Privacytips voor de zorg na een hete zomer

31 augustus 2017

Tip 1: maak een verwerkingsregister

De Wbp verplichtte zorgaanbieders om melding te doen aan de Autoriteit Persoonsgegevens van alle nieuwe verwerkingscategorieën binnen de organisatie. Er hoefde geen melding te worden gemaakt van gegevensverwerkingen die in het Vrijstellingsbesluit stonden. Voor gegevensverwerkingen met betrekking tot zorgverlening hoefde er niets gemeld te worden.

De Avg gooit het over een andere boeg. Er hoeft geen melding meer te worden gedaan aan de Autoriteit Persoonsgegevens, maar verwerkingscategorieën moeten wel allemaal in een register verwerkingsactiviteiten worden opgenomen. Dit kan een elektronisch register zijn. Deze verplichting geldt ook voor eerstelijnszorgaanbieders. De Avg beschrijft welke gegevens in het register moeten worden opgenomen. Op verzoek moet het register ter beschikking van de AP worden gesteld.

Het register van de verwerkingsverantwoordelijke bevat onder meer:

- a) de doeleinden van de gegevensverwerking;
- b) een beschrijving van de groep personen waarop de gegevens betrekking hebben en van de categorieën van persoonsgegevens;
- c) degenen aan wie de persoonsgegevens worden verstrekt (de ontvangers);
- d) een beschrijving van de technische en organisatorische beveiligingsmaatregelen die zijn getroffen.

Ontvangers kunnen zowel derden zijn als degene die als verwerker is ingeschakeld. Door het register in te vullen ontstaat een goed overzicht van welke persoonsgegevens binnen de organisatie worden verwerkt, door wie dit gebeurt, naar wie deze gegevens toegaan en hoe de beveiliging zowel technisch als organisatorisch is ingevuld. Daarmee is het halve werk al gedaan.

Tip 2: stel een functionaris gegevensbescherming (FG) aan

In een eerder nummer van ICT&health schreven wij er al over. De functionaris gegevensbescherming (FG) wordt verplicht in de zorg. Dit was al duidelijk door de formulering in de Avg. Deze stelt een FG verplicht als er grootschalig persoonsgegevens worden verwerkt die betrekking hebben op de gezondheid. Voor wie nog zou menen dat dit voor de eigen organisatie niet opgaat, heeft onze eigen overheid bedacht dat de FG verplicht wordt voor elke organisatie die kwalificeert als instelling in de zin van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) en die is aangesloten op een elektronisch uitwisselingssysteem (of deze in stand houdt). Dit is nader uitgewerkt in het Begz, dat overigens nog niet is ingevoerd. Deze omschrijving is zo ruim dat feitelijk iedereen die zich beroepsmatig met gezondheidszorg bezighoudt eronder valt. Alleen solisten vallen buiten de omschrijving. Vanwege de omschrijving die de Avg geldt, is de verwachting dat ook de meeste zorgaanbieders die niet aangesloten zijn op een elektronisch uitwisselingssysteem toch een FG zullen moeten aanstellen.
Een FG kan een goede bijdrage leveren aan het compliant maken van de organisatie. Het is namelijk zijn taak om daarover te adviseren. De FG moet zijn taken onafhankelijk kunnen uitvoeren en mag dus geen instructies ontvangen van zijn (formeel) leidinggevenden. Zijn positie binnen de organisatie is te vergelijken met een lid van de ondernemingsraad. De verwerkingsverantwoordelijke en de verwerker moeten de FG ondersteunen bij de vervulling van zijn taken.

De FG informeert en adviseert over de verplichtingen die volgen uit het privacyrecht in brede zin. Verder ziet hij toe op de naleving van het privacyrecht en kan hij hierover aanwijzingen geven (de verordening spreekt van ‘toewijzing van verantwoordelijkheden’) aan en bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits. Daarnaast kan hij advies geven over een gegevensbeschermingseffectbeoordeling en toezien op de uitvoering daarvan. Hij werkt samen met de Autoriteit Persoonsgegevens (AP) en treedt ook als contactpersoon op bij alle aangelegenheden waarbij de AP betrokken is.

De FG hoeft geen onderdeel uit te maken van de instelling. Hij kan ook extern worden ‘ingehuurd’. Hij zou daardoor ook regionaal kunnen worden aangesteld voor een groep zorgaanbieders. Ook belangenorganisaties kunnen er een aanstellen om hun leden te bedienen. Op deze manier kunnen kleine zorgaanbieders ook gemakkelijk(er) aan hun verplichtingen voldoen.

Zorg er wel voor dat de FG echt onafhankelijk is. Hij kan dus niet tevens ook privacy officer of security officer zijn. Dan zou hij immers zijn eigen ‘vlees’ keuren. Het is ook niet zo verstandig om gebruik te maken van bureaus die aan koppelverkoop doen. Bijvoorbeeld organisaties die eigen normen schrijven en daarop toetsen. Ook dan is een FG niet onafhankelijk meer.

Je kunt er ook voor kiezen om in eerste instantie een externe FG in te huren en dan ondertussen iemand van de eigen organisatie op te leiden om het later zelfstandig te kunnen doen. Dan kunnen er al grote stappen worden gemaakt in een vroeg stadium.