



Op 25 mei 2016 trad de nieuwe Europese Privacyverordening – de Algemene Verordening Gegevensbescherming (AVG) – in werking. Deze verordening heeft betrekking op de verwerking van persoonsgegevens en is daarom ook van groot belang voor zorgaanbieders, temeer daar deze als verordening dwingend is voor alle lidstaten. Organisaties hebben tot 25 mei 2018 de tijd om te voldoen aan de verplichtingen die de AVG met zich meebrengt. Gelukkig zijn veel zorginstellingen hier al druk mee aan de slag, maar wij constateren ook dat veel andere aanbieders hier nog niet of onvoldoende mee bezig zijn.

Er wordt veel van u als zorgaanbieder verwacht. De druk om aan de informatiebeveiligingsnormen NEN7510, NEN7512 en NEN7513 te voldoen wordt immers groter met het Besluit elektronische gegevensverwerking door zorgaanbieders, u heeft te maken met de Wet Meldplicht Datalekken, maar ook de verplichting om een Functionaris Gegevensbescherming (FG) te benoemen en te laten registreren bij de Autoriteit Persoonsgegevens die strenger zal gaan handhaven.



Lidstaten hebben twee jaar de tijd om hun nationale wetgeving aan te passen in verband met deze verordening. Dit betekent dat voor 25 mei 2018 de huidige Wet Bescherming Persoonsgegevens wordt vervangen door een nieuwe wet waar u zich vanaf die datum aan dient te conformeren.

De combinatie met de meldplicht datalekken zal snel bloot leggen in welke mate organisaties aan deze nieuwe wetgeving voldoen en welke organisaties kwetsbaar zijn.

WIJ ROEPEN ALLE ZORGAANBIEDERS OP OM NU IN ACTIE TE KOMEN EN MET ONS DE NODIGE VOORBEREIDINGEN TE TREFFEN !!

BTN heeft met CareSecure BV afspraken gemaakt over ondersteuning van haar leden om dit op een vooral praktische wijze op te pakken. Voorkomen moet worden dat dit een grote papieren tijger wordt. Vooruitlopend op de invulling van de FG rol bieden wij ondersteuning aan bij een aantal acties die minimaal moeten worden uitgevoerd (alvorens de FG rol goed kan worden uitgevoerd).

Hieronder worden enkele belangrijke acties toegelicht:

1. Breng de verwerkingen van persoonsgegevens in kaart

Als zorgaanbieder dient u een register van verwerkingen op te stellen, bij te houden en te publiceren. In het register legt u precies vast welke persoonsgegevens u met welk doel verwerkt, wie die gegevens ontvangen, wat de grondslag is voor de verwerking, de wijze waarop de expliciete toestemming wordt ingevuld, hoe lang de gegevens worden bewaard, welke technische en organisatorische beveiligingsmaatregelen om de gegevens te beschermen (o.a. NEN7510) u heeft getroffen, etc.

2. Loop de verwerkersovereenkomsten na

Is met iedere bewerker een bewerkersovereenkomst afgesloten? Loop dan ook de inhoud na. In de AVG is veel uitgebreider dan in de Wet Bescherming Persoonsgegevens beschreven welke onderwerpen opgenomen moeten worden in de bewerkersovereenkomsten.

3. Controleer de processen voor de privacyrechten van de cliënten

Rechten van betrokkenen (zoals cliënten) komen in de nieuwe AVG veel nadrukkelijker naar voren en zijn ook veel steviger verankerd dan in de huidige Wet Bescherming Persoonsgegevens. Het recht op inzage is niet beperkt tot de gegevens die in het ECD zijn vastgelegd; ook gegevens die in andere applicaties en/of dossiers zijn vastgelegd, dienen te worden opgeleverd. En ook nog binnen vier weken. Naast de reeds bestaande rechten op inzage, correctie en verwijdering van gegevens, zijn toegevoegd het recht op “vergetelheid” en het recht op dataportabiliteit; dit laatste geeft de cliënt het recht om gegevens in een gestructureerde, gangbare en machineleesbare vorm te ontvangen en deze ongehinderd aan een andere organisatie te kunnen overdragen.

4. Incorporeer de PIA in de werkprocessen

Een verwerking van persoonsgegevens mag onder de AVG niet worden gestart, als er geen Privacy Impact Assessment (PIA) is opgesteld en is goedgekeurd door de Functionaris voor de gegevensbescherming. Een PIA brengt de risico's van de verwerking in kaart voor de privacy van betrokkenen (cliënten). De risico's die uit de PIA naar voren komen, dienen te worden beperkt met passende technische en organisatorische maatregelen. De resultaten van de PIA's vormen een goede basis voor het samen te stellen register.

5. Stel een functionaris voor de gegevensbescherming (FG) aan

Op grond van de AVG is aanstelling van een FG verplicht voor zorgaanbieders die vanwege hun aard op grote schaal bijzondere persoonsgegevens verwerken. Deze functionaris heeft een adviserende en informerende taak, maar ook een toezichthoudende rol en treedt daarbij op als contactfunctionaris voor de Autoriteit Persoonsgegevens.

Wilt u meer informatie over de implementatie van de AVG, neem contact op met

Peter van der Zwan (email: peter.vanderzwan@caresecure.nl / telefoon: 06 – 2874 1845)