

### Inleiding

Peridos bevat persoonsgegevens van zwangeren die deelnemen aan de prenatale screening en van zorgverleners die werkzaamheden uitvoeren in het screeningsproces. Een persoonsgegeven is een gegeven aan de hand waarvan een persoon kan worden geïdentificeerd. Een persoon kan worden geïdentificeerd als degene die het persoonsgegeven gebruikt de persoon kan identificeren zonder een bijzondere inspanning te leveren.

In Peridos worden zowel *algemene* -als *bijzondere persoonsgegevens* vastgelegd. De wet onderscheidt *bijzondere persoonsgegevens* van *algemene* persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens die zo gevoelig zijn dat de verwerking ervan iemands privacy ernstig kan beïnvloeden. Dergelijke gegevens mogen daarom alleen onder zeer strenge voorwaarden worden verwerkt.<sup>1</sup> Voorbeelden van bijzondere persoonsgegevens zijn gegevens die iets zeggen over iemands gezondheid, ras, godsdienst, strafrechtelijk verleden of seksuele leven. Maar ook voor algemene persoonsgegevens geldt, dat deze op een dusdanige manier moeten worden verwerkt dat een passende beveiliging ervan gewaarborgd is. Denk bijvoorbeeld aan het inzien of uitwisselen van de combinatie naam/geboortedatum/BSN, waarmee een kwaadwillende identiteitsfraude zou kunnen plegen.

Het is daarom essentieel dat de gegevens in Peridos op een goede manier worden beveiligd en dat alleen bevoegde personen toegang hebben tot Peridos (authenticatie) en dat die personen alleen toegang hebben tot relevante gegevens (autorisatie).

### Autorisatie

Voor het gebruik van gegevens kent Peridos een aantal rollen. Aan elke rol zijn één of meerdere rechten gekoppeld die aangeven welke onderdelen van Peridos voor die rol toegankelijk zijn. Een counselor heeft bijvoorbeeld andere rechten dan een SEO-echoscopist of een ondersteunend zorgverlener. Elke Peridos gebruiker heeft één of meerdere rollen en heeft op die manier toegang tot de voor die rol(len) relevante functionaliteit en gegevens.

### Authenticatie

Om in Peridos in te loggen is in het verleden gekozen voor een gebruikersnaam en wachtwoord. Peridos accounts zijn strikt persoonlijk en eventueel ook gekoppeld aan persoonlijke opleidingsgegevens en een kwaliteitsovereenkomst. Gezien de aard van de in Peridos vastgelegde gegevens vormt deze manier van inloggen op dit moment een relatief zwakke plek in de beveiliging van die gegevens. De afgelopen tijd zijn er regelmatig voorbeelden in het nieuws geweest waarbij hackers in het bezit zijn gekomen van gebruikersnamen en wachtwoorden. Via deze gebruikersnamen en wachtwoorden kunnen onbevoegden dan ongeoorloofd toegang krijgen tot vertrouwelijke informatie.<sup>2</sup>

De Autoriteit Persoonsgegevens (AP) en het Nationale Cyber Security Centrum (NCSC) geven aan dat de toegang tot gevoelige gegevens extra beveiligd dient te worden: er moet sprake zijn van een

---

<sup>1</sup> <https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens>

<sup>2</sup> Bijvoorbeeld: <https://radar.avrotros.nl/nieuws/item/hacker-zet-zoekmachine-met-miljoenen-nederlandse-wachtwoorden-online/>



---

unieke gebruikersidentificatie en er moet sprake zijn van zogenaamde twee-factor-authenticatie voor toegang tot de applicatie.<sup>3</sup>

#### Twee-factor-authenticatie

Twee-factor-authenticatie (2FA) is een veilige(re) manier van inloggen. De identiteit van de gebruiker wordt hierbij vastgesteld door middel van twee factoren. Het digitale slot wordt als het ware niet met één sleutel, maar met twee sleutels geopend. Dit betekent dat naast het invoeren van een gebruikersnaam en wachtwoord (de eerste sleutel), er nog een tweede sleutel of factor nodig is. Dit kan bijvoorbeeld in de vorm van een code die wordt gegenereerd door een app of een token.

Een bekend voorbeeld van twee factor authenticatie wordt gebruikt bij het pinnen van geld. De eerste factor voor bepaling van de identiteit is het invoeren van een bankpas (een voorwerp dat alleen de betrokkene heeft). De tweede factor is het invoeren van een pincode (een code die alleen de betrokkene weet).

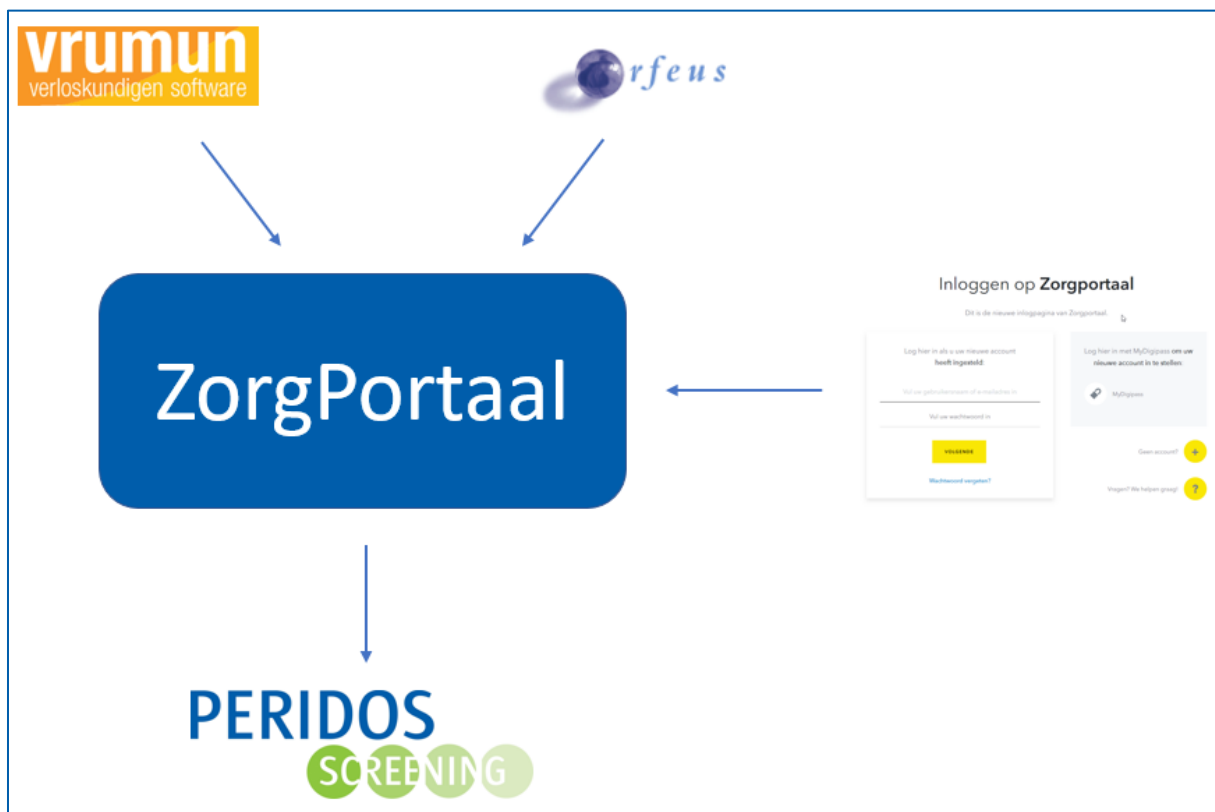
#### Twee-factor-authenticatie in Peridos

Gezien het bovenstaande is het voor Peridos noodzakelijk dat gebruikers gaan inloggen via 2FA. Hiervoor wordt gebruik gemaakt van Zorgportaal, een dienst die de leverancier van Peridos aanbiedt en waar ook andere (zorg)systemen op kunnen worden aangesloten. Zorgportaal fungeert hierbij als een zogenaamde identity-provider, ofwel een applicatie die de identiteit vaststelt en deze identiteit doorgeeft aan de aangesloten systemen. Voor Peridos gebruikers gaat dit inhouden dat zij niet meer inloggen in Peridos, maar in Zorgportaal. Vanuit Zorgportaal wordt dan een verbinding naar Peridos gelegd.

---

<sup>3</sup> <https://autoriteitpersoonsgegevens.nl/nl/nieuws/apothekers-treffen-privacybeschermende-maatregelen-na-onderzoeken-cbp>  
<https://autoriteitpersoonsgegevens.nl/nl/nieuws/huisartsenposten-verbeteren-beveiliging-na-onderzoek-cbp>  
[https://www.nctv.nl/binaries/Factsheet%20gebruik%20tweefactorauthenticatie\\_tcm31-242994.pdf](https://www.nctv.nl/binaries/Factsheet%20gebruik%20tweefactorauthenticatie_tcm31-242994.pdf)





Aanmelden bij Zorgportaal kan op verschillende manieren:

- Gebruikers die ingelogd zijn in Vrumum of Orfeus zijn ook aangemeld bij Zorgportaal. Vanuit het bronsysteem kan dan direct, zonder opnieuw in te moeten loggen, Peridos worden geopend. Hoe dit werkt is per bronsysteem verschillend.
- Gebruikers kunnen rechtstreeks inloggen in Zorgportaal en worden dan verder geleid naar Peridos. Om in te kunnen loggen is een e-mail adres nodig en een wachtwoord (beiden op te geven in het registratieproces) en de tweede factor. Voor de tweede factor is er voor Peridos keuze uit de volgende twee mogelijkheden (een gebruiker kan maar één methode gebruiken):
  - Een gratis app die op de smartphone wordt geïnstalleerd en die codes genereert.
  - Een hardware token, dit is een klein apparaatje wat de codes op een schermje genereert. Zo'n hardware token kan bij CLBPS worden aangevraagd en is niet gratis. Een hardware token is, net als het account waarbij het wordt gebruikt, strikt persoonlijk.

Meer informatie

- Een beschrijving van het registratieproces is te vinden in het document <http://www.peridos.nl/wp-content/uploads/2021/11/02.06-20211109-Beschrijving-2FA-registratie-ZorgPortaal-v1.4.pdf>
- Het bestellen van een hardware token kan via [https://www.peridos.nl/hardware\\_token/](https://www.peridos.nl/hardware_token/)
- Op de Peridos website: <https://www.peridos.nl/zorgportaal> zijn de hier genoemde documenten (inclusief dit document) te vinden. Daarnaast wordt een aantal vragen beantwoord en is aangegeven waar eventuele vragen kunnen worden gesteld.

