# Toelichting op het voorbeeld Verwerkingsregister

Het voorbeeld Verwerkingsregister is ingevuld voor een fictieve apotheek. Het kan naar eigen inzicht worden aangepast. We horen graag uw feedback, zodat we het voorbeeld verder kunnen verbeteren.

## Categorieën persoonsgegevens

| *Categorie* | *Bevat* |
|---|---|
| Arbeidsgegevens | Naam, Adres Woonplaats (NAW), BSN, Identiteitsbewijs, Werkprestatie, verzuim/verlof |
| Declaratiegegevens | Patiëntgegevens, verstrekte medicatie en zorgprestaties |
| Etiketgegevens | NAW, geboortedatum en medicatiegegevens |
| Farmaceutisch dossier | Patiënt en medicatiegegevens, incl. Intoleranties, Contra-indicaties en Allergieën (ICA) en labwaarden |
| Financiële gegevens | NAW, BSN, salaris en bankgegevens |
| Medicatiegegevens | Geneesmiddel, dosering en toediengegevens |
| Patiëntgegevens | NAW, BSN, contactgegevensgeslacht, geboortedatum |
| Receptgegevens | NAW, BSN en medicatiegegevens |

Ook andere categorieën kunnen worden gebruikt. Denk er hierbij aan dat het duidelijk moet zijn welke informatie onderdeel uitmaakt van een categorie. Ook hierbij bevelen we aan dit niet te gedetailleerd te maken, om de leesbaarheid van het register te waarborgen.
Aandachtspunt hierbij is dat persoonsgegevens vaak verstopt zitten op plekken waar weinig zicht opis, zoals e-mail postvakken.

## Aanvullende, optionele kolommen

In het voorbeeld zijn een aantal optionele gegevens toegevoegd, naast in de AVG verplichte gegevens. Hiermee worden de verschillende invalshoeken ondersteund en helpt het de Functionaris Gegevensbescherming om zicht te houden op belangrijke afspraken, zoals de verwerkersovereenkomst (zie ook de Beslisboom) en de verantwoordelijke voor de gegevens.

## Samenhang met DPIA

Het verwerkingsregister is de eerste stap om een *Privacy Impact Assessment* (PIA) te maken. Op de hierboven benoemde categorieën van persoonsgegevens is een DPIA van toepassing. Op basis van het benoemde doeleinde kan worden beoordeeld of aan de eisen van 'doelbinding' wordt voldaan.

## Samenhang met Risicobeoordeling

Door ook de systemen te benoemen, biedt het verwerkingsregister tegelijkertijd een opzet voor de gestructureerde Risicobeoordeling waarvan de uitkomst kan worden gebruikt om de maatregelen in het verwerkingsregister te vullen (conform de NEN7510 – Informatiebeveiliging in de zorg).

# Vragen en antwoorden verwerkingsregister

De Algemene Verordening Gegevensbescherming (AVG), die per 25 mei 2018 van kracht wordt, verplicht het bijhouden van een verwerkingsregister. Het verwerkingsregister bevat informatie over de persoonsgegevens die worden verwerkt. Het vervangt de bestaande verplichting uit de Wet Bescherming Persoonsgegevens om gegevensverwerkingen bij de Autoriteit Persoonsgegevens te melden. Het is zodoende een belangrijk instrument om naleving van de AVG als zorgaanbieder aan te tonen.

## Wat moet er in het verwerkingsregister staan?

Het verwerkingsregister is vooral bedoeld om inzichtelijk te maken welke persoonsgegevens, met welk doel, hoe lang en door wie worden gebruikt. Hoe dit register er precies uit ziet wordt niet voorgeschreven, maar de volgende onderdelen zijn verplicht:

- *Contactgegevens. De naam en contactgegevens van de eigen organisatie (Verantwoordelijke) en de eigen Functionaris voor de Gegevensbescherming (FG).*
- *Categorieën van betrokkenen van wie gegevens worden verwerkt. Bijvoorbeeld personeel en patiënten.*
- *Categorieën van persoonsgegevens[1], zoals administratieve gegevens, medische gegevens, camerabeelden of IP-adressen.*
- *Bewaartermijnen. De (voorgenomen) termijn waarna u de gegevens moet wissen.*
- *Categorieën van ontvangers aan wie de persoonsgegevens worden verstrekt.*
- *Doel. Het doel van de verwerking van deze gegevens.*
- *Maatregelen. Een algemene beschrijving van de technische en organisatorische maatregelen die u hebt/heeft genomen om persoonsgegevens die u verwerkt te beveiligen.*

Daarnaast dient u te kunnen aantonen of de verwerking rechtmatig is, dus dient tevens de *wettelijke grondslag* genoteerd te zijn.

## Aanpak: hoe wordt het register ingevuld?

Verschillende wegen leiden tot een volledig ingevuld verwerkingsregister:

- Vanuit de *aanwezige systemen* kan worden bedacht welke categorieën van gegevens van welke categorieën van personen door welk systeem en met welk doel worden verwerkt en door wie.
- Vanuit de *werkprocessen* kan worden bedacht welke categorieën van gegevens van welke categorieën van personen door wie waar in het proces en met welk doel worden verwerkt.
- Ook kan vanuit de onderdelen van het verwerkingsregister zelf, bijvoorbeeld *categorieën van gegevens* of *personen* kan worden gedacht, wie daar met welk doel wat mee doet.

We bevelen aan om hier de tijd voor te nemen, en er met een aantal personen met een verschillende invalshoek over te spreken, zodat een compleet beeld ontstaat. Hierbij moet ervoor worden gewaakt dat het overzicht niet te gedetailleerd wordt. Dit kan worden voorkomen door de gegevens te bundelen rondom het doel van de registratie.

## Wettelijke grondslag: wettelijke verplichting of toestemming?

In het verwerkingsregister wordt ook aangegeven of er voor de betreffende verwerking een wettelijke grondslag is, zoals een behandelovereenkomst of een wettelijke verplichting, zoals voor

[1] Wanneer de gegevens met een land of internationale organisatie buiten de Europese Economische Ruimte worden gedeeld, dan moet dit expliciet in het register worden aangegeven.

de Zorgverzekeringswet. Als deze er niet is, dan moet in veel gevallen toestemming worden gevraagd voor de verwerking van de gegevens. Dit geldt bijvoorbeeld voor het gebruik van (patiënt)gegevens voor onderzoek.

## Wat zijn logische bewaartermijnen?

Vanuit de WGBO wordt een bewaartermijn van 15 jaar gehanteerd voor patiëntgegevens. Voor financiële en fiscale bestanden geldt een bewaartermijn van 7 jaar. Voor tijdelijke bestanden en gepseudonimiseerde bestanden wordt aanbevolen om die zo kort mogelijk te bewaren. Bedenk daarbij dat pseudonimisering op vrij korte termijn al onveilig kan zijn (‘gekraakt’ worden). Voor sommige (tijdelijke) bestanden kan aan een praktische termijn worden gedacht. Zo is een bewaartermijn van 13 maanden voor jaarlijks terugkerende processen soms praktisch