. Bijvoorbeeld een administratiekantoor.

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

Eisen AVG
De organisatie en de verwerker zijn verplicht om een aantal onderwerpen vast te leggen in een schriftelijke overeenkomst. De volgende onderwerpen dienen vastgelegd te worden:

Algemene beschrijving
Een omschrijving van het onderwerp, de duur, de aard en het doel van de verwerking, het soort persoonsgegevens, de categorieën van betrokkenen en uw rechten en verplichtingen als verwerkingsverantwoordelijke.

Instructies verwerking
De verwerking vindt in principe uitsluitend plaats op basis van uw schriftelijke instructies. De verwerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken.

Geheimhoudingsplicht
Personen in dienst van of werkzaam voor de verwerker hebben een geheimhoudingsplicht.

Beveiliging
De verwerker treft passende technische en organisatorische maatregelen om de verwerking te beveiligen. Bijvoorbeeld pseudonimisering en versleuteling van persoonsgegevens, permanente informatiebeveiliging, herstel van beschikbaarheid en toegang tot gegevens bij incidenten, regelmatige beveiligingstesten.

Subverwerkers
De verwerker schakelt geen subverwerker(s) in zonder uw voorafgaande schriftelijke toestemming. De verwerker legt aan een subverwerker in een subverwerkersovereenkomst dezelfde verplichtingen op als de verwerker richting u heeft.

Privacyrechten
De verwerker helpt u om te voldoen aan uw plichten als betrokkenen hun privacyrechten uitoefenen.

Andere verplichtingen
De verwerker helpt u ook om te voldoen aan andere verplichtingen, zoals de DPIA.

Gegevens verwijderen
Na afloop van de verwerkingsdiensten verwijdert de verwerker de gegevens. Of bezorgt hij deze aan u terug, als u dat wilt. Ook verwijdert hij kopieën. Tenzij de verwerker wettelijk verplicht is om deze gegevens te bewaren.

Audits
De verwerker werkt mee aan uw audits of die van een derde partij. En stelt alle relevante informatie beschikbaar om te kunnen controleren of hij zich als verwerker houdt aan de hierboven genoemde verplichtingen.

Stap 9: Leidende toezichthouder

Deze stap is minder relevant voor organisaties die werkzaam zijn in de zorg– en welzijn.

De AVG gaat uit van de zogeheten onestopshop-regel. Onestopshop houdt in dat organisatie die zogeheten grensoverschrijdende gegevensverwerkingen uitvoeren, nog maar met één privacy-toezichthouder zaken hoeven te doen. Dit wordt de 'leidende toezichthouder' genoemd.

Onder grensoverschrijdende gegevensverwerkingen wordt verstaan dat een organisatie gegevens verwerkt in verschillende EU-lidstaten of dat de verwerkingen in meerdere lidstaten impact hebben.

De leidende toezichtshouder is als eerste verantwoordelijk voor het toezicht op de organisaties met grensoverschrijdende gegevensverwerkingen.

Stap 10: Toestemming

Uw gegevensverwerking kan gebaseerd zijn op toestemming van betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert.

Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken.

Hoe kan je aantonen dat je toestemming hebt ontvangen?
U moet vanuit de AVG aan de AP kunnen laten zien dat u toestemming heeft ontvangen. Dat maakt onderdeel uit van de verantwoordingsplicht die onder de AVG valt.

Twee van de specifieke eisen die de AVG stelt aan 'toestemming' zijn dat deze *'geïnformeerd'* en *'specifiek'* gegeven is. Om geldige toestemming aan te tonen is het dan ook essentieel dat u kunt 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.

Zorgorganisaties en de AVG

De bovenstaande stappen bereiden u voor op de AVG die dus eind mei in werking treedt. Het is inmiddels duidelijk dat onder de AVG nieuwe informatieverplichtingen en nieuwe regels gelden over bijvoorbeeld het werken met toestemming van de cliënt.

De bestaande regels over privacy worden door de AVG bevestigd en op onderdelen versterkt. De volgende wetten blijven dus gelden:

- Wet op geneeskundige behandelovereenkomst (WGBO)
- Wet kwaliteit, klachten en geschillen zorg (Wkkgz)
- Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)
- Zorgverzekeringswet
- Wet marktordening gezondheidszorg (Wmg)
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.

Vragen over zorgaanbieders en de AVG

<u>Mag ik onder de AVG persoonsgegevens verstrekken aan zorgverzekeraars?</u>

Als zorgaanbieder mag u onder de AVG persoonsgegevens blijven verstrekken aan zorgverzekeraars.

De regels die onder de huidige Wbp gelden voor bijvoorbeeld het verstrekken van gegevens aan zorgverzekeraars voor de declaratie van zorgkosten, het aanvragen van machtigingen en het uitvoeren van formele en materiële controle blijven onder de AVG dus bestaan.

<u>Wat is de verhouding tussen de AVG en de Wet cliëntenrechten bij elektronische verwerking van gegevens?</u>
De AVG is een Europese privacywet die boven nationale wetgeving staat. De 'Wet cliëntenrechten bij elektronische verwerking van gegevens' geldt in aanvulling op de AVG. Dat betekent dat daar waar de AVG meer bescherming voor cliënten biedt, de AVG voor gaat.

De AVG geeft de zorgsector de mogelijkheid om specifieke regels in te stellen in nationale wetgeving. De 'Wet cliëntenrechten bij elektronische verwerking van gegevens' is een voorbeeld van zo'n nationale uitwerking.

Deze wet schept voorwaarden voor het veilig elektronisch uitwisselen van medische gegevens in de zorgsector. Het gaat om elektronische uitwisselingssystemen waarmee u als zorgaanbieder op elektronische wijze dossiers, gedeelten van dossiers of gegevens uit dossiers, voor andere zorgaanbieders inzichtelijk kunt maken.

Veel regels van de AVG komen overeen met deze wet.

Welke diensten biedt BTN u als ondersteuning en voorbereiding op de AVG?

Informatiebeveiliging in de zorg

De NEN 7510 'informatiebeveiliging in de zorg' geeft richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen die elke organisatie in de gezondheidszorg moet treffen ter beveiliging van de informatievoorziening.

BTN biedt haar leden de volgende hulpmiddelen:

- Het Basis Beveiligingsmodel Care (BBMCare model); dit model is gebaseerd op een generieke risicoanalyse voor de zorgprocessen met de bijbehorende wet– en regelgeving. Het model bevat een inventarisatie van processen en informatiecomponenten, een hierop betrekking hebbende classificatie en selectie van maatregelen.

- Handvatten informatieveiligheid voor de zorgsector.; deze handvatten zijn gebaseerd op de twaalf belangrijkste normelementen van de geldende NEN-normen. De handvatten zijn met name voor kleine zorgaanbieders goed hanteerbaar om op een effectieve, efficiënte en laagdrempelige wijze invulling te geven aan informatiebeveiliging. Maar ook voor grote zorgaanbieders bieden de handvatten meerwaarde als opstap naar het BBMCare model.

- Bewustwordingscursus informatiebeveliging VVT-sector— een e-learning; de mens is de zwakste schakel in de beveiligingsketen. Een van de belangrijkste beheersmaatregelen uit de NEN 7510 is bewustwording, opleiding en training van medewerkers ten aanzien van informatiebeveiliging. Voor BTN leden is een cursus tegen een gereduceerde prijs beschikbaar.

Voorbereiding op AVG

BTN heeft met CareSecure BV afspraken gemaakt over ondersteuning van haar leden met de voorbereiding op de AVG.

Vooruitlopend op de invulling van de FG biedt CareSecure BV ondersteuning bij een aantal acties die minimaal moeten worden uitgevoerd (alvorens de FG rol goed kan worden uitgevoerd). Deze ondersteuning richt zich op het samenstellen van het register van verwerkingen van persoonsgegevens en de inventarisatie van de benodigde acties om te voldoen aan de (nieuwe) regelgeving.

Het aanbod bevat een workshop die hiervoor allereerst het vereiste inzicht in de huidige stand van zaken moet opleveren. Aansluitend op de workshop wordt vier uur ondersteuning geboden bij uitwerking van de benodigde producten, waarbij zoveel mogelijk gebruik wordt gemaakt van reeds beschikbare templates en standaard beschrijvingen. Als zorgaanbieder wordt u hiermee geholpen bij het opstellen van documenten, ondersteuning bij training van personeel en inrichting van procedures en processen.

Voorbereiding op AVG en invulling rol FG

Samen met CareSecure en Smartmirrors heeft BTN een ondersteuning voor haar leden georganiseerd rondom de invulling van de AVG en de FG.

Op dit moment inventariseren wij nog welke behoefte ligt bij de leden. We komen hier dus nog op terug bij u.

Al deze hulpmiddelen zijn terug te vinden op de ledensite van BTN, 'onderwepen A-Z', dan kiest u voor