# Memo

**Aan:**
Alle betrokkenen

**Van:**
DPO PALGA

**Kopie aan:**
-

**Telefoonnummer**
088 – 04 02 700

**Datum**
23 april 2018

**Onderwerp:**
Frequently Asked Questions GDPR

## 1. Wat is de AVG/GDPR, en wat verandert er?

De GDPR is een harmonisering van de Europese wetgeving zodat alle burgers in Europa dezelfde rechten krijgen, en voor aanbieders van diensten er minder naar lokale wetgeving gekeken hoeft te worden. De overheid heeft aangegeven dat de invoering van de GDPR zoveel mogelijk “beleidsneutraal” wordt doorgevoerd: men wil dus geen inhoudelijke wijzigingen van wetgeving en-passant meenemen maar alleen het Europese framework adopteren. Dus inhoudelijk zal gelden dat wat vroeger mocht, straks nog steeds mag, en wat niet mocht, nog steeds niet mag. Wat wel gebeurt is dat zaken die vroeger door middel van jurisprudentie al door rechters waren bepaald nu expliciet in de wet worden vastgelegd.

Er is voor Nederland wel sprake van een fundamentele wijziging in de omgang met informatiebeveiliging/privacy: als verantwoordelijke moeten zaken expliciet vastgelegd worden en moet de patiënt kunnen zien en beslissen hoe er met zijn gegevens wordt omgegaan. Ook geldt dat er voor ziekenhuizen een Data Protection Officer aangesteld moet zijn, die vanuit zijn rol uiteraard vragen stelt over de legitimiteit van bepaalde zaken.

## 2. Waar moet ik beginnen?

De meest eenvoudige stap is het kijken op de website van de Autoriteit Persoonsgegevens, die op haar website een stappenplan heeft staan[1]. Enkele zaken zijn van belang, die eigenlijk voor alle pathologie afdelingen hetzelfde zijn, en die beschrijven we hier. De belangrijkste stappen zijn het inventariseren van de gegevensstromen en kijken hoe daar de belangen van de patiënt zijn gewaarborgd. Op enkele onderwerpen kunnen we als PALGA wel onze visie beschrijven.

## 3. Waar gaan de patiëntgegevens heen?

Het is voor de GDPR van belang om de verschillende gegevensstromen te inventariseren. De belangrijkste is uiteraard die van de patiënt-/onderzoeks-informatie. Bedenk dat informatie ook verder gedeeld wordt buiten het ziekenhuis om, rechtstreeks vanuit de pathologie afdeling. Bij PALGA bekende afnemers zijn:

1. **De aanvrager / ziekenhuis of huisarts**: dit vindt plaats binnen een expliciete behandelrelatie op basis van een doorverwijzing (grondslag is uitvoering contract en de WGBO).

[1] Zie https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/voorbereiding-op-de-avg

2. **Uitbesteding** van onderzoek, 2nd opinion, etc.: ook hier ligt een behandelrelatie aan ten grondslag waar werk wordt uitbesteed aan de derde partij (grondslag is uitvoering contract en de WGBO).
3. De uitwisseling van de informatie voor **landelijke patiëntenzoekvragen**: onderzoeken worden potentieel met andere labs gedeeld als het voor de behandeling van de patiënt noodzakelijk is. Hierbij treedt de patholoog op als medebehandelaar van de patiënt, (zoals bedoeld in artikel 457, lid 2 van de WGBO). Hierbij wordt opgemerkt dat voor het stellen van een landelijke zoekvraag een behandelrelatie met de patiënt noodzakelijk is, wat wordt getoetst doordat de gegevens via de landelijke pathologie infrastructuur alleen gedeeld worden als de patholoog een onderzoeksdossier in zijn eigen afdeling heeft aangemaakt én daarin de naam, geboortedatum en/of BSN heeft opgenomen.
4. De **wetenschappelijke database** van PALGA. De GDPR beschouwt het hergebruik van rapportages ten behoeve van wetenschappelijk onderzoek als “verenigbaar” (overweging 50 en artikel 5 AVG, artikel 458 WGBO en artikel 24 uitvoeringswet AVG), waarbij uiteraard passende maatregelen ter bescherming van de gegevens moeten worden genomen. Dit is geregeld doordat deze gegevens al gepseudonimiseerd worden vóórdat ze het ziekenhuis verlaten, zodat de gegevens niet herleidbaar zijn naar de patiënt. Dit betekent dat er geen expliciete toestemming nodig is van de patiënt voor het gebruik van deze gegevens voor wetenschappelijk onderzoek.
5. **Panels**: dit bevat geen identificerende gegevens, en zijn primair bedoeld voor opleiding en bijscholing, met ook een deel diagnostisch nut voor de patiënt. Doordat deze panels geen herleidbare patiëntinformatie bevatten, en de medische historie door de panelvoorzitter wordt gescreend, wordt deze als weinig risicovol voor de privacy van de patiënt gezien.
6. **Externe partijen** zoals:
    a. **Screeningorganisaties** voor het bevolkingsonderzoek,
    b. **DICA**,
    c. **IKNL**.

    Hier liggen in het algemeen individuele contracten tussen het ziekenhuis of pathologieafdeling en de externe partij aan ten grondslag die bepalen waarom en hoe deze informatie wordt uitgewisseld.

**4. Is nu overal toestemming van de patiënt nodig?**

Voor alle verwerking van persoonsgegevens is een grondslag nodig: een wettelijk geaccepteerde reden om de gegevens te mogen verwerken. Eén van die grondslagen is “toestemming van de patiënt”, maar een andere is “Wettelijke verplichting”. Voor de pathologie is de verwerking van onderzoeken van patiënten uiteraard de hoofdstroom van informatie, waarbij er een wettelijke verplichting is om deze vast te leggen én minimaal 15 jaar op een toegankelijke wijze te bewaren (Wet op de Geneeskundige Behandelovereenkomst, WGBO artikel 454, lid 3[2]). Dit is dan ook de wettelijke basis voor vastlegging van alle informatie. Voor vastlegging is geen toestemming van de patiënt noodzakelijk omdat de wet de patholoog verplicht een registratie te voeren, alhoewel dit vaak nog eens overgedaan wordt via de overeenkomst met het ziekenhuis. Voor de doorverstrekking van deze gegevens aan PALGA is ook geen uitdrukkelijke toestemming noodzakelijk (overweging 50 en artikel 5 AVG, artikel 458 WGBO en artikel 24 uitvoeringswet AVG).

[2] Zie ook https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/medisch-dossier

Wel is het zo dat als de patiënt bezwaar maakt tegen deling van zijn informatie, dit gehonoreerd moet worden (artikel 458 lid 2c WGBO). Dit laatste moet via de patholoog, waarbij deze uiteraard het proces moet kennen om dit netjes af te handelen. Ook zal de patiënt op de hoogte moeten zijn van zijn recht, wat waarschijnlijk op ziekenhuisniveau georganiseerd zal zijn.

**5 Rechten patiënten**
De GDPR geeft de patiënt expliciet rechten: de patiënt moet zijn gegevens kunnen inzien, indien nodig corrigeren en desnoods verwijderen. Dit moet uiteraard op de afdeling pathologie geregeld worden hoe deze gegevens ingezien/gewijzigd/verwijderd moeten worden en onder welke voorwaarden dit kan/mag. Ook hier ligt het voor de hand dat dit in het ziekenhuis centraal georganiseerd is.

Essentieel is dat er een beschreven proces is, wat op enige wijze bij de patiënt bekend gemaakt is en realistisch is om voor een patiënt te doorlopen. Zoals al gemeld zal dit waarschijnlijk centraal door ziekenhuizen worden ingeregeld. PALGA heeft hiervoor de patiëntfolder beschikbaar.

Pathologie afdelingen die zelfstandig acteren en meerdere opdrachtgevers hebben moeten hier dus wel afspraken maken met de verschillende opdrachtgevers over de inrichting van het proces. Het is hierbij goed denkbaar dat een patiënt zich meldt bij het ziekenhuis en dat er dus gegevens aangepast moeten worden in het laboratorium.

**6. Logging/vastlegging**
Vanuit de GDPR, maar ook al vanuit de huidige wetgeving, moet men vastleggen wie een medisch dossier heeft ingezien. Dit moet op naam/persoon worden vastgelegd. De patiënt krijgt over enkele jaren ook het recht om ook in te zien wie zijn dossier heeft ingezien (Wet Cliëntenrechten bij elektronische verwerking van gegevens). Dit is op zich niets nieuws, en het gemiddelde Laboratorium Informatie Systeem (LIS) zal dit dan ook gewoon doen.

Wel moeten er ook registraties bijgehouden worden voor het verstrekken van informatie. Dus als onderzoeken gedeeld worden met externe partijen (bijvoorbeeld ten behoeve van wetenschappelijk onderzoek of kwaliteitscontrole) dan moet dit ook worden vastgelegd. Opgemerkt wordt dat voor verstrekkingen via PALGA dit in de PALGA portal wordt vastgelegd.

**7. Zijn de gegevens passend beschermd?**
De wet eist dat gegevens passend beschermd zijn op zowel organisatorisch als technisch vlak, en dat er gebruik gemaakt wordt bij principes als “Privacy by Design”.

PALGA hanteert voor alle leveranciers de eis dat ze ISO27001 en/of NEN7510 gecertificeerd zijn. PALGA is zelf ISO27001 gecertificeerd. Hiermee is er in de organisaties die met (anonieme) onderzoeksgegevens omgaan voldoende geborgd. “Privacy by Design” is een vrij complexe materie, en bij PALGA wordt altijd uitgegaan van de privacy van de patiënt. Ook worden alle technische ontwerpen van systemen die in contact komen met medische gegevens extern beoordeeld.

Een deel van de beveiliging van de patiëntgegevens (specifiek de gegevens in het LIS) is de verantwoordelijkheid van het laboratorium. De onderaannemer die namens PALGA werkzaamheden uitvoert is ISO27001 en NEN7510 gecertificeerd en wordt bovendien ook regelmatig door PALGA ge-audit. Echter, het beheer van de omgeving om het LIS heen (netwerkbeveiliging) is een verantwoordelijkheid van het laboratorium zelf.