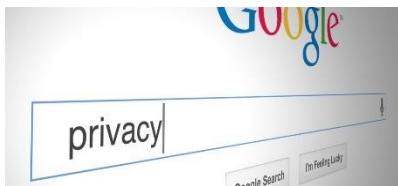


De AVG: Wat verandert er voor u?

Met het inwerkingtreden van de AVG verandert er voor u als zorgverlener veel. Natuurlijk bestonden er al veel verplichtingen, maar deze nieuwe wet legt meer verantwoordelijkheden bij u als Verwerkingsverantwoordelijke en bij ons als Verwerker. De cliënten krijgen ook meer en duidelijk omschreven rechten. Door middel van onderstaande 8 stappen hopen wij u op weg te helpen naar het voorbereiden op de AVG in uw praktijk. Bij elke stap zetten wij in een kader in hoeverre WinBase voor u zaken heeft geregeld.

1. Maak een privacybeleid

U dient intern privacybeleid te publiceren waarin staat wie welke rol heeft bij de omgang met persoonsgegevens in het algemeen en cliëntgegevens in het bijzonder. Het is belangrijk dat medewerkers daarvan op de hoogte zijn. Zij moeten dus regelmatig worden getraind in het zorgvuldig omgaan met persoonsgegevens.



Voor de belanghebbenden binnen en buiten de praktijk maakt u een privacyverklaring. Die verklaring moet in eenvoudige taal precies en

volledig uitleggen wat u doet met persoonlijke gegevens. Ook moet u mensen wijzen op hun rechten, zoals dat men gegevens mag aanpassen, het dossier mag inzien of zelfs laten vernietigen. Ook staan er contactgegevens in van de contactpersoon voor wat betreft gegevensbescherming (FG). Bovendien moet u de mensen wijzen op de mogelijkheid een klacht in te dienen bij de toezichthouder, de Autoriteit Persoonsgegevens

*Incura en Abakus zijn gecertificeerd voor zowel **ISO 27001** als **NEN 7510**. Deze kwaliteitsnormen vormen een dwingende leidraad voor onze processen en worden ieder jaar getoetst door een onafhankelijke auditor. Daarmee zijn uw gegevens bij ons in veilige handen. De volgende certificaten zijn beschikbaar: [certificaat ISO 27001](#), [certificaat NEN 7510](#) en de [Verklaring van toepasselbaarheid](#).*

2. Alle datalekken moeten goed worden gedocumenteerd

Een datalek is een incident waarbij vertrouwelijke persoonsgegevens (mogelijk) onterecht verloren zijn gegaan, beschadigd werden of voor onbevoegden beschikbaar waren. Een datalek is natuurlijk niet leuk en iedereen probeert dat te voorkomen. Mocht het toch gebeuren, dan moet u dat datalek goed documenteren. Ook als er geen verplichting bestaat tot het melden van het datalek aan de toezichthouder. Leg goed vast wat de oorzaak was, de gevolgen, wat u heeft gecommuniceerd en wat u heeft veranderd om herhaling te voorkomen. Mocht u vermoeden dat de oorzaak van een datalek bij Incura-Abakus ligt, neem dan direct contact met ons op.

3. Leg vast wat u doet met persoonsgegevens



Nieuw is dat alle verwerkingen (gebruik en/of opslag) van persoonsgegevens dienen te worden gedocumenteerd in een register. Daarin staan: uw praktijknaam, contactpersoon (verantwoordelijk voor gegevensbescherming) en contactgegevens.

Daarnaast beschrijft u de categorieën persoonsgegevens en de doeleinden waarvoor deze worden verwerkt en aan wie ze eventueel worden verstrekt.

Tenslotte wordt informatie opgenomen over de bewaartermijn van deze gegevens en hoe deze zijn beveiligd. Leg ook vast hoe en op welk moment gegevens worden verwijderd omdat u deze niet meer nodig hebt.

4. Sluit een verwerkersovereenkomst met uw leveranciers

In een dergelijke overeenkomst staan afspraken tussen u en de leverancier over de omgang met persoonlijke gegevens. Te denken valt aan het doel waarvoor de leverancier gegevens verwerkt, maar ook hoe te handelen bij een datalek. Ook staat er een geheimhoudingsverklaring in en informatie over eventuele sub-verwerkers aan wie diensten door de verwerker zijn uitbesteed. Een leverancier kan uw software-aanbieder zijn, maar ook uw accountant (salarisadministratie), een waarnemer, de schoonmaker en een externe systeembeheerder/ IT-adviseur.

Classificatie: 4 – Openbaar

SLA / VERWERKERSOVEREENKOMST

Hoe Incura-Abakus haar gegevensbescherming heeft geregeld kunt u vinden in de [verwerkersovereenkomst](#). Daarin staan ook afspraken met betrekking tot eventuele datalekken en audits.

5. Benoem een verantwoordelijke (FG)



Ook al is het niet helemaal duidelijk of het benoemen van een Functionaris Gegevensbescherming (FG) voor praktijken verplicht is, adviseren wij dit wel. Het gaat tenslotte om gevoelige zorggegevens. Het is goed een vaste persoon in uw praktijk te benoemen die de centrale contactpersoon is op het gebied van gegevensbescherming. Communicatie en documentatie worden centraal en dus eenduidiger uitgevoerd. Als u een eenmanspraktijk hebt, is de praktijk eigenaar natuurlijk zelf het aanspreekpunt.

Incura-Abakus heeft Jan Pieter Schoon aangesteld als functionaris gegevensbescherming. Vragen over de gegevensbescherming rond Incura-Abakus kunt u stellen via e-mail aan fg@winbase.nl.

6. Onderzoek privacyrisico's

Als je ná 31 mei aanstaande een nieuwe gegevensverwerking start waar een risico met betrekking tot persoonlijke gegevens bestaat, dan dient u dat risico te onderzoeken voordat u die gegevens-

verwerking start. Dat geldt ook wanneer een dergelijke gegevensverwerking wijzigt. U kunt denken aan wanneer u een praktijk overneemt, u van locatie verhuist of nieuwe software implementeert. In een dergelijk onderzoek (PIA = Privacy Impact Assessment) benoemt u risico's en formuleert u maatregelen om die risico's te verkleinen.

7. Beveiliging moet op orde zijn



Uw beveiliging moet op orde zijn en blijven. Die beveiligingsmaatregelen moeten passend zijn bij het risico en de gevoeligheid van de gegevens. Ze kunnen fysiek zijn (afsluitbare ruimten en kasten, opgeruimde bureau's) en digitaal (firewall, virusbeveiliging, encryptie bij communicatie, 2-factor-authenticatie). Zorg bijvoorbeeld dat u bij uitdiensttreden van medewerkers direct sleutels inneemt en hun systeemrechten verwijdert.

Door uw gegevens onder te brengen in de webapplicatie Incura-Abakus heeft u een belangrijke stap genomen om uw cliëntgegevens te beschermen. Uw gegevens staan op een streng beveiligde locatie en worden regelmatig gebackupt.

8. Uw cliënt krijgt meer rechten

Een aantal rechten bestaat al langer, maar nu worden rechten voor cliënten meer nadrukkelijk neergezet. Te denken valt aan het recht op correctie, op inzage en op verwijdering (wissing). Houd bij gegevenswissing rekening met het feit dat bestaande wetgeving soms in tegenspraak is met het recht op gegevenswissing.

Nieuw is een recht op dataportabiliteit, waarbij een cliënt het recht heeft zijn/haar gegevens mee te nemen in een veelgebruikt en machineleesbaar formaat. Een goed formaat is Excel, Word en pdf. Zorg wel dat er een pdf wordt gemaakt per document en niet één grote pdf met alle documenten.

In Incura-Abakus zullen wij deze cliëntrechten zoveel mogelijk ondersteunen. Dit zal in de komende maanden worden gerealiseerd, hetzij via het patiëntportaal, hetzij via de webapplicatie.

Voor de goede orde: het gaat hier alleen om informatie die de cliënt zelf aan u heeft aangeleverd. Dus niet om informatie van de zorgverlener, zoals behandelinformatie en diagnoses. Meer informatie over cliëntrechten vindt u [hier](#).

Incura-Abakus gaat een stap verder!

Op korte termijn zal Incura-Abakus een set voorbeelden van documenten en sjablonen (Word en Excel) aanbieden waarmee u als zorgpraktijk veel werk uit handen wordt genomen. Deze set documenten (bijvoorbeeld een Privacyverklaring, Privacybeleid, een Verwerkingsregister, een datalekregistratie en een PIA-risicobeoordeling) kunt u gebruiken om snel en compleet uw beleid en procedures vast te leggen en daarmee aan de vereisten van de AVG te voldoen.

///./AVG2018-02.docx