# Uitwerking Meet the Expert

*met Peter Schell (Functionaris Gegevensbescherming, PrivacyZorg)*

***"Tijdens de eerste expert namiddag (6 juni) blijkt dat regelgeving en praktijk soms goed en soms minder te combineren zijn. Synchroon probeert praktijken te ondersteunen bij de implementatie van de AVG. Dit doen we door een contract met PrivacyZorg af te sluiten voor u en onszelf. Ondersteunen trachten we ook te doen door de berg informatie te structureren naar toepasbare documenten. In dit document wederom een poging.***
***In dit document een overzicht van gestelde vragen tijdens de avond. Het was niet mogelijk alle vragen te beantwoorden helaas. Door hier te klikken kunt u uw vraag stellen. We gaan de vragen en antwoorden toevoegen aan deze uitwerking, Dit houden we vol totdat de vragen minimaal geworden zijn. In de nieuwsbrief van Synchroon kunt u dit document vinden. Overigens, onderaan dit document in een begrippenlijst toegevoegd"***

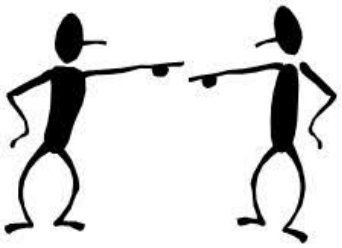
**Wat is de basis van deze wetgeving?**

Je mag geen gegevens verwerken tenzij een wet daartoe machtigt of bevoegd maakt. Dit kan dus een arts zijn of indien er gevraagd wordt gegevens te bewaren (bijvoorbeeld bij een HIS).
Deze wetgeving is niet sectorspecifiek, het is algemene wetgeving. Het geldt bijvoorbeeld ook voor Google of Facebook, waar de impact veel groter is.
Met de AVG wordt transparantie en aantoonbaarheid afgedwongen.

**Hoe ziet het contract eruit tussen PrivacyZorg – Synchroon – individuele huisartsenpraktijk**
PrivacyZorg adviseert Synchroon (en andere zorggroepen en ziekenhuizen) op het gebied van informatiebeveiliging. Daarnaast heeft Synchroon met Stichting PrivacyZorg voor alle huisartsenpraktijken een collectief contract afgesloten. De kosten hiervoor worden door Synchroon vergoed. U doet mee door de online vragenlijst in te vullen, dat is belangrijk!
Als u als praktijk niet meedoet door middel van de online vragenlijst, zal dit worden vastgelegd. Door het KIS heeft een datalek in een huisartsenpraktijk ook gevolgen voor de regio, deze verantwoordelijkheid kan door Synchroon niet genomen worden in dien een praktijk geen actie onderneemt.


Binnen dit contract wordt het volgende geregeld:
- Ondersteuning bij het tijdig melden van een datalek
- Ondersteuning bij overige incidenten op het gebied van informatiebeveiliging
- Bijhouden, aanmaken van verwerkingenregister.
- Functionaris Gegevensbescherming
- Ondersteuning bij geheimhoudingsverklaringen voor medewerkers, een format vindt u hier
- Afsluiten verwerkersovereenkomst (VitalHealth, Minddistrict, HIS). Wellicht heeft u al een getekende verwerkersovereenkomst met de HIS leverancier, deze kunt u dan in uw portaal van PrivacyZorg zetten.

**Wie is er verantwoordelijk voor de gegevensverwerking?**
Dit is de verwerker (in 99,9% van de gevallen gelijk aan de (rechts)persoon waarop het kvk-nummer geregistreerd staat). Indien praktijken een eigen kvk-nummer hebben en gezamenlijk een HOED vormen, dan is dus de individuele praktijk verantwoordelijk.



**Enkele praktijkvoorbeelden rondom AVG:**
- Praktijk A en B delen gezamenlijk een assistente. Assistente veroorzaakt bij B een datalek, dan is praktijk B verantwoordelijk.
- Bij een datalek dient de verantwoordelijke de patiënt te informeren, dit altijd in overleg met PrivacyZorg. Indien het een 'serieus' datalek is maakt PrivacyZorg een apart telefoonnummer aan waarop de betrokkenen kunnen bellen.
- Soms zijn er meerdere wetten die spelen. Bijvoorbeeld. Dient een waarnemer een geheimhoudingsverklaring te tekenen? Een waarnemer heeft namelijk ook beroepsgeheim. Klopt. Het advies is echter om toch een geheimhoudingsverklaring te laten tekenen.
- Een NAS (voor opslag van data) is zo handig omdat deze veel open verbindingen heeft. Een NAS 'zuigt als een teek alle beveiliging weg'. Advies: ben hier erg voorzichtig mee en laat u goed adviseren!
- Indien een computer alleen achtergelaten wordt, lock deze dan.
- Bij papieren dossiers is het lastig bij te houden wie er in heeft gekeken, een log is dus moeilijk bij te houden. Het is wel zaak deze dossiers te beveiligen, dus in ieder geval de kast afsluiten. Het is onduidelijk hoe lang een papieren dossier bewaard dient te blijven, daarover is onduidelijkheid tussen de verschillende aanwezigen. Uitgangspunt lijkt te zijn: 15 jaar tenzij er reden is van deze norm af te wijken. Indien u hier vragen over heeft, richt u zich dan tot PrivacyZorg.
- Bij een MDO worden patiëntgegevens besproken met mensen die hier geen behandelrelatie mee hebben. Hier botsen praktijk en wetgeving met elkaar. Advies is om specifiek te zijn bij het informeren. Wettelijk gezien mag gegevensoverdracht enkel plaatsvinden binnen de behandelrelatie. Indien gemeente is aangesloten dient er goed over nagedacht te worden wat er wel en niet gedeeld wordt.


- Een voorbeeld: indien een patiënt toestemming geeft zijn dossier te delen met Google, dan mag dit dus wel. Toestemming is dus essentieel!
- Is een fax veilig? De point-to-point verbinding van een fax is veilig. Het gaat er dus om waar de ontvangend fax staat.
- De HOV of ziekenhuis stuurt een foutief bericht (bijvoorbeeld doordat huisartsen dezelfde achternamen hebben of doordat patiënt van huisarts is gewisseld zonder dat dit geregistreerd is in het ziekenhuis). Advies van de functionaris gegevensbescherming is om dit wel te melden bij PrivacyZorg. Overigens, HOV of ziekenhuis is verantwoordelijk voor het foutief versturen.

**Wat dient u zelf te doen?**

- Het nummer en de naam van de functionaris gegevensbescherming op de eigen website vermelden. Synchroon heeft een functionaris voor de gegevensbescherming aangemeld bij de autoriteit. Deze gegevens dient u dus op uw eigen website zetten: *Praktijk …. heeft een functionaris voor de gegevensbescherming aangemeld bij de autoriteit (AP) onder nummer FG001912. Contactgegevens:*
*Ing. P.W.A. Schell MA*
*Strichting PrivacyZorg*
*https://www.privacyzorg.nl/*
*info@privacyzorg.nl*
*0800 - 1090*


-Een Eventueel datalek melden bij PrivacyZorg
- Relevante stukken delen met PrivacyZorg zodat u een compleet register heeft, bijvoorbeeld geheimhoudingsverklaringen en verwerkersovereenkomsten. Het is niet noodzakelijk om gehele contracten te delen, enkel een bijlage met geheimhouding getekend is voldoende als voorbeeld. U kunt deze documenten uploaden in het portaal van PrivacyZorg:
https://www.privacyzorg.nl/web/login
- Geheimhoudingsverklaringen afsluiten met personeelsleden
- In veel gevallen worden gegevens van medewerkers aan een verwerker beschikbaar gesteld (verzekeraar, ARBO dienst, loonadministratie en/of accountant). Het gaat dus om personeelssystemen 'buiten de deur'. Daar waar dat het geval is, dienen ook afspraken te worden gemaakt met betrokkenen, waarbij de eisen van de AVG worden gevolgd. U dient zelf uw verzekering, ARBO dienst, salarisadministratie of accountant te informeren.
- Met PrivacyZorg is geen verwerkersovereenkomst nodig: er is een rechtmatige grondslag bij PrivacyZorg, dus geen extra overeenkomsten voor nodig.
- Denk na over inlog management. Dus hoe gaan we om met wachtwoorden en hoe vaak verversen we deze. Een briefje op de computer met het wachtwoord is niet meer van deze tijd!

Eerder hebben we een overzicht gemaakt van zaken die geregeld dienen te worden inzake AVG. We hebben geprobeerd dit in een pragmatisch overzicht te zetten:
http://www.synchroon.info/nieuws/16-04-2018_privacywetgeving/

**Is een functionaris gegevensbescherming verplicht?**

Voor een zorggroep altijd. Voor een huisartsenpraktijk vanaf 10.000. Elke praktijk heeft een functionaris gegevensbescherming via PrivacyZorg.

**Hoe weet ik of ik het goed doe?**

Vanuit PrivacyZorg gaan we kijken naar de mogelijkheden om een visitatie te doen.
Deze kosten zijn dan voor de praktijk zelf. Informatie hierover volgt later.

**Is er een advies rondom back-ups?**

Er zijn cloud systemen, waarmee een back-up gerealiseerd wordt (bijvoorbeeld Medicom).
Er zijn ook systemen die data lokaal bewaren. Het advies is daar om op de volgende manier back-ups

te maken:
Maak drie back-ups van de laatste drie maanden, dus in april heeft u een back-up van januari, februari en maart. In mei maakt u een back-up van april en die van januari kan verwijderd worden. Mocht er een virus of andere beschadiging zijn dan heeft u keuze.
Bovendien is het advies om een dubbele back up te hebben, dus binnen en buiten het pand.


**Hoe wordt er 'omgegaan' met een datalek?**
De belangrijkste vraag is, heb je gedaan wat je dient te doen? Dus:
1. Er is geen fundamentele schending van privacy rechten (hoogste prioriteit)
2. Een incident is gemeld (lagere prioriteit)
Er is nog weinig jurisprudentie op dit gebied, dus wat dat betreft is het nog afwachten.
Bovendien, een datalek is niet enkel een lek, het gaat ook om verlies van data!

**Hoe ga ik om met mail?**
BELANGRIJK: maak geen gebruik van gratis mailboxen (live, gmail, hotmail). Want bij deze mailboxen is er inzagemogelijkheid. Gegevens kunnen dus gescand worden op woorden! Bovendien gaat het vervoer over Amerikaanse servers en data worden daar gegevens opgeslagen, dat mag niet. Dit kan dus gezien worden als een ansichtkaar versturen die elke postbode kan lezen. Er is geen sleutel nodig tot inzage.

Het beste is om veilige mail te gebruiken. Daarna in ieder geval betaalde mail. Nogmaals. Het vervoer is op zich niet zo spannend, inzagemogelijkheid zeker wel! PrivacyZorg komt met een beveiligd mailen optie. Zodra deze er is, informeren we u hierover.

**Woordenlijst:**

**AVG:**
Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat in de hele Europese Unie (EU) dezelfde privacywetgeving geldt. De Wet bescherming persoonsgegevens (Wbp) geldt niet meer. De AVG is ook wel bekend onder de Engelse naam: General Data Protection Regulation (GDPR).

**Datalek:**
Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie.

**Functionaris Gegevensbescherming:**
Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming.

**Lock:**
De computer vergrendelen, zodat er geen toegang is tot de data.

**Point-to-point:**
Refereert naar een type netwerk communicatie waarbij informatie van 1 punt naar 1 specifiek ander punt gestuurd wordt.

**Verwerker:**
Verwerken is: alle handelingen die een organisatie kan uitvoeren met persoonsgegevens, van verzamelen tot en met vernietigen.
Dit is dus een zeer ruim begrip. Handelingen die er volgens de Algemene verordening gegevensbescherming (AVG) in ieder geval onder vallen, zijn: het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen van gegevens

**Verwerkersovereenkomst:**
Een verwerkersovereenkomst regelt de verantwoordelijkheden bij de verwerking van persoonsgegevens **als een bedrijf voor de verwerking een derde partij inschakelt**.

**Verwerkingenregister:**
Het register van verwerkingsactiviteiten bevat informatie over de persoonsgegevens die u verwerkt. De AVG schrijft voor welke informatie u als verantwoordelijke of verwerker in het register moet zetten. Als de Autoriteit Persoonsgegevens (AP) daar om vraagt, moet u het register direct kunnen laten zien.