Zorginstituut Nederland

Blockchain in de zorg passend binnen de AVG

Hoe maak je blockchain in de zorg AVG-proof?

Ontwerpfase

1. Verricht een DPIA om de concrete privacyrisico's van de blockchain in kaart te brengen
2. Ontwerp de blockchain overeenkomstig de beginselen van privacy by design & default
3. Zorg bij voorkeur dat de transacties in de blockchain geen persoonsgegevens bevatten (de (gehashte) public key uitgezonderd), bijv. door het gebruik van pointers naar off-chain opgeslagen persoonsgegevens die zelf ook geen persoonsgegevens bevatten; óf, indien dit niet mogelijk is, beperk de persoonsgegevens in transacties tot een minimum en hash en versleutel deze persoonsgegevens voor niet-geautoriseerde gebruikers

Inrichting besloten blockchain

4. Stel vast welke gebruikers van de blockchain handelen als verwerkingsverantwoordelijke of verwerker
5. Bepaal of de verwerkingsverantwoordelijken een voldoende wettelijke grondslag hebben voor het verwerken van de persoonsgegevens
6. Zorg voor een controleproces dat borgt dat geen sprake is van internationale doorgifte, dan wel dat eventuele internationale doorgifte in lijn is met de AVG
7. Leg de verplichtingen en bevoegdheden van de verwerkingsverantwoordelijken vast in een onderlinge regeling. Sluit met de verwerkers verwerkersovereenkomsten
8. Stel vast of het noodzakelijk is om een super user aan te wijzen
9. Beveilig de blockchain op een passende wijze
10. Zorg dat uitvoering kan worden gegeven aan de rechten van de betrokkenen. Een belangrijk onderdeel hiervan is het recht op beperking en verwijdering

Aan de materiële toepassingscriteria van de AVG is voldaan zodra binnen de blockchain persoonsgegevens worden verwerkt, bijvoorbeeld:

- In de header en de inhoud van het blok
- Met de public key die is opgenomen in het blok
- Met de private key
- In het smart conract

Ga er zekerheidshalve vanuit dat het versleutelen en/of hashen van persoonsgegevens weliswaar een beveiligingsmaatregelen vormt maar er niet voor zorgt dat er geen persoonsgegevens worden verwerkt

Blockchains in de zorg zijn meestal nationaal of EU georiënteerd en vallen daardoor binnen de territoriale reikwijdte van de AVG

Het enkel raadplegen van persoonsgegevens vormt een verwerking van persoonsgegevens

Wie verwerken persoonsgegevens?

- De (nodes van) geautoriseerde gebruikers
- De niet-geautoriseerde gebruiker die de hash van de inhoud van de blokken verwerkt

Stel per geautoriseerde gebruiker vast of een doorbrekingsgrond en wettelijke grondslag bestaat voor het verwerken van (bijzondere) persoonsgegevens aan de hand van:

1. Medisch beroepsgeheim
2. De doorbrekingsgronden voor bijzondere persoonsgegevens
3. De doorbrekingsgronden voor de verwerking van strafrechtelijke gegevens
4. De algemene en bijzondere wettelijke grondslagen
5. De wettelijke mogelijkheden voor de verwerking van nationale identificatienummers

Blockchain in de zorg passend binnen de AVG

Rechten van de betrokkene
Tref technische en organisatorische maatregelen om uitvoering te kunnen geven aan de rechten van de betrokkene:
- recht op inzage
- recht op correctie
- recht op wissing
- recht op beperking van de verwerking
- recht op dataportabiliteit

Het beginsel van opslagbeperking
- Na het verlopen van de bewaartermijn moeten persoonsgegevens verwijderd worden
- Volledige verwijdering van persoonsgegevens kan slechts bij het gebruik van pointers (verwijzing) of bij gebruik van één blockchain per persoon als die gehele blockchain wordt verwijderd
- Voor zover persoonsgegevens op de blockchain zijn opgenomen, en de gehele blockchain niet wordt verwijderd, kunnen persoonsgegevens slechts onomkeerbaar ontoegankelijk worden gemaakt

Een besloten (permissioned) blockchain is het best passend in zorg

Onderlinge regeling tussen de gezamenlijke verwerkings-verantwoordelijke gebruikers
Maak daarin onder meer afspraken over:
- het informeren van betrokkenen
- tot wie de betrokkenen zich kunnen wenden voor de uitoefening van hun rechten
- het gezamenlijk afhandelen van datalekken
- welke toegangsprocedure voor de blockchain geldt
- de beveiliging van de blockchain
- hoe de onderlinge regeling bekend wordt gemaakt aan de betrokkene

Privacy by design & default
Onder meer:
- Integreer privacy in het technisch én organisatorische ontwerp van de blockchain
- Zorg voor standaardinstellingen die een zo hoog mogelijke privacy-bescherming aan de betrokkene biedt
- Zorg voor privacymanagement en doorlopende beveiliging

Zet geen persoonsgegevens in de blockchain en voor zover dat niet kan beperk het tot een minimum

Ga er zekerheidshalve van uit dat een hash een gepseudonimiseerd persoonsgegeven is