PELS RIJCKEN

# Rapport Blockchain in de zorg in relatie tot de AVG

Marte van Graafeiland & Tim Gillhaus

20 februari 2019

# Wie zijn wij?

LedgerLeopard
your blockchain partner

PELS RIJCKEN

## Jeroen van Megchelen

- T: +31 642450786
- E: jeroen.van.megchelen@ledgerleopard.com
- LinkedIn

## Marte van Graafeiland

- T: +31 70 5153 830
- E: marte.vangraafeiland@pelsrijcken.nl
- LinkedIn

## Tim Gillhaus

- T: +31 70 5153 903
- E: tim.gillhaus@pelsrijcken.nl
- LinkedIn

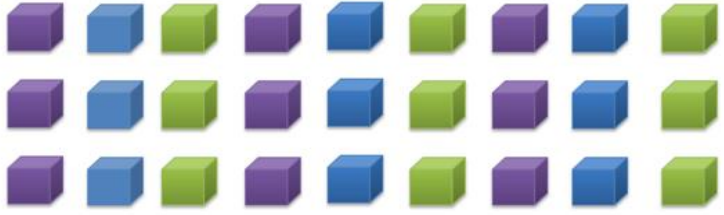
# Inleiding

- **VOOR WIE IS DIT RAPPORT BEDOELD?**
  - juristen en informatiemanagers in de zorg die voornemens zijn gegevens via blockchain te verwerken;
  - bouwers van blockchains worden gebruikt om reeds bij het ontwerp en de bouw van de blockchain ervoor te zorgen dat deze in overeenstemming is met de vereisten van de AVG;
  - Enige basiskennis van de AVG is vereist.

- **HOE IS DIT RAPPORT TOT STAND GEKOMEN?**
  - Samenwerking tussen Pels Rijcken & Ledger Leopard
    - Pels Rijcken beschrijft de juridische vraagstukken en mogelijke juridische oplossingen
    - Ledger Leopard komt (voor zover noodzakelijk) met technische oplossingen.

**ONDERZOEKSVRAAG**

"Op welke wijze kan het gebruik van blockchain in de zorg in overeenstemming worden gebracht met de regels van de AVG?”



# Conclusie – Blockchain in de zorg en de AVG zijn verenigbaar, maar er zijn wel enkele aandachtspunten

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. •Zet bij voorkeur geen persoonsgegevens in de transactie (bijv. door het gebruik van pointers die ook geen persoonsgegevens bevatten), óf;
   •Beperk de persoonsgegevens in transacties tot een minimum en hash en versleutel deze persoonsgegevens voor niet-geautoriseerde gebruikers.
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.

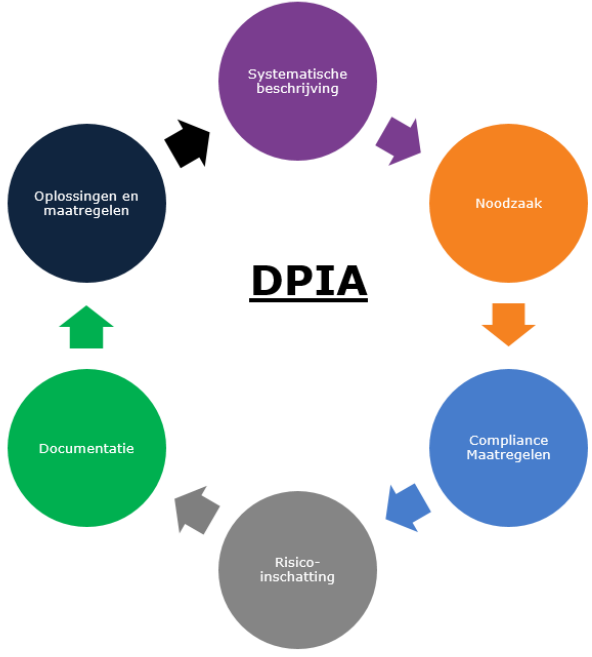
1. **•Verricht een DPIA om de concrete privacyrisico's van de blockchain in kaart te brengen.**
2. •Ontwerp de blockchain overeenkomstig de beginselen van privacy by design & default.
3. •Zet bij voorkeur geen persoonsgegevens in de transactie (bijv. door het gebruik van pointers die ook geen persoonsgegevens bevatten), óf;
   •Beperk de persoonsgegevens in transacties tot een minimum en hash en versleutel deze persoonsgegevens voor niet-geautoriseerde gebruikers.
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.

# 1. Verricht een DPIA

- Bij gebruik van Blockchain is het verrichten van een PIA vrijwel altijd verplicht: nieuwe technologie.

**WAT IS HET DOEL VAN EEN DPIA?**

- In kaart brengen van de mogelijke privacyrisico's, zodat de blockchain zo kan worden ontwerpen dat een zo hoog mogelijke privacybescherming wordt geboden.



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. •Zet bij voorkeur geen persoonsgegevens in de transactie (bijv. door het gebruik van pointers die ook geen persoonsgegevens bevatten), óf;
   •Beperk de persoonsgegevens in transacties tot een minimum en hash en versleutel deze persoonsgegevens voor niet-geautoriseerde gebruikers.
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.

# 2. Privacy by design & default

- **WAT HOUDT PRIVACY BY DESIGN & DEFAULT IN?**
  - Zorgplicht om een zo hoog mogelijke privacybescherming te bieden, geïntegreerd in het ontwerp van de blockchain:
    - Voorkom dat persoonsgegevens worden verwerkt of minimaliseer de persoonsgegevens;
    - Geef de betrokkene zoveel mogelijk controle;
    - Doorlopend verbeteren van de beveiliging

**CONCRETE ORGANISATORISCHE EN TECHNISCHE MAATREGELEN**

Zie voor concrete organisatorische en technische maatregelen paragraaf 5.6 van het rapport.

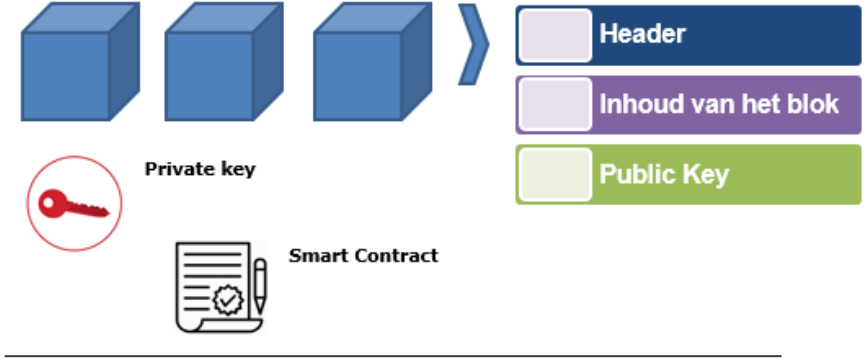
1. **•Verricht een DPIA om de concrete privacyrisico's van de blockchain in kaart te brengen.**
2. **•Ontwerp de blockchain overeenkomstig de beginselen van privacy by design & default.**
3. **•Zet bij voorkeur geen persoonsgegevens in de transactie (bijv. door het gebruik van pointers die ook geen persoonsgegevens bevatten), óf;**
   **•Beperk de persoonsgegevens in transacties tot een minimum en hash en versleutel deze persoonsgegevens voor niet-geautoriseerde gebruikers.**
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.

# 3. Voorkom (of beperk) de opslag van persoonsgegevens

**VOORKOM DE OPSLAG VAN PERSOONSGEGEVENS OP DE BLOCKCHAIN DOOR HET OPNEMEN VAN LINKS NAAR OFF-CHAIN PERSOONSGEGEVENS**

- *Het versleutelen en/of hashen van de persoonsgegevens op de blockchain, maakt in de meeste gevallen niet dat geen persoonsgegevens meer worden verwerkt.*
- *Gelet hierop verdient het de voorkeur om de gegevens op de blockchain te beperken tot pointers naar off-chain persoonsgegevens.*
- *Is dit niet mogelijk? Beperk de persoonsgegevens tot het strikt noodzakelijke en versleutel en hash de persoonsgegevens.*

*Schematische weergave van de volledige blockchain*



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. **•Zet bij voorkeur geen persoonsgegevens in de transactie (bijv. door het gebruik van pointers die ook geen persoonsgegevens bevatten), óf;**
   **•Beperk de persoonsgegevens in transacties tot een minimum en hash en versleutel deze persoonsgegevens voor niet-geautoriseerde gebruikers.**
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.

# 4. Stel vast wie verwerkingsverantwoordelijke of verwerker zijn

**WAAROM?**

- Verwerkingsverantwoordelijken bepalen het doel en de middelen en hebben een eigen wettelijke grondslag nodig.

  ! Doordat een hash vaak een persoonsgegeven is, zal ook voor het verwerken van gehashte transactie een afzonderlijke wettelijke grondslag nodig zijn. Vaak is deze er niet.

- Verwerkers ontlenen hun wettelijke grondslag aan de verwerkingsverantwoordelijke die hem inschakelt.

**BOUWER VAN DE BLOCKCHAIN**

- Afhankelijk van zijn verdere rol kan een bouwer verwekingsverantwoordelijke, verwerker of geen van beide zijn.

## Geautoriseerde gebruikers

Kunnen persoonsgegevens plaatsen en/of raadplegen

- Geautoriseerde verwerkingsverantwoordelijke
- Geautoriseerde verwerker

## Niet-geautoriseerde gebruikers

Hebben geen toegang tot de inhoud van het blok, zien slechts een hash.

Conclusie rapport: mogelijk verwerker.

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. **•Zet bij voorkeur geen persoonsgegevens in de transactie (bijv. door het gebruik van pointers die ook geen persoonsgegevens bevatten), óf;**
   **•Beperk de persoonsgegevens in transacties tot een minimum en hash en versleutel deze persoonsgegevens voor niet-geautoriseerde gebruikers.**
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.

# 5. Wettelijke grondslag

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. **Zet bij voorkeur geen persoonsgegevens in de transactie (bijv. door het gebruik van pointers die ook geen persoonsgegevens bevatten), óf;**
   **Beperk de persoonsgegevens in transacties tot een minimum en hash en versleutel deze persoonsgegevens voor niet-geautoriseerde gebruikers.**
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.

Subtitel tekst & foto

# 6. Voorkom (of reguleer) Internationale doorgifte

- **WANNEER IS SPRAKE VAN INTERNATIONALE DOORGIFTE?**
  - (Node) van de gebruiker bevindt zich buiten de EU.

- **INTERNATIONELE DOORGIFTE (BUITEN DE EU) SLECHTS TOEGESTAAN ONDER STRIKTE EISEN**
  - Richt een controleproces in zodat kan worden gecontroleerd of een gebruiker zich buiten de EU bevindt.
  - Beoordeel of de buitenlandse gebruiker een grondslag heeft voor de internationale doorgifte.

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. **Zet bij voorkeur geen persoonsgegevens in de transactie (bijv. door het gebruik van pointers die ook geen persoonsgegevens bevatten), óf;**
   **Beperk de persoonsgegevens in transacties tot een minimum en hash en versleutel deze persoonsgegevens voor niet-geautoriseerde gebruikers.**
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.

# 7. Het sluiten van een onderlinge regeling & verwerkersovereenkomsten

- De verwerkingsverantwoordelijke gebruikers van de blockchain zijn gezamenlijke verwerkingsverantwoordelijke voor de blockchain als geheel.

- De gezamenlijke verwerkingsverantwoordelijke zullen in een onderlinge regeling onder meer afspraken moeten maken over:
  - de inhoud van de privacyverklaring
  - tot wie de betrokkenen zich kunnen wenden indien zijn hun rechten willen uitoefenen en hoe daar uitvoering aan kan worden gegeven (bijv. een contactpunt);
  - de toegangsprocedure om deel te nemen aan de blockchain;
  - de beveiliging van de blockchain;
  - hoe de onderlinge regeling bekend moet worden gemaakt aan de betrokkenen.

- Tot slot moet met alle gebruikers die optreden als verwerkers (geautoriseerde verwerkers en niet-geautoriseerde gebruikers) verwerkersovereenkomsten worden gesloten.

! Let op blockchain-specifieke eisen.

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. •Zet bij voorkeur geen persoonsgegevens in de transactie (bijv. door het gebruik van pointers die ook geen persoonsgegevens bevatten), óf;
   •Beperk de persoonsgegevens in transacties tot een minimum en hash en versleutel deze persoonsgegevens voor niet-geautoriseerde gebruikers.
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.

# 8. Het aanwijzen van een super user

**Beoordeel of het noodzakelijk is om een super user aan te wijzen**

- Bij een grote hoeveelheid aan verwerkingsverantwoordelijke gebruikers kan het verplicht zijn om een super user aan te wijzen.

- Een super user is een door de verwerkingsverantwoordelijke gebruikers opgerichte/aangewezen (rechts)persoon die (een deel van) de verplichtingen van de gezamenlijke verwerkingsverantwoordelijke gebruikers uitvoert.

- Achtergrond daarvan is (mede) dat de betrokkene anders niet weet tot wie hij zich moet richten.

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. •Zet bij voorkeur geen persoonsgegevens in de transactie (bijv. door het gebruik van pointers die ook geen persoonsgegevens bevatten), óf;
   •Beperk de persoonsgegevens in transacties tot een minimum en hash en versleutel deze persoonsgegevens voor niet-geautoriseerde gebruikers.
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.

# 9. Beveilig de blockchain op passende wijze

**Tref passende beveiligingsmaatregelen**

- De verwerkingsverantwoordelijke gebruikers zijn verplicht om te waarborgen dat de blockchain voldoende is beveiligd.

- De verwerkingsverantwoordelijken kunnen daarbij verschillende organisatorische en technische maatregelen treffen.

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. •Zet bij voorkeur geen persoonsgegevens in de transactie (bijv. door het gebruik van pointers die ook geen persoonsgegevens bevatten), óf;
   •Beperk de persoonsgegevens in transacties tot een minimum en hash en versleutel deze persoonsgegevens voor niet-geautoriseerde gebruikers.
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.

Subtitel tekst & foto

# 10. Rechten van de betrokkene

- Recht op inzage
- Recht op rectificatie
- **Recht op wissing**
- Recht op beperking van de verwerking
- Recht op dataportabiliteit
- Recht op bezwaar

Met name recht op wissing en recht op beperking van de verwerking brengen blockchain-specifieke privacy-uitdagingen met zich mee.

Tref technische maatregelen die het mogelijk maken om zoveel mogelijk invulling te geven aan de (verplichte) verwijdering van persoonsgegevens op de blockchain

**Volledige verwijdering van de persoonsgegevens**

a) Gebruik van pointers – Doorknippen link
b) Volledige vernietiging van de blockchain (voor zover sprake is van een persoonlijke blockchain)

**Ontoegankelijk maken van de gegevens**

a) Vernietiging van de private key door gebruikers
b) Vernietiging van de private key via de smart contract
c) Het door middel van het User Management ontkoppelen van de gebruiker met zijn sleutels

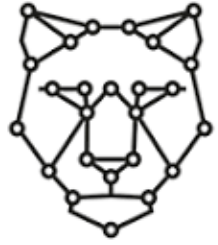
1. •Verricht een DPIA om de concrete privacyrisico's van de blockchain in kaart te brengen.
2. •Ontwerp de blockchain overeenkomstig de beginselen van privacy by design & default.
3. •Zet bij voorkeur geen persoonsgegevens in de transactie (bijv. door het gebruik van pointers die ook geen persoonsgegevens bevatten), óf;
   •Beperk de persoonsgegevens in transacties tot een minimum en hash en versleutel deze persoonsgegevens voor niet-geautoriseerde gebruikers.
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.


## Conclusie

Bovengenoemde aanbevelingen kunnen slechts in een besloten blockchain worden verwezenlijkt.

# Technische oplossingen blockchain

- Betrek juristen bij uw oplossing
- Heb een goede reden voor blockchain
- Privacy by design voor de lange en korte termijn
- Hashes en pointers
- Beveiliging
- De toekomst; ZKP en SSI



LedgerLeopard

your blockchain partner

PELS RIJCKEN


ALGEMEEN

T: +31 70 515 30 00
F: +31 70 515 31 00
E: info@pelsrijcken.nl

BEZOEKADRES

New Babylon
Bezuidenhoutseweg 57
2594 AC Den Haag

POSTADRES

Pels Rijcken & Droogleever Fortuijn N.V.
Postbus 11756
2502 AT Den Haag