Zorginstituut Nederland

LedgerLeopard
your blockchain partner

PELS RIJCKEN

Blockchain in de zorg in relatie tot de AVG

Een onderzoek naar de wijze waarop het gebruik van blockchain in de zorg in overeenstemming kan worden gebracht met de AVG. Uitgevoerd in opdracht van Zorginstituut Nederland.

Sandra van Heukelom-Verhage – Marte van Graafeiland – Tim Gillhaus (Pels Rijcken)
Jeroen van Megchelen (Ledger Leopard)

VOORWOORD VAN HET ZORGINSTITUUT NEDERLAND

Voor u ligt een onderzoek naar de Algemene verordening gegevensbescherming (‘AVG’) in relatie tot blockchain in de zorg.

Zorginstituut Nederland (‘Zorginstituut’ of ‘ZIN’) onderzoekt of en hoe nieuwe technologieën, zoals blockchain, toepasbaar zijn in de zorg. Daarmee beoogt het ZIN de kwaliteit van de gezondheidszorg in Nederland te bevorderen, zodat elke burger toegang houdt tot goede zorg, tegen aanvaardbare kosten.

Eén van de taken van het Zorginstituut is om een bijdrage te leveren aan het op peil houden van de kwaliteit, toegankelijkheid en betaalbaarheid van de gezondheidszorg. Door toenemende digitalisering verandert de omgeving van de zorg. Er ontstaan nieuwe mogelijkheden om processen en informatievoorziening in de zorg in Nederland sneller en soepeler te organiseren en tegelijkertijd de burger meer inzicht en regie te geven.

Het is de verwachting dat blockchaintechnologie in de komende jaren toegepast zal worden in de zorg. Deze nieuwe technologie maakt het mogelijk dat burgers en professionals rechtstreeks gegevens kunnen uitwisselen en delen, wat voordelen oplevert zoals meer transparantie binnen het zorgproces.

Blockchain biedt kansen voor de zorg, maar er is ook behoefte aan kennis van en inzicht in hoe blockchain veilig en verantwoord in te zetten in de zorg. De juridische, organisatorische, maatschappelijke en technische randvoorwaarden waaronder blockchain van waarde kan zijn voor de zorg, vragen specificaties om rekening mee te houden. Er bestaat veel onduidelijkheid over het gebruik van blockchain in relatie tot de AVG. Dit bleek ook uit de reacties die het Zorginstituut ontving op de resultaten van de in 2018 uitgevoerde praktijkproef blockchain in de kraamzorg.

Om duidelijkheid te verschaffen in hoeverre blockchain in de zorg en de AVG te combineren zijn, heeft het Zorginstituut aan Pels Rijcken en Ledger Leopard gevraagd dit te analyseren en handvatten te bieden voor de voorwaarden.

De onderzoeksresultaten bieden meer inzicht in een deel van de juridische kaders waarbinnen blockchain in de zorg kan en mag opereren. De AVG is slechts één van de vele wetten in het speelveld van blockchain in de zorg. Dit onderzoek stelt vast dat de toepassing van blockchain zeker mogelijk is binnen de wettelijke kaders van de AVG, maar dat wel rekening moet worden gehouden met de voorwaarden die de AVG stelt.

Een verantwoorde toepassing van blockchain in de zorg kan bijdragen aan de realisatie van publieke waarden, zoals het toegankelijk en betaalbaar houden van de zorg. Daarnaast kan het de regiepositie van de burger versterken. Dit onderzoek geeft richting aan die verantwoorde ontwikkeling en toekomstige toepassing.

Zorginstituut Nederland
juni 2019
blockchainindezorg.nl

Inhoudsopgave

BEGRIPPENLIJST

Applicatielaag	Het gebruik van blockchain-technologie wordt veelal ondersteund door een gebruikersvriendelijke applicatie, zoals een website, database of app. Een dergelijke applicatielaag vergemakkelijkt het gebruik. Zo kan een gebruiker via de app zien welke gegevens kunnen worden ingevoerd.
Besloten blockchain (private blockchain)	Een blockchain waaraan niet iedereen zonder meer kan deelnemen. Er is een toegangsaanvraag en goedkeuring vereist voor deelname aan de blockchain. Bovendien kunnen de toebedeelde lees- en schrijfrechten per gebruiker en zelfs per transactie verschillen.
Consensusmodel	Het model dat de nodes hanteren om nieuwe blokken aan de blockchain toe te voegen.
Geautoriseerde gebruiker	Een gebruiker van de blockchain die geautoriseerd is om de inhoud van een transactie te raadplegen, dan wel bevoegd is om gegevens op de blockchain te plaatsen.
Geautoriseerde verwerkings-verantwoordelijke	Een geautoriseerde gebruiker die zelfstandig bepaalt of hij persoonsgegevens op de blockchain verwerkt en voor welke doelen hij dat doet. Meer concreet wordt in dit rapport tot uitgangspunt genomen dat: - (de node van) de geautoriseerde gebruiker als verwerkingsverantwoordelijke optreedt voor de persoonsgegevens die hij op de blockchain heeft geplaatst; - (de node van) de geautoriseerde gebruiker verwerkingsverantwoordelijke is voor de persoonsgegevens in de blokken die hij kan raadplegen, wijzigen en/of verwijderen.
Geautoriseerde verwerker	Een geautoriseerde gebruiker die in opdracht van een of meer van de geautoriseerde verwerkingsverantwoordelijken deelneemt aan de blockchain en ten behoeve van hen persoonsgegevens verwerkt op de blockchain.

Hash	Een persoonsgegevens van willekeurige omvang dat door middel van een bepaalde techniek (‘hashing’) wordt omgevormd naar reeks van een vaste grootte.
Header	Ieder blok wordt voorzien van een unieke code. De unieke code verwijst naar de unieke code van het vorige blok.
Encryptie	Het cryptografisch versleutelen van (persoons)gegevens. De versleutelde persoonsgegevens kunnen door het gebruik van de sleutel ontsleuteld worden.
Minen	Het proces waarbij de nodes van een blockchain door middel van een wiskundige berekening een nieuwe blok aan de blockchain toevoegen.
Niet-geautoriseerde gebruikers	Een gebruiker van de blockchain die niet geautoriseerd is om de inhoud van een bepaalde transactie te raadplegen. Een niet-geautoriseerde gebruiker verwerkt slechts een hash van de inhoud van de transactie.
Node	Iedere aan de blockchain gekoppelde computer.
Nonce	Een getal dat door de nodes zal worden gebruikt om een nieuwe blok op de blockchain te zetten.
Off-chain	Persoonsgegevens worden ‘off-chain’ verwerkt indien de persoonsgegevens niet worden verwerkt in de transacties die op de blockchain zijn opgenomen. Hierbij kan worden gedacht aan de situatie dat via pointers naar persoonsgegevens in externe databases wordt verwezen, maar ook aan additionele persoonsgegevens die bijv. in de wallet van de gebruiker worden verwerkt.
On-chain	Persoonsgegevens worden ‘on-chain’ verwerkt indien de persoonsgegevens worden verwerkt in de transacties die op de blockchain zijn opgenomen.
Openbare blockchain	Een blockchain waarbij het iedereen volledig vrij staat

(publieke blockchain)	om eraan deel te nemen. Eenieder kan de software van een node uitvoeren en deze met het blockchainnetwerk verbinden via het internet.
Participating node (light node)	Een node die weliswaar een kopie verwerkt van de blockchain, maar die niet deelneemt aan het consensusmodel en aldus niet bevoegd is om nieuwe blokken aan de blockchain toe te voegen.
Permissioned blockchain	Een blockchain waarbij per specifieke gebruiker lees- en schrijfrechten kunnen worden toebedeeld.
Permissionless blockchain	Een blockchain waarbij iedere gebruiker dezelfde lees- en schrijfrechten heeft.
Proof of stake	Een consensusmodel voor het valideren van transacties op de blockchain, waarbij een specifiek aangewezen (en in de meeste gevallen steeds wisselende) node het consensusmodel uitvoert.
Proof of work	Een consensusmodel waarbij alle validating nodes deelnemen aan het consensusmodel en aldus berekenen of een blok aan de blockchain mag worden toegevoegd.
Pointer	Een URL-link (in de transactie op de blockchain) die verwijst naar persoonsgegevens die off-chain staan opgeslagen.
Private key	Een geheime sleutel van de gebruiker die is gekoppeld met zijn of haar public key. De gebruiker kan met zijn private key de inhoud van de transacties binnen de blockchain - voor zover hij daartoe geautoriseerd is - ontsleutelen.
Public key	De public key wordt per transactie van de gebruiker aan de ontvangende gebruikers meegezonden. De public key is een unieke sleutel die is gekoppeld aan de gebruiker en die bestaat uit een lange reeks getallen en cijfers.
Salt	Een salt is een willekeurig reeks van leestekens die aan persoonsgegevens kunnen worden toegevoegd voordat de persoonsgegevens worden gehasht. Door het toevoegen van een salt wordt het risico verkleind dat

	de hash kan worden gekraakt en de invoerwaarden (de oorspronkelijke, gehashte, gegevens) dus kunnen worden herleid.
Smart contract	Een smart contract is een programmeercode waarin een handeling afhankelijk is gemaakt van het voltrekken van één of meer gebeurtenissen. Een smart contract bestaat in de kern altijd uit een als/dan-constructie. Het is een deterministisch computerprogramma: gegeven een bepaalde input en bepaalde beginwaarden – geregistreerd op de blockchain – zal het altijd dezelfde output genereren. De werking is anders gezegd volledig voorspelbaar.
Single Sovereign Identity (SSI)	Een digitale identiteit die wordt toebedeeld aan een betrokkene en waarmee de mogelijkheid wordt geboden om zelfstandig te bepalen welke gebruikers van de blockchain zijn of haar persoonsgegevens mogen inzien. Bij een dergelijke oplossing krijgt de betrokkene de regie over zijn of haar persoonsgegevens op de blockchain.
Transactie	Een transactie is een informatieregel (blok) op de blockchain. Die informatieregel kan bijvoorbeeld een pointer bevatten, maar kan ook inhoudelijke gegevens bevatten. Geautoriseerde gebruikers zullen de inhoud van de transactie kunnen raadplegen. Voor niet-geautoriseerde gebruikers is, zo wordt in dit rapport tot uitgangspunt genomen, de inhoud van de transactie versleuteld en gehasht en aldus niet raadpleegbaar.
Wallet	De wallet van de gebruiker is de persoonlijke omgeving of de gebruiksvriendelijke applicatie waarmee de gebruiker toegang kan krijgen tot de blockchain. In de wallet kunnen persoonsgegevens over de gebruiker worden bewaard (bijv. de private key van de gebruiker). De persoonsgegevens die in de wallet zijn opgeslagen worden in dit rapport aangemerkt als off-chain persoonsgegevens.
Validating node (full node)	Een node die deelneemt aan het consensusmodel en aldus bevoegd is om blokken aan de blockchain toe te voegen.

Zero Knowledge Proof (ZKP)	Een techniek waarbij via de blockchain een claim wordt getoond, maar niet de informatie die daaraan ten grondslag ligt. Vaak zal het bij ZPK gaan om het voldoen aan een minimumvoorwaarde (bijv. patiënt A is ouder dan 18, of, breder, persoon A voldoet aan de minimumvoorwaarden voor deelname aan de medische test).

INLEIDING

In dit rapport wordt onderzocht op welke wijze het gebruik van blockchain in de zorg in overeenstemming kan worden gebracht met de regels van de AVG.

Dit rapport is primair bedoeld voor juristen en informatiemanagers in de zorg die voornemens zijn gegevens via blockchain te verwerken. Dit rapport kan tevens door 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. Hoewel dit rapport is toegespitst op het gebruik van blockchain in de zorg, zullen de conclusies en aanbevelingen in dit rapport ook relevant kunnen zijn voor blockchains buiten de zorg.

In dit rapport wordt tot uitgangspunt genomen dat u als lezer bekend bent met de definities uit de AVG. Deze definities worden slechts nader toegelicht voor zover dat in relatie tot het gebruik van blockchain relevant is. Er wordt met name stilgestaan bij de vraag op welke wijze de definities van de AVG bij het gebruik van blockchain moeten worden uitgelegd.

Opmerking verdient verder dat er bij blockchain verschillen rechtsvragen spelen die op dit moment nog niet met zekerheid zijn te beantwoorden, omdat de basisbeginselen en uitgangspunten van (de nog relatief jonge) blockchain technologie in combinatie met persoonsgegevens niet altijd aansluiten bij die van de AVG en Uitvoeringswet AVG ('UAVG'). De juridische analyse in dit onderzoek heeft daardoor soms een tentatief karakter. Voorts verdient vermelding dat in dit rapport verschillende oplossingsrichtingen worden genoemd en aanbevelingen worden gedaan voor de inrichting van blockchains in de zorg. Die oplossingsrichtingen en aanbevelingen zijn niet limitatief. Vanzelfsprekend kunnen er ook nog andere oplossingsrichtingen en aanbevelingen zijn.

Opbouw van dit rapport

De volgende onderwerpen komen bij dit onderzoek aan bod:

- in deel I van dit rapport zal worden besproken wat blockchain precies is;
- in deel II wordt toegelicht wanneer de AVG van toepassing is op het gebruik van blockchain in de zorg;
- in deel III komt aan bod wie er persoonsgegevens op de blockchain verwerken en in welke hoedanigheid zij dat kunnen doen: als verwerkingsverantwoordelijke en als verwerker;
- in deel IV wordt stilgestaan bij de vraag op welke wijze kan worden vastgesteld of een gebruiker van de blockchain een wettelijke grondslag heeft voor het verwerken van persoonsgegevens op de blockchain;
- vervolgens zal in deel V worden besproken welke technische en organisatorische maatregelen getroffen zouden kunnen worden om te voldoen aan de materiële vereisten van de AVG;

- tot slot komt in deel VI van dit rapport aan bod hoe de uit de AVG voortvloeiende rechten van de betrokkene bij het gebruik van blockchain (zoveel mogelijk) gewaarborgd kunnen worden.

Conclusies van dit rapport

In dit rapport wordt geconcludeerd dat het gebruik van blockchain in de zorg in overeenstemming lijkt te kunnen worden gebracht met de AVG. De tien belangrijkste aanbevelingen die volgen uit dit rapport zijn de volgende.

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 op 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.

   Kies – gelet op de hierna achter 4 t/m 10 genoemde aanbevelingen – voor een 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.

LEESWIJZER

Deel I – Wat is blockchain

In deel I van dit rapport wordt kort toegelicht wat blockchain precies is.

Deel II – Is de AVG van toepassing op de blockchain?

De AVG is van toepassing indien via de blockchain persoonsgegevens worden verwerkt. Bij het verwerken van gegevens in een blockchain in de zorg zal al snel sprake zijn van verwerking van persoonsgegevens, en zal dus snel aan de materiële eisen voor toepasselijkheid van de AVG worden voldaan (zie paragraaf 2.2 van dit rapport).

Om te kunnen vaststellen of binnen de (beoogde) blockchain persoonsgegevens worden verwerkt, dient aan de hand van deel I van dit rapport te worden nagelopen of verschillende onderdelen van de blockchain persoonsgegevens bevatten (zie paragraaf 2.3 van dit rapport).

De AVG is niet van toepassing op gegevens die zodanig anoniem zijn (gemaakt) dat de persoon waarop ze betrekking hebben niet (meer) identificeerbaar is. Hoewel daar in bepaalde gevallen discussie over mogelijk is, wordt er in dit rapport zekerheidshalve vanuit gegaan dat versleutelen en/of hashen van persoonsgegevens op de blockchain niet maakt dat geen persoonsgegevens meer worden verwerkt, maar dat versleuteling en hashing veeleer kan worden gezien als een beveiligingsmaatregel (pseudonimisering) (zie randnrs. 2.2.7 tot en met 2.2.13 van dit rapport).

Gelet hierop verdient het de voorkeur om de gegevens op de blockchain te beperken tot pointers naar off-chain persoonsgegevens, waarbij de pointers zelf ook geen persoonsgegevens bevatten. Een belangrijk voordeel van deze benadering is dat de AVG niet van toepassing is op de inhoud van de transacties op de blockchain (met uitzondering van de (gehashte) public key die altijd in de transactie zal worden verwerkt).

Voor zover wordt voldaan aan de materiële toepassingscriteria van de AVG (er worden persoonsgegevens verwerkt), dient op grond van artikel 3 AVG ook nog te worden bezien of de blockchain valt binnen de territoriale reikwijdte van de AVG. Dat zal in ieder geval zo zijn bij inzet van blockchain door zorgpartijen in Nederland (zie paragraaf 2.4 van dit rapport).

Deel III – Wie verwerken persoonsgegevens op de blockchain?

Indien wordt vastgesteld dat de blockchain persoonsgegevens bevat, is vervolgens de vraag *wie* deze persoonsgegevens verwerken. Dit zijn in ieder geval (de nodes van) de geautoriseerde gebruikers, oftewel:

- de gebruikers die door middel van de blockchain een transactie met daarin persoonsgegevens aan (een deel van) de andere geautoriseerde gebruikers verzenden, en;
- de gebruikers die de transactie ontvangen en bevoegd zijn om de inhoud van het blok te raadplegen.

Het enkele raadplegen van de persoonsgegevens in het blok vormt al een verwerking van persoonsgegevens.

In dit rapport wordt aangenomen dat ook de niet-geautoriseerde gebruikers persoonsgegevens verwerken. Hoewel zij als niet-geautoriseerde gebruikers de inhoud van bepaalde blokken (de blokken waarvoor zij niet-geautoriseerd zijn) niet kunnen raadplegen, verwerken zij wel de hash van de inhoud van de blokken. Dit zijn, zo wordt in dit rapport zekerheidshalve tot uitgangspunt genomen, gepseudonimiseerde persoonsgegevens waarop de AVG van toepassing is (zie randnr. 3.1 van dit rapport).

> De (nodes van) geautoriseerde gebruikers van een blockchain kunnen worden onderverdeeld in geautoriseerde verwerkingsverantwoordelijken en geautoriseerde verwerkers (zie randnrs. 3.3.1 tot en met 3.3.9 van dit rapport). De geautoriseerde verwerkingsverantwoordelijke van de blockchain is een gebruiker die zelfstandig bepaalt of hij[1] persoonsgegevens op de blockchain verwerkt en voor welke doelen hij dat doet. De geautoriseerde verwerkers zijn de externe partijen die in opdracht van een of meer geautoriseerde verwerkingsverantwoordelijken deelnemen aan de blockchain en ten behoeve van hen persoonsgegevens op de blockchain verwerken.

De gezamenlijke verwerkingsverantwoordelijken van de blockchain zijn op grond van artikel 26, eerste lid, AVG verplicht tot het vaststellen van een onderlinge regeling waarin hun respectieve verplichtingen ten aanzien van de verwerking op een transparante wijze worden vastgelegd (zie randnrs. 3.3.10 tot en met 3.3.13 van dit rapport).

Bij een groot aantal gezamenlijke verwerkingsverantwoordelijken kan het volgens de Europese privacy toezichthouders (waaronder de AP) verplicht zijn om één super user aan te wijzen, die een deel van de taken van de gezamenlijke verwerkingsverantwoordelijken uitvoert (zie randnrs. 3.3.14 tot en met 3.3.18 van dit rapport).

Het vaststellen van een onderlinge regeling en het aanwijzen van een super user vereist dat gebruikers met elkaar in overleg treden en heldere afspraken maken. Dit lijkt bij een openbare, permissionless blockchain een vrijwel onmogelijke exercitie. Mede in dit licht bezien, verdient het dan ook de voorkeur om voor blockchains in de

[1] Waar in dit rapport over de mannelijke vorm wordt gesproken, is ook de vrouwelijke vorm bedoeld.

zorg waarin persoonsgegevens worden verwerkt te kiezen voor een private, permissioned blockchain, óók zodat daadwerkelijk uitvoering kan worden gegeven aan de afspraken die zijn opgenomen in de onderlinge regeling.

Een private, permissioned blockchain is verder onder meer noodzakelijk om aan de super user (voor zover deze is aangesteld) taken toe te kunnen bedelen. In het verdere vervolg van het rapport wordt er dan ook vanuit gegaan dat sprake is van een private, permissioned blockchain (zie randnr. 3.3.18 van dit rapport).

Hoewel hierover discussie mogelijk is, is het verdedigbaar om niet-geautoriseerde gebruikers ten aanzien van de gehashte persoonsgegevens in de transacties waarvoor zij niet geautoriseerd zijn aan te merken als (sub)verwerkers. De niet-geautoriseerde gebruikers bepalen namelijk slechts in beperkte mate het doel en de middelen van de verwerking van die persoonsgegevens. Dit doen zij grotendeels – zo is althans de gedachte en dat wordt in dit rapport ook tot uitgangspunt genomen – ten behoeve van de veilige en betrouwbare uitwisseling tussen geautoriseerde gebruikers (zie randnrs. 3.3.19 tot en met 3.3.28 van dit rapport).

> Ten aanzien van de niet-geautoriseerde gebruikers rijst ook de vraag wat hun grondslag is voor de verwerking van persoonsgegevens. Als (sub)verwerker kunnen zij de grondslag van de verwerkingsverantwoordelijk(en) voor wie zij (sub)verwerker zijn overnemen.

De inzet van een groot aantal verwerkers zou in strijd kunnen komen met het beginsel van dataminimalisatie. Om dit risico te verkleinen, doen gebruikers er verstandig aan om bij het ontwerp van de blockchain ontwerpkeuzes te maken die borgen dat het aantal niet-geautoriseerde gebruikers beperkt blijft tot het strikt noodzakelijke. Zo is het raadzaam om per patiënt / verzekerde een persoonlijke blockchain te hanteren. Zodoende kan worden bewerkstelligd dat de groep gebruikers van de blockchain (en het aantal niet-geautoriseerde gebruikers) beperkt blijft tot de gebruikers die in een relatie staan tot de betreffende patiënt/verzekerde (zie randnr. 3.3.28 van dit rapport).

Voor zover de niet-geautoriseerde gebruikers inderdaad optreden als (sub)verwerkers voor de geautoriseerde gebruikers, zal een verwerkersovereenkomst moeten worden gesloten (zie randnrs. 3.3.29 tot en met 3.3.31 van dit rapport).

De verwerkersovereenkomst dient in ieder geval een aantal onderdelen te bevatten zoals beschreven in de artikelen 28 en 29 van de AVG (zie randnrs. 3.3.29 tot en met 3.3.31 van dit rapport).

Het gebruik van de blockchain mag er niet toe leiden dat een instantie die wettelijk is aangewezen als verwerkingsverantwoordelijke of verwerker na ingebruikname van de blockchain een rol krijgt (geautoriseerde of niet-geautoriseerde gebruiker) die niet past bij die wettelijk vastgestelde rol (zie paragraaf 3.4 van dit rapport).

Afhankelijk van de rol die de bouwer van (delen van) de blockchain vervult, zal de bouwer kwalificeren als verwerkingsverantwoordelijke, verwerker of als niets (zie paragraaf 3.5 van dit rapport)

Deel IV – Wettelijke grondslagen voor het verwerken van persoonsgegevens

Zodra is vastgesteld dat op de blockchain persoonsgegevens worden verwerkt dient per verwerkingsverantwoordelijke gebruiker te worden vastgesteld of en zo ja, in hoeverre een wettelijke grondslag bestaat voor het verwerken van (bijzondere) persoonsgegevens in de transacties. Om dit te kunnen vaststellen, dienen de volgende stappen te worden doorlopen:

1. Vallen de persoonsgegevens onder een (medisch) beroepsgeheim en zo ja, doet zich een wettelijke grond voor op basis waarvan deze geheimhoudingsplicht zou kunnen worden doorbroken (randnrs. 4.3.2 tot en met 4.3.14 van dit rapport)?
2. Voor zover er sprake is van het verwerken van bijzondere persoonsgegevens (bijv. medische gegevens, genetische gegevens of biometrische gegevens), doet zich voor de verwerking daarvan een wettelijke doorbrekingsgrond voor (randnrs. 4.3.15 tot en met 4.3.61 van dit rapport)?
3. Voor zover er persoonsgegevens van strafrechtelijke aard worden verwerkt (bijv. in aanvulling op medische gegevens), is daar een wettelijke grondslag voor (randnrs. 4.3.62 tot en met 4.3.65 van dit rapport)?
4. Kan de verwerking van de (bijzondere) persoonsgegevens op de blockchain worden gebaseerd op een (algemene of bijzondere) wettelijke grondslag (randnrs. 4.3.66 tot en met **Fout! Verwijzingsbron niet gevonden.** van dit r apport)?
5. Worden er op de blockchain nationale identificatienummers (zoals het burgerservicenummer) verwerkt? Zo ja, is het gebruik daarvan voorgeschreven bij een formele wet of bij algemene maatregel van bestuur (randnrs. 4.3.78 tot en met 4.3.86 van dit rapport)?

De verwerkingsverantwoordelijke zal altijd alert moeten zijn op het feit dat in ieder geval een deel van de gebruikers op de blockchain niet bevoegd zal zijn tot het verwerken (waaronder begrepen: lezen) van de persoonsgegevens. Dit aan het gebruik van de blockchain inherente risico, lijkt slechts te kunnen worden opgelost in een private, permissioned blockchain, waarbij lees- en schrijfrechten kunnen worden toegekend aan specifieke gebruikers (zie paragraaf 4.3 van dit rapport).

Deel V – Materiële vereisten van de blockchain

Geautomatiseerde besluitvorming
Voor zover bij het gebruik van de blockchain en het daaraan ten grondslag liggende smart contract sprake is van geautomatiseerde besluitvorming met rechtsgevolg of die

besluitvorming (anderszins) aanmerkelijke gevolgen heeft voor de betrokkene, dient de blockchain te voldoen aan de strikte vereisten van artikel 22 AVG jo. artikel 40 UAVG. (zie par. 5.2 van dit rapport)

Internationale doorgifte
Voor zover bij het gebruik van de blockchain sprake is van internationale doorgifte, dienen de verwerkingsverantwoordelijke gebruikers van de blockchain vast te stellen of de internationale doorgifte kan worden gebaseerd op een toereikende wettelijke grondslag. Bovendien dient een buitenlandse verwerkingsverantwoordelijke gebruiker – enkele uitzonderingen daargelaten – een vertegenwoordiger in de Europese Unie aan te wijzen (zie paragraaf 5.3 van dit rapport).

Het beginsel van rechtmatigheid, behoorlijkheid en transparantie
De gegevensverwerking op de blockchain dient rechtmatig, behoorlijk en transparant plaats te vinden (artikel 5, eerste lid, aanhef en onder a, AVG). De eis van rechtmatigheid, behoorlijkheid en transparantie brengt in blockchain-verband geen onoverkomelijke privacyrechtelijke problemen met zich mee. Niettemin verdient het aanbeveling dat de gebruikers met elkaar afspreken dat zij de privacyregels in acht zullen nemen bij het gebruik van de blockchain (zie randnrs. 5.4.3 tot en met 5.4.4 van dit rapport).

Het doelbindingsbeginsel
Deze eis roept in blockchain-verband geen specifieke privacyrechtelijke vragen op. De verwerkingsverantwoordelijke gebruikers dienen voorafgaand aan het ontwerp en het gebruik van de blockchain een heldere en duidelijke omschrijving te geven van de doelstelling(en) van de verwerkingen die via de blockchain plaats zullen vinden. Slechts aan de hand van een afgebakende en concreet omschreven doelstelling, kan worden beoordeeld welke persoonsgegevens noodzakelijk zijn om binnen de blockchain te verwerken (zie randnrs. 5.4.5 tot en met 5.4.6 van dit rapport).

Het beginsel van dataminimalisatie
Op grond van artikel 5, eerste lid, aanhef en onder c, AVG moeten persoonsgegevens toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Deze eis heeft onder meer tot gevolg dat de partij die informatie op de blockchain plaatst steeds zal moeten nagaan welke andere gebruikers de informatie mogen zien en of die persoonsgegevens ook (nog langer) nodig zijn. De verwerking dient steeds beperkt te zijn tot het strikt noodzakelijke (zie randnr. 5.4.7 van dit rapport).

Het waarborgen van het beginsel van dataminimalisatie in een blockchain wordt gezien als één van de grootste privacy-uitdagingen bij het gebruik van blockchain, vanwege het uitgangspunt dat elke gebruiker van de blockchain een kopie heeft van de (gehashte) persoonsgegevens en de ‘immutability’ ervan.

Hoewel het een uitdaging kan zijn om de verwerking van persoonsgegevens in een blockchain in lijn te brengen met het beginsel van dataminimalisatie, lijkt dit niet onmogelijk. Er kunnen maatregelen worden getroffen om er (zoveel mogelijk) voor te zorgen dat de persoonsgegevens die op de blockchain worden verwerkt zijn beperkt tot het strikt noodzakelijke (zie randnrs. 5.4.11 tot en met 5.4.25 van dit rapport).

Het juistheidsbeginsel
Verwerkingsverantwoordelijke gebruikers moeten op grond van artikel 5, eerste lid, aanhef en onder d, AVG alle redelijke maatregelen nemen om persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren. De gebruiker die persoonsgegevens op de blockchain plaatst, moet ervoor zorgdragen dat deze juist en nauwkeurig zijn. Mochten gegevens toch onjuist zijn, dan dienen de gegevens te kunnen worden gerectificeerd of gewist (zie randnrs. 5.4.30 tot en met 5.4.28 van dit rapport).

Het beginsel van opslagbeperking
Het beginsel van opslagbeperking houdt in dat persoonsgegevens na het verlopen van de bewaartermijn verwijderd moeten worden. Evenals het beginsel van dataminimalisatie brengt ook dit beginsel blockchain-specifieke privacy-uitdagingen met zich mee. Eenmaal in transacties opgenomen persoonsgegevens kunnen niet meer worden verwijderd (zie randnrs. 5.4.31 tot en met 5.4.32 van dit rapport).

In dit rapport worden enkele (technische) suggesties gedaan om toch (zoveel mogelijk) uitvoering te geven aan bovengenoemde verwijderingsplicht (zie randnrs. 5.4.34 tot en met 5.4.58 van dit rapport).

Minimale beveiligingseisen
De verwerkingsverantwoordelijke gebruikers zijn verplicht om te waarborgen dat de blockchain voldoende is beveiligd (zie randnrs. 5.4.59 tot en met 5.4.77 van dit rapport). De verwerkingsverantwoordelijken kunnen daarbij verschillende organisatorische en technische maatregelen treffen (zie randnrs. 5.4.63 tot en met 5.4.77 van dit rapport).

De verantwoordingsplicht
De verwerkingsverantwoordelijke gebruikers van de blockchain moeten kunnen aantonen dat zij de hiervoor beschreven beginselen van de AVG bij het gebruik van de blockchain naleven. De verantwoordingsplicht roept geen blockchain-specifieke privacyvragen op (zie paragraaf 5.5 van dit rapport).

De beginselen van privacy by design & default
De blockchain dient te voldoen aan de beginselen van *privacy by design* en *privacy by default*. Er kan in feite alleen uitvoering worden gegeven aan privacy by design en default als de blockchain nog moet worden vormgegeven, dan wel de blockchain weliswaar reeds is ontworpen, maar nog kan worden gewijzigd. Er kunnen diverse

technische en organisatorische maatregelen worden getroffen om uitwerking te geven aan privacy by design en privacy by default (paragraaf 5.6 van dit rapport).

De meldplicht datalekken
De verwerkingsverantwoordelijke gebruikers zullen bij eventuele datalekken in specifieke gevallen verplicht zijn om deze te melden aan de Autoriteit Persoonsgegevens (AP) en de betrokkenen (zie paragraaf 5.7 van dit rapport).

Privacy Impact Assessment
Bij het gebruik van blockchain in de zorg zal een DPIA verplichting vrijwel altijd gelden, omdat sprake is van de toepassing van een nieuwe technologie en mogelijk op grote schaal (bijzondere) persoonsgegevens en andere gevoelige persoonsgegevens worden verwerkt. Na het verrichten van de DPIA, geldt bovendien dat doorlopend gemonitord moet worden of verwerkingen binnen de blockchain conform de DPIA plaatsvinden (zie paragraaf 5.8 van dit rapport).

Deel VI – Transparantie & de rechten van de betrokkene

De verwerkingsverantwoordelijke gebruikers van de blockchain zullen (aanvullende) technische en organisatorische maatregelen moeten treffen om de uitoefening van de rechten van de betrokkene mogelijk te maken.

Het recht op informatie
Op de verwerkingsverantwoordelijke gebruiker van de blockchain rust, enkele uitzonderingen daargelaten, de verplichting om de betrokkene te informeren over de verwerkingen van persoonsgegevens die binnen de blockchain plaatsvinden (artikel 13 en 14 AVG) (zie paragraaf 6.2 van dit rapport).

Bovengenoemde informatieverplichting leidt in beginsel niet tot blockchain-specifieke privacyrechtelijke issues. Het verdient aanbeveling om maatregelen te treffen die borgen dat de privacyverklaring tijdig - en bij voorkeur geautomatiseerd - aan de betrokkene wordt verstrekt.

Het recht op inzage
De verwerkingsverantwoordelijke gebruikers van de blockchain zullen maatregelen moeten treffen om de uitoefening van het recht op inzage van de betrokkene mogelijk te maken. Het gebruik van een blockchain voor verwerking van persoonsgegevens in de zorg brengt geen blockchain-specifieke issues met zich mee voor het kunnen voldoen aan inzageverzoeken van de betrokkene (zie paragraaf 6.3 van dit rapport).

Het recht op rectificatie
Voor zover de betrokkene aantoont dat de persoonsgegevens die over hem (op de blockchain) worden verwerkt onjuist zijn, heeft de betrokkene op grond van artikel 16 AVG recht op rectificatie. Een rectificatieverzoek kan leiden tot diverse blockchain-specifieke issues (zie randnrs. 6.4.5 tot en met 6.4.10 van dit rapport).

Het recht op wissing
Op grond van artikel 17, eerste lid, AVG heeft de betrokkene onder omstandigheden recht op wissing van hem betreffende persoonsgegevens op de blockchain (zie randnrs. 6.4.9 tot en met 6.4.15 van dit rapport). Het wissen van persoonsgegevens in een blockchain vormt één van de grootste (technische) uitdagingen van het gebruik van blockchain.

Het recht op beperking van de verwerking
Verder heeft de betrokkene op grond van artikel 18, eerste lid, AVG onder omstandigheden het recht op beperking van de verwerking van zijn persoonsgegevens (op de blockchain) (zie randnrs. 6.4.13 tot en met 6.4.21 van dit rapport). Ook met het bestaan van dit recht moet bij de bouw van de blockchain rekening worden gehouden.

Het recht op dataportabiliteit
Verwerkingsverantwoordelijke gebruikers van een blockchain zullen voorts maatregelen moeten nemen zodat betrokkenen hun eventuele recht op overdraagbaarheid (ook wel het recht op dataportabliteit) uit kunnen oefenen ten aanzien van hun persoonsgegevens op de blockchain (zie paragraaf 6.5 van dit rapport).

Het recht op bezwaar
Als de persoonsgegevens op de blockchain worden verwerkt op grond van artikel 6, eerste lid, aanhef onder e en f AVG, kan de betrokkene daartegen op grond van artikel 21, eerste lid, AVG bij de verwerkingsverantwoordelijke gebruiker te allen tijde bezwaar maken vanwege met zijn specifieke situatie verband houdende redenen (zie paragraaf 6.6 van dit rapport). Bij een gehonoreerd bezwaar moet de verwerking worden gestaakt.

Uitzonderingen op de rechten van de betrokkene
Als hoofdregel geldt dat de rechten van betrokkenen (waaronder het recht om geïnformeerd te worden) en de plicht van de verwerkingsverantwoordelijke om een datalek te melden aan de betrokkene, van toepassing is in alle situaties. Op grond van artikel 23 AVG kunnen uitzonderingen worden gemaakt op de rechten van betrokkenen en de meldplicht aan de betrokkene. Deze uitzonderingen zijn uitgewerkt in artikel 41, eerste lid, Uitvoeringswet AVG (zie paragraaf 6.7 van dit rapport).

1 WAT IS BLOCKCHAIN?

1.1 Inleiding

1.1.1 Blockchain is een distributed ledger technology. Het is in de basis een register waarin de geschiedenis van alle door het netwerk vertrouwde transacties met daarin bijvoorbeeld gegevens of betalingen worden bijgehouden. Eén of meer transacties worden in een blok gezet; dit blok wordt aan de blockchain toegevoegd. Ieder blok wordt voorzien van een unieke code (header). In deze header wordt verwezen naar de header van het vorige blok. Als gevolg daarvan worden alle blokken aan elkaar gekoppeld en ontstaat een chain; de blockchain.

1.1.2 Men vergelijkt blockchain-technologie vaak met een grootboek. Iedere gekoppelde computer, 'node', bevat een identiek exemplaar van het grootboek. Het grootboek wordt, met andere woorden, tussen de nodes gedistribueerd.
De kracht van blockchain-technologie is dat als via een van de nodes al toegevoegde informatie gewijzigd wordt, de andere exemplaren van het grootboek deze wijzigingen zullen herkennen en een foutmelding zullen geven. Dit zorgt ervoor dat als er maar genoeg nodes deel uitmaken van een blockchain-netwerk, het vrijwel onmogelijk is om informatie in een blockchain (eenzijdig) te wijzigen. Dit zorgt voor onveranderlijkheid ('immutability')[2], integriteit (geen aanpassingen achteraf) en onweerlegbaarheid (niemand kan claimen dat een transactie niet heeft plaatsgevonden).

Figuur 1. Een visuele weergaven van een centraal, een decentraal en een gedistribueerd systeem, zoals blockchain. Ieder puntje vertegenwoordigt een afzonderlijke node. (bron: Paul Baran – On distributed communications (1964))

Openbare versus besloten blockchains

1.1.3 Er zijn verschillende typen blockchains. Enerzijds zijn er openbare blockchains zoals Bitcoin. Anderzijds zijn er besloten blockchains.[3]

[2] Dit dient genuanceerd te worden tot: "kan niet eenzijdig teruggedraaid worden". Als er algemeen consensus is tussen alle nodes dat iets teruggedraaid dient te worden, dan kan dat wel degelijk. Niet zozeer door het oude, onjuiste blok, te verwijderen of te overschrijven, maar door met elkaar een nieuwe (juiste) waarheid in een nieuw blok vast te leggen.
[3] Sommige 'puristen' beschouwen enkel openbare blockchains als 'echte' blockchains.

1.1.4 Een openbare blockchain is een blockchain waarbij het iedereen volledig vrij staat om eraan deel te nemen. Eenieder kan de software van een node uitvoeren en deze met het blockchainnetwerk verbinden via het internet.

1.1.5 Op openbare blockchains vindt geen identificatie en authenticatie van deelnemers plaats. Deelnemers zijn in die zin dus nagenoeg anoniem, al is pseudoniem meer correct. Om transacties te kunnen uitvoeren wordt gewerkt met zogenoemde cryptografische sleutelparen: een openbare (hash van een) public key en een geheime private key om transacties mee te ondertekenen. Alle transacties en alle informatie in de betreffende blockchain zijn openbaar. Iedereen kan ook voorstellen doen voor software updates, maar een upgrade van het netwerk gebeurt alleen als (de meerderheid van) de deelnemers vrijwillig de software op hun eigen nodes updaten. In een openbare blockchain is er al met al geen enkele partij 'de baas'; er zijn dus ook geen super-users of dergelijke constructies.

1.1.6 Aan een besloten blockchain kan niet iedereen zonder meer deelnemen. Er is een toegangsaanvraag en goedkeuring vereist. Bovendien kunnen de toebedeelde lees- en schrijfrechten per gebruiker en zelfs per transactie verschillen.
Nieuwe blockchainplatform-ontwerpen hebben als doel om de voordelen van openbare en besloten blockchains te verenigen. Zo kan een tweelaags ontwerp bijvoorbeeld bestaan uit twee interoperabele blockchains:

1. Een besloten blockchain met een klein aantal nodes van bekende vooraf geselecteerde gebruikers, dat zorg draagt voor de daadwerkelijke real time gegevensverwerking tussen die (daartoe gerechtigde) gebruikers.
2. Een openbare blockchain met een veelheid aan nodes, waarop (bewerkte (bijvoorbeeld geanonimiseerde)) gegevens voor langere tijd opgeslagen kunnen worden en die kan dienen als schakel naar andere netwerken zonder dat de gegevens van de besloten blockchain gecompromitteerd worden.

Smart contracts

1.1.7 Een smart contract is een programmeercode waarin een handeling afhankelijk is gemaakt van het voltrekken van één of meer gebeurtenissen. Een smart contract bestaat in de kern altijd uit een als/dan-constructie. Het is een deterministisch computerprogramma: gegeven een bepaalde input en bepaalde beginwaarden – geregistreerd op de blockchain – zal het altijd dezelfde output genereren. De werking is anders gezegd volledig voorspelbaar. Een smart contract is dus eigenlijk niet 'slim'; het voert uit wat het is opgedragen, enig 'nadenken' of pro-activiteit komt er niet bij kijken. Alle regels zijn voorgeprogrammeerd. Anders dan de term doet vermoeden wordt met een smart contract bovendien niet noodzakelijk een contract of een andere

rechtshandeling gecreëerd of uitgevoerd. Hoe een smart contract juridisch wordt geduid hangt helemaal af van de specifieke toepassing[4].

1.1.8 Smart contracts kunnen aldus processen automatiseren met behulp van blockchain. Smart contracts kunnen bijvoorbeeld ook zonder menselijke tussenkomst zorgen voor 'communicatie' tussen machines (machine-2-machine).

Oracles

1.1.9 Om te kunnen vaststellen of aan de voorwaarden voor de uitvoering van een smart contract is voldaan, zal veelal input van buiten de blockchain nodig zijn. Bijvoorbeeld de bevestiging dat een bepaalde handeling is uitgevoerd of dat een besluit is genomen ("als de cliënt heeft bevestigd dat de zorg is geleverd, dan wordt de betaling in werking gezet"). Een blockchain is "doof en blind": de blockchainsoftware kan niet zelfstandig informatie van buiten ophalen. Hier komen zogenoemde orakels of in het Engels 'oracles' in beeld. Oracles kunnen input leveren aan een smart contract; ze kunnen (feitelijke) informatie, oordelen en beslissingen die van belang zijn voor de executie van een smart contract – maar die daar zelf geen onderdeel van uit maken – op de blockchain brengen. Achter een oracle kan bijvoorbeeld een externe informatiebron schuilgaan, zoals een database of register van een vertrouwd instituut of een hardware oracle zoals een IoT-apparaat of sensor (machine-2-machine). Maar het kan ook gaan om een partij of een persoon, zoals een beslissingsbevoegde of verslagleggende notaris of ambtenaar. De partijen die gebruik maken van het smart contract accepteren op voorhand de informatie of het oordeel van het oracle en de betekenis daarvan voor de uitvoering van het smart contract.

Blockchain eenvoudig uitgelegd

Stel, er bestaat een grote kluis, zoals die vroeger bij banken in de kelder aanwezig was. Die kluis is nu niet fysiek, maar digitaal. Om in de kluis te kunnen kijken, moet men beschikken over een sleutel, in dit geval een digitale sleutel. Er zijn in dat kader twee mogelijkheden. De eerste mogelijkheid is dat iedereen die een sleutel wil krijgen, een sleutel krijgt. Het enige wat iemand daarvoor moet doen, is zich als gebruiker van het systeem registreren. We noemen zo'n systeem een openbare blockchain. De tweede mogelijkheid is dat alleen geselecteerde gebruikers een sleutel krijgen. We spreken dan over een besloten blockchain.

De sleutel geeft gebruikers toegang tot de kluis. Als zij de kluis openen, ziet iedere sleutelhouder een afschrift van hetzelfde notitieboekje. In dat notitieboekje kan per regel informatie worden genoteerd. Die informatie kan versleuteld zijn en dan alleen worden ontsleuteld door gebruikers die daartoe op grond van hun sleutel zijn

[4] Zie Smart contracts als specifieke toepassing van de blockchaintechnologie, Smart Contract Werkgroep – Dutch blockchain Coalition, voor een uiteenzetting van verschillende juridische verschijningsvormen van smart contracts en een algemene juridische verdieping.

geautoriseerd. Doen zij dat, dan zien zij per regel leesbare informatie. Die informatie kan bestaan uit de registratie van een transactie tussen sleutelhoudende gebruikers (zoals bij Bitcoin), of uit gegevens die voor de sleutelhoudende gebruikers relevant zijn. Naast de informatie die tussen gebruikers wordt gedeeld, bevat de regel in het notitieboekje ook andere informatie, waaronder een verwijzing naar de voorgaande regel met informatie (een header). Op deze wijze worden de regels met informatie onlosmakelijk met elkaar verbonden en ontstaat er een ketting van informatieblokken. Er wordt alleen informatie aan het notitieboekje toegevoegd, als dat gebeurt volgende regels die vooraf zijn vastgesteld c.q. geprogrammeerd, danwel als gebruikers daarover overeenstemming bereiken.

Het notitieboekje wordt vervolgens naar iedere computer in het netwerk gedistribueerd. Zo heeft iedere sleutelhoudende partij een afschrift van het notitieboekje op zijn computer staan. Die computer noemen we een node. Aanpassing van het notitieboekje gebeurt synchroon. Het ongemerkt aanpassen van het notitieboekje op één van de nodes is daarom niet mogelijk, omdat de computers een afwijking tussen de verschillende notitieboekjes zullen vaststellen.

De kracht van het voorgaande is dat iedere sleutelhoudende partij op hetzelfde moment naar dezelfde informatie kijkt. Of die informatie juist is, staat ter beoordeling van de sleutelhoudende gebruikers. Zij kunnen dat zelf vaststellen, of ter verificatie van de informatie in het notitieboekje een externe bron gebruiken. We noemen dat een oracle.

Applicatielaag

1.1.10 Het gebruik van blockchain-technologie wordt veelal ondersteund door een gebruikersvriendelijke applicatie, zoals een website, database of app. Een dergelijke applicatielaag vergemakkelijkt het gebruik. Zo kan een gebruiker bijvoorbeeld in een app zien waar hij gegevens kan invoeren, die vervolgens zichtbaar worden in de app voor anderen die leesrechten hebben (vergelijkbaar met de Mijn Zorg Log-toepassing van Zorginstituut Nederland, zie ook hieronder). Op de applicatielaag kunnen ook andere bronnen van informatie worden aangesloten en voor de gebruikers zichtbaar worden gemaakt. De blockchain zelf kan ook verwijzingen naar informatie op externe bronnen bevatten. In dat geval wordt die informatie niet in de transactie zelf opgenomen (‘on chain’), maar wordt naar die informatie verwezen (‘off chain’) en kan die informatie worden opgehaald met behulp van een link (pointer) die op de blockchain wordt geplaatst.

Toepassingen van blockchain

1.1.11 Er zijn verschillende toepassingen van blockchain-techniek denkbaar. Toegespitst op de zorgsector kan deze bijvoorbeeld worden ingezet om:

- uitwisseling van gegevens mogelijk te maken (bijvoorbeeld tussen zorgaanbieder en zorgverzekeraar);
- de patiënt inzage in zijn gegevens te geven;
- verzending en betaling van declaraties te verwezenlijken, en;
- bewijs vast te leggen van bijvoorbeeld medische verrichtingen die hebben plaatsgevonden (doordat de patiënt via blockchain heeft bevestigd dat die verrichtingen hebben plaatsgevonden).

1.1.12 Let op: voor zover de blockchain kan worden aangemerkt als een elektronisch uitwisselingssysteem in de zin van artikel 1 aanhef en onder j van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg[5] (Wabvpz) moet rekening worden gehouden met de specifieke regels die daarvoor gelden. Zo bepaalt artikel 15a Wabvpz dat de zorgaanbieder slechts gegevens van de cliënt beschikbaar mag stellen via een elektronisch uitwisselingssysteem, voor zover de zorgaanbieder heeft vastgesteld dat de cliënt daartoe uitdrukkelijk toestemming heeft gegeven. Verder bepaalt artikel 15f Wabvpz dat een zorgverzekeraar geen toegang mag hebben tot elektronische uitwisselingssystemen. Ook kan bijv. gewezen worden op het op artikel 15j Wabvpz gebaseerde Besluit elektronische gegevensverwerking door zorgaanbieders, waarin regels zijn gesteld over de functionele, technische en organisatorische maatregelen voor het beheer, de beveiliging en het gebruik van een elektronisch uitwisselingssysteem of een zorginformatiesysteem.[6] Wij besteden hierna geen aandacht meer aan de regels voor elektronische uitwisselingssystemen en zorginformatiesystemen. Voor zover daarvan met een blockchain in de zorg sprake zou zijn moet met die regels, ook bij de bouw, wel rekening worden gehouden.

[5] Een elektronisch uitwisselingssysteem is blijkens artikel 1 aanhef en onder j Wabvpz: een systeem waarmee zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar kunnen maken, waaronder niet begrepen een systeem binnen een zorgaanbieder, voor het bijhouden van een elektronisch dossier.
[6] Een zorginformatiesysteem is blijkens artikel 1 aanhef en onder m Wabvpz een elektronisch systeem van een zorgaanbieder voor het verwerken van persoonsgegevens in een dossier, niet zijnde een elektronisch uitwisselingssysteem.

2 TOEPASSELIJKHEID VAN DE AVG[7] OP DE BLOCKCHAIN

2.1 Inleiding

2.1.1 Een toets of een blockchain voldoet aan de regels van de AVG, is pas aan de orde als de AVG van toepassing is. Of dat zo is, zal dus eerst moeten worden beoordeeld. Dit aan de hand van de vraag of aan de materiële en territoriale toepassingseisen van de AVG is voldaan.

2.2 Materieel toepassingsgebied

2.2.1 Om te beoordelen of de blockchain valt binnen het materieel toepassingsgebied van de AVG moet eerst worden vastgesteld of persoonsgegevens[8] worden verwerkt[9].

Wanneer is sprake van persoonsgegevens?

2.2.2 Een persoonsgegeven is elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Als een identificeerbaar persoon wordt beschouwd iedere informatie die direct (bijv. naam van de patiënt, adres, telefoonnummer), dan wel indirect (patiëntvolgnummer, BSN) herleidbaar is tot een natuurlijke persoon.[10] Van een persoonsgegeven is aldus snel sprake.

> Voor de vraag of sprake is van identificeerbaarheid moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is, dan wel door derden in te zetten zijn, om de persoon te identificeren. Daarbij moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen (denk aan de toenemende rekenkracht van computers en het groeiende aantal beschikbare hulpmiddelen).[11]

2.2.3 Let op: de AVG is niet van toepassing op de persoonsgegevens van overleden personen, tenzij die persoonsgegevens ook iets zeggen over andere natuurlijke personen die nog wél in leven zijn. In dat geval is het gegeven immers een zelfstandig

---

[7] Zie voor de tekst: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex%3A32016R0679.
[8] Zie artikel 2 AVG. Ook moet worden beoordeeld of sprake is van een (gedeeltelijk) geautomatiseerde verwerking of verwerking in een bestand. Dat eerste is bij een blockchain altijd het geval, alleen al omdat persoonsgegevens digitaal worden opgeslagen op de nodes van de gebruikers. Aan dit criterium voor toepasselijkheid van de AVG wordt om die reden geen verdere aandacht meer besteed.
[9] Zoals hierna zal worden toegelicht, is het verwerken van persoonsgegevens een zeer ruim begrip. Het enkele raadplegen van persoonsgegevens kan al worden aangemerkt als verwerken.
[10] Artikel 4, aanhef en onder 1, AVG: "persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
[11] Overweging 26 van de AVG.

persoonsgegeven over de andere natuurlijke persoon.[12] De omstandigheid dat de persoonsgegevens van overleden personen niet vallen onder de bescherming van de AVG, sluit overigens niet uit dat de verwerking van dergelijke gegevens via andere wettelijke regelingen wordt gereguleerd. Een voorbeeld daarvan is het medisch beroepsgeheim van een arts (artikel 7:457 BW). Het medische beroepsgeheim blijft van toepassing op de (medische) informatie patiënt, ook nadat de patiënt is overleden. Het is een arts – enkele uitzonderingen daargelaten – daardoor niet toegestaan om de gegevens van de overleden patiënt met derden te delen.[13] Voor zover op de blockchain gebruik wordt gemaakt van gegevens van overleden personen, zal dus altijd aanvullend moeten worden nagegaan of andere wettelijke regels de verwerking van die gegevens aan banden legt.

Zijstap: bijzondere persoonsgegevens

2.2.4 De AVG maakt onderscheid tussen persoonsgegevens en bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn persoonsgegevens die naar hun aard gevoelig zijn. De categorieën bijzondere persoonsgegevens zijn limitatief opgesomd in artikel 9, eerste lid, AVG. Voorbeelden van bijzondere persoonsgegevens zijn gegevens over iemands ras, gezondheid en religie en gegevens met betrekking tot iemands seksueel gedrag. Ook genetische gegevens (bijv. DNA) worden onder de AVG aangemerkt als bijzondere persoonsgegevens.[14] Het begrip bijzondere persoonsgegevens dient ruim te worden uitgelegd. Zowel indirecte als directe gegevens kunnen onder de definitie van bijzondere persoonsgegevens vallen.[15]

2.2.5 In de zorg worden op grote schaal bijzondere persoonsgegevens verwerkt. Dit zijn veelal persoonsgegevens betreffende iemands gezondheid. Het begrip 'gezondheid' moet ruim worden uitgelegd. Het omvat niet enkel de gegevens die in het kader van een medisch onderzoek of een medische behandeling door een arts of zorgverlener worden verwerkt, maar alle gegevens die iets over de (geestelijke of lichamelijke) gezondheid van een persoon zeggen. Elke conclusie over iemands gezondheid is een gezondheidsgegeven, ongeacht de betrouwbaarheid daarvan. Voor de kwalificatie van een gezondheidsgegeven is bovendien niet relevant of het gegeven informatie prijs geeft over de *aard* van de aandoening.[16] Het enkele gegeven dat iemand ziek is, pijn heeft[17] of een afspraak heeft bij een medisch specialist is een gezondheidsgegeven.

---

[12] Overweging 27 van de AVG.
[13] Zie voor een nadere bespreking van (het doorbreken van) het medisch beroepsgeheim deel IV, randnrs. 4.3.2 van dit rapport.
[14] Vgl. artikel 4, aanhef en onder 13, AVG jo. artikel 9, eerste lid, AVG.
[15] Een voorbeeld van een direct gevoelig persoonsgegevens is bijvoorbeeld de aard van een medische aandoening van een persoon (direct gezondheidsgegeven). Een voorbeeld van een indirect persoonsgeven is iemands patiëntnummer. Op zichzelf is het patiëntnummer niet te herleiden tot de natuurlijke persoon, maar zodra het patiëntnummer wordt gekoppeld aan de andere gegevens van die persoon zal het patiëntnummer iets (kunnen) zeggen over (de medische gesteldheid van) de patiënt.
[16] Het onderscheid tussen medische gegevens over de aard van de aandoening en gegevens die daar geen inzicht in geven, wordt in de praktijk dikwijls aangeduid als 'wat'-informatie respectievelijk 'dat'-informatie. Beiden betreffen een gezondheidsgegeven waarop het strikte het regime van artikel 9 AVG van toepassing is (zie hierover de volgende alinea). Enig verschil is dat de privacyinbreuk in het geval van het verwerken van 'dat'-informatie naar verhouding minder groot zal zijn dan de privacyinbreuk die gepaard gaat met het verwerken van 'wat'-informatie, hetgeen van belang kan zijn bij de beoordeling van proportionaliteit en subsidiariteit van de verwerking (zie randnrs. 5.4.7 e.v. van dit rapport).
[17] Ook het Europese Hof van Justitie hanteert een ruime benadering van de definitie van gezondheidsgegevens. Zo overweegt het Hof in het Lindqvist-arrest dat gezondheidsgegevens "alle – zowel fysieke als psychische – aspecten van iemands gezondheid" omvat. In dit arrest oordeelde het Hof dat het enkele feit dat iemand zijn

2.2.6 Het vaststellen of sprake is van het verwerken van bijzondere persoonsgegevens in blockchain-verband is van belang, omdat op het verwerken van bijzondere persoonsgegevens een strikt (privacy)regime van toepassing is. De verwerking van bijzondere persoonsgegevens is verboden, tenzij hiervoor een algemene of specifieke doorbrekingsgrond bestaat in de AVG of een bijzondere wet.[18] Hieruit volgt dat slechts bijzondere persoonsgegevens in een blockchain mogen worden verwerkt[19] indien daarvoor een doorbrekingsgrond voorhanden is. Dit heeft directe gevolgen voor het ontwerp en het gebruik van een blockchain.

Anonieme gegevens en gepseudonimiseerde persoonsgegevens

2.2.7 De AVG is niet van toepassing op gegevens die zodanig anoniem zijn (gemaakt) dat de persoon waarop ze betrekking hebben niet (meer) identificeerbaar is. In dat geval is er, met andere woorden, geen sprake van persoonsgegevens meer. Er bestaat veel discussie over de vraag wanneer sprake is van anonieme gegevens, zeker ook in het kader van blockchain. Reden daarvoor is dat in een blockchain veel gebruik wordt gemaakt van versleuteling[20] en hashing[21] om (persoons)gegevens onleesbaar te maken. Onderwerp van discussie is of deze versleuteling- en hashingtechnieken anonieme gegevens opleveren, wat zou maken dat de AVG niet (meer) van toepassing is.

2.2.8 De gezaghebbende Artikel 29-Werkgroep (inmiddels: de European Data Protection Board) – waarin de Europese privacy toezichthouders zijn verenigd – hanteert als uitgangspunt dat pas gesproken kan worden van 'anonieme gegevens' indien iedere mogelijkheid tot identificatie van de betrokkene onherroepelijk is uitgesloten.[22] Een veel voorkomende gedachte is dat versleuting en/of hashing van persoonsgegevens leidt tot anonieme persoonsgegevens. De Europese privacy toezichthouders zijn echter van oordeel dat de versleuteling en/of hashing van persoonsgegevens (veelal) moet worden gezien als een manier om persoonsgegevens te pseudonimiseren, en dus als een beveiligingsmaatregel.[23] Gepseudonimiseerde persoonsgegevens vallen daarmee onverkort onder de reikwijdte van de AVG.

---

voet bezeerd heeft een bijzonder (gezondheids)gegeven is. Zie HvJ EU 6 november 2003, C 101/01 (Bodil Lindqvist t. Zweden).

[18] De algemene doorbrekingsgronden staan beschreven in artikel 9, tweede lid, AVG en artikelen 22 tot en met 30 UAVG. Bijzondere wetten kunnen in aanvulling daarop specifieke doorbrekingsgronden bevatten. Deze specifieke doorbrekingsgronden kunnen volgen uit de toepasselijke sectorale wetgeving, zoals bijvoorbeeld de ZVW, de Wmo, de Wlz en de Jw. In deel III van dit rapport wordt nader ingegaan op de afzonderlijke doorbrekingsgronden die in de zorg relevant kunnen zijn.

[19] Wij benadrukken dat het niet enkel gaat om het plaatsen van bijzondere persoonsgegevens op de blockchain, maar bijv. ook het raadplegen, verwijderen, rectificeren en/of anonimiseren van die persoonsgegevens. Verwerken is een ruim begrip. Zie randnr. 2.2.14 van dit rapport.

[20] Versleuteling houdt in dat de persoonsgegevens door middel van encryptie met een geheime sleutel worden beveiligd. Zie de hierna genoemde voorbeelden achter randnummer 2.2.11 van dit rapport.

[21] Hashing houdt in dat persoonsgegevens van een willekeurige omvang door middel van een hashfunctie worden omgevormd naar reeks van een vaste grootte. De persoonsgegevens zijn dus niet meer zichtbaar, tenzij de gehashte gegevens bijv. door middel van brutekrachtaanvallen zouden worden herberekend.

[22] In deze groep waren (tot en met 25 mei 2018) de Europese privacy toezichthouders verenigd. De groep bracht onder meer adviezen uit over de interpretatie van begrippen in de privacyrichtlijn en de Wbp. De opinies van deze groep waren en zijn nog steeds zeer gezaghebbend. Sinds 25 mei 2018 heeft de European Data Protection Board ('EDPB') de taken van de Artikel 29-Werkgroep overgenomen. De eerdere adviezen van de Artikel 29-Werkgroep zijn door de EDPB bekrachtigd.

[23] Zie Artikel 29-Werkgroep, Advies 5/2014 over anonimiseringstechnieken, WP 216, p. 1. Zie ook artikel 32, eerste lid, aanhef en onder a AVG.

2.2.9 Reden daarvoor is volgens de Artikel 29-Werkgroep dat – anders dan bij anonimisering, waarbij *elke* mogelijkheid tot identificatie onomkeerbaar wordt uitgesloten – bij pseudonimisering de kans op identificatie blijft bestaan. De inzet van pseudonimisering heeft enkel tot gevolg dat de koppelbaarheid van een dataset aan de oorspronkelijke dataset wordt *beperkt*. Degene die versleuteling en/of hashing heeft toegepast, houdt echter de beschikking over de encryptiesleutel en/of de oorspronkelijke gegevens.[24] In de optiek van de Europese privacy toezichthouders blijft het daardoor voor de sleutelhouder mogelijk om de versleuteling/hashing van de persoonsgegevens terug te draaien. Zolang de oorspronkelijke gegevens en de encryptiesleutel worden bewaard, blijft bovendien het risico bestaan dat (onbevoegde) derden de gegevens kunnen de-pseudonimiseren, bijvoorbeeld doordat zij de encryptiesleutel in handen krijgen (al dan niet door hacks, brutekrachtaanvallen of datalekken). Ook dit vormt een zelfstandig risico op herleidbaarheid tot de betrokkenen.

2.2.10 Het maakt volgens de Artikel 29-Werkgroep overigens geen verschil of de encryptiesleutel en/of de oorspronkelijke gegevens worden bewaard door een vertrouwde derde partij (een zogenoemde Trusted Third Party ('TTP')). In die situatie wordt de herleidbaarheid tot het identificeren van de betrokkenen volgens de Artikel 29-Werkgroep eveneens onvoldoende uitgesloten.

2.2.11 Het standpunt van de (Europese) privacy toezichthouders lijkt zich uit te strekken tot in ieder geval een groot aantal, maar mogelijk ook wel alle hashing- en versleutelingstechnieken. De Artikel 29-Werkgroep heeft in 2014 een opinie over anonimiseringstechnieken gepubliceerd (opinie 5/2014). Daarin worden verschillende technieken beschreven:

- *Encryptie met een geheime sleutel*: in dit geval worden de persoonsgegevens cryptografisch versleuteld. De versleutelde persoonsgegevens kunnen door het gebruik van de sleutel weer ontsleuteld worden.

- *Hashfunctie*: door middel van deze functie worden gegevens van een willekeurige omvang gehasht naar een uitvoer met vaste grootte[25], wat op zichzelf niet kan worden teruggedraaid, tenzij voor gebruikers duidelijk zou zijn wat de invoer is geweest.
  De hashfunctie kan worden versterkt met een salt. In dat geval wordt aan de te hashen gegevens een willekeurige reeks met leestekens toegevoegd ('salt'). Daardoor wordt het risico verkleind dat de hash kan worden gekraakt en de invoerwaarden (de oorspronkelijke, gehashte, gegevens) dus kunnen worden herleid.

[24] Tussen partijen op de blockchain zal een governance moeten worden vormgegeven die ook ziet op het sleutelbeheer en de wijze waarop encryptie/hashing op de blockchain plaatsvindt.
[25] Hiermee wordt bedoeld dat iedere hash even lang is, onafhankelijk van de lengte van de tekst die wordt gehasht.

- *Keyed-hashfunctie met opgeslagen sleutel*: de gegevens worden gehasht, maar daarnaast wordt een geheime sleutel als aanvullende invoer gebruikt. Dit onderscheidt zich van de salted-hashfunctie doordat de sleutel (anders dan de salt) geheim is. Hierdoor is het moelijker om de hash met brutekrachtaanvallen terug te berekenen.

- *Deterministische encryptie of keyed-hashfunctie met verwijdering van de sleutel*: deze techniek komt erop neer voor elk attribuut (cel) in de database een willekeurig (aselect) getal te kiezen als pseudoniem en vervolgens de correspondentietabel te verwijderen. Deze oplossing vermindert de koppelbaarheid tussen de persoonsgegevens in de dataset en de gegevens betreffende diezelfde persoon in een andere dataset waar een ander pseudoniem wordt gebruikt.

- *Tokenisering*: Deze techniek komt erop neer mechanismen voor eenrichtingsencryptie toe te passen of via een indexfunctie een volgnummer of willekeurig (aselect) getal toe te wijzen dat rekenkundig niet af te leiden valt uit de oorspronkelijke gegevens.[26]

2.2.12 De Artikel 29-Werkgroep concludeert ten aanzien van bovengenoemde technieken dat het in veel gevallen vrijwel onmogelijk zal zijn om tot volledige anonimiteit te komen:

> "Geen van de in dit advies uiteengezette technieken beantwoordt met zekerheid aan de drie criteria voor een doeltreffende anonimisering, namelijk dat het niet mogelijk mag zijn een persoon te individualiseren (herleidbaarheid), persoonsgebonden records met elkaar in verband te brengen (koppelbaarheid) en persoonsgegevens af te leiden (deduceerbaarheid). Niettemin kan deze of gene techniek sommige van die risico's geheel of ten dele ondervangen. Het is derhalve zaak om zorgvuldig af te wegen hoe een op zichzelf staande techniek kan worden toegepast in de specifieke situatie die aan de orde is. Voorts moet worden bekeken of een combinatie van die technieken ertoe kan bijdragen het resultaat beter bestand te maken tegen privacyschendingen."[27]

2.2.13 Hoewel de Europese privacy toezichthouders niet snel zullen aannemen dat persoonsgegevens door middel van versleuteling of hashing geanonimiseerd kunnen worden, sluiten zij deze mogelijkheid niet geheel uit.[28] Een dataset kan mogelijk als anoniem worden beschouwd wanneer extra stappen worden ondernomen in aanvulling op de pseudonimisering, bijvoorbeeld door het wegnemen van gegevens (attributen) en generaliseren, de oorspronkelijke gegevens te verwijderen of op zijn minst samen

[26] Zie Artikel 29-Werkgroep, Advies 5/2014 over anonimiseringstechnieken, WP 216, p. 23-24.
[27] Zie Artikel 29-Werkgroep, Advies 5/2014 over anonimiseringstechnieken, WP 216, p. 24
[28] Zie bijvoorbeeld https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens ten aanzien van hasing: "Gehashte persoonsgegevens zijn meestal niet anoniem." (onderstreping toegevoegd).

te voegen tot een hoog aggregatieniveau.[29] Duidelijkheid over wanneer aan deze (aanvullende) voorwaarden is voldaan, is door de Europese privacy toezichthouders vooralsnog niet gegeven. Zolang deze onduidelijkheid blijft bestaan, verdient het aanbeveling om er – en dat wordt in dit rapport ook gedaan – van uit te gaan dat het hashen of versleutelen van persoonsgegevens in een blockchain slechts leidt tot pseudonimisering, ook al is daar in bepaalde gevallen discussie over mogelijk.[30] Dat betekent ook dat in dit rapport zekerheidshalve wordt aangenomen dat voor zover er aldus persoonsgegevens worden verwerkt op de blockchain, de AVG op die persoonsgegevens van toepassing is, óók na de inzet van hashing- of versleutelingstechnieken.

Wanneer is sprake van een verwerking?

2.2.14 Als gezegd, is bij de vraag naar de materiële toepasselijkheid van de AVG ook van belang of persoonsgegevens worden *verwerkt*. Een verwerking is iedere bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens. Dit betreft een zeer ruim begrip. Als voorbeelden noemt artikel 4, tweede lid, AVG onder meer het verzamelen, opslaan, bijwerken en doorzenden van persoonsgegevens.[31]

2.2.15 Uit het voorgaande volgt dat blockchains met daarin persoonsgegevens, behoudens enkele hierna te bespreken uitzonderingen, zonder meer vallen onder de materiële reikwijdte van de AVG.

2.3 De verwerking van persoonsgegevens op de blockchain

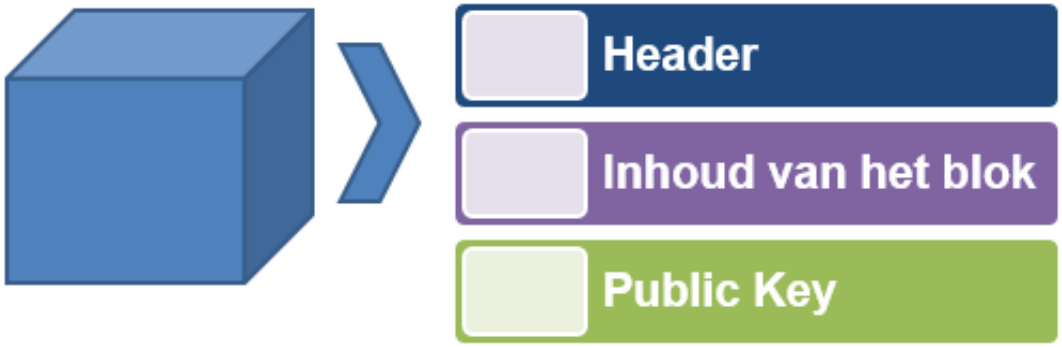
2.3.1 Na deze bespreking van het onderscheid tussen (bijzondere) persoonsgegevens, gepseudonimiseerde persoonsgegevens en anonieme gegevens, zullen wij in deze paragraaf belichten op welke wijze er persoonsgegevens in een blockchain (kunnen) worden verwerkt. Daarbij stellen wij voorop dat de vraag of en zo ja, in hoeverre persoonsgegevens in een blockchain worden verwerkt slechts door middel van een concrete beoordeling van de inhoud en opzet van de blockchain kan worden beantwoord. Het hiernavolgende overzicht is bedoeld als een algemene checklist om vast te stellen of binnen de blockchain persoonsgegevens worden verwerkt en of dus aan de materiële toepassingscriteria van de AVG wordt voldaan.

---

[29] Zie Artikel 29-Werkgroep, Advies 5/2014 over anonimiseringstechnieken, WP 216, p. 24-25 en p. 34.
[30] Er is discussie mogelijk, aangezien (lagere) rechtspraak bestaat die enige steun biedt voor de opvatting dat het onomkeerbaar dubbel pseudonimiseren van persoonsgegevens ertoe kan leiden dat niet meer gesproken kan worden van persoonsgegevens (Rb. Midden Nederland 2 augustus 2017, CLI:NL:RBMNE:2017:4011, rov. 4.10-4.11). Aan deze rechtspraak lijkt echter geen doorslaggevende betekenis te kunnen worden toegekend, aangezien in deze rechtspraak met enige nadruk wordt benadrukt dat voor de vaststelling of er inderdaad wél of géén sprake is van persoonsgegevens 'een gedetailleerde beoordeling' nodig is 'van de precieze inhoud van hetgeen door een instantie aan gegevens wordt geregistreerd en de wijze van registratie, alsmede een adequaat zicht op de zich steeds verder ontwikkelende (informatie-)technologische middelen die ter identificering van de betrokken persoon kunnen worden ingezet'.
[31] Zie voor de volledige opsomming artikel 4, tweede lid, AVG: "verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens."

2.3.2 Een blok omvat kort gezegd een header, de inhoud van het blok en de public key. Dit kan schematisch als volgt worden weergegeven.

Schematische weergave van de inhoud van een blok op de blockchain



2.3.3 De vraag rijst welke onderdelen van de blockchain persoonsgegevens kunnen bevatten. Hieronder volgt een bespreking per afzonderlijk onderdeel van een blok.

Header

De header van het blok is niets anders dan de aanduiding van het nummer van het blok op de blockchain, inclusief een verwijzing naar het vorige blok. De header bevat kort gezegd de volgende onderdelen:

- het versienummer van het huidige blok;
- een hash (van het nummer én de inhoud) van het vorige blok;
- de tijdcode van de datum en tijd dat het huidige blok is aangemaakt;
- de nonce, oftewel een getal dat door de nodes zal worden gebruikt om een nieuwe blok op de blockchain te zetten.

Bevat de header persoonsgegevens?
Ja, dat is mogelijk. De header kan, afhankelijk van de inhoud daarvan, (bijzondere) persoonsgegevens bevatten. Dit hangt af van de inhoud van de hash van het vorige blok. Twee situaties zijn denkbaar:

I. geen van de vorige blokken bevatten (bijzondere) persoonsgegevens

In dit geval worden in de header van het huidige blok geen persoonsgegevens verwerkt. De hash bevat niets anders dan een hash van het vorige blok zonder persoonsgegevens. De AVG is niet op de header van toepassing. We benadrukken dat het hier gaat om de situatie dat *alle* voorgaande blokken geen persoonsgegevens bevatten. Hiervan is slechts sprake in het geval de

header, de inhoud van het blok en de public key van *al* die voorgaande blokken (en het blok zelf) geen persoonsgegevens bevatten.

II. alle of een deel van de vorige blokken bevatten wél (bijzondere) persoonsgegevens met als gevolg dat de hash in de header een (gehaste) kopie van de persoonsgegevens in het vorige blok bevat.

In dit geval is aannemelijk dat in de header gehashte (oftewel gepseudonimiseerde) persoonsgegevens worden verwerkt.[32]

De inhoud van het blok

De inhoud van het blok kan (bijzondere) persoonsgegevens bevatten. Of dat zo is, is geheel afhankelijk van de gegevens die door middel van de blockchain worden uitgewisseld en de wijze waarop dat gebeurt. Hieronder volgt een beschrijving van een aantal situaties:

I. het blok bevat een persoonsgegeven (bijv. de naam van een patiënt) dat voor alle gebruikers op de blockchain zichtbaar is.

In dit geval is aan de materiële toepassingscriteria van de AVG voldaan.

II. het blok bevat een bijzonder persoonsgegeven (bijv. de medische behandeling die de patiënt heeft ondergaan) dat voor alle gebruikers op de blockchain zichtbaar is.

In dit geval is aan de materiële toepassingscriteria van de AVG voldaan. Doordat sprake is van een bijzonder persoonsgegeven geldt als aanvullend vereiste dat sprake moet zijn van een doorbrekingsgrond.[33]

III. het blok bevat een (bijzonder) persoonsgegeven, maar de inhoud van het blok is versleuteld of gehasht. Slechts geautoriseerde gebruikers van de blockchain kunnen de inhoud van het blok zien. Niet-geautoriseerde gebruikers kunnen dat niet. Zij zien slechts een gehashte/versleutelde versie van de inhoud van het blok.

Zowel de geautoriseerde gebruikers als de niet-geautoriseerde gebruikers verwerken persoonsgegevens:

- De *geautoriseerde gebruikers* kunnen de persoonsgegevens raadplegen. Dit betreft een verwerking van persoonsgegevens. In dit geval is aan de materiële toepassingscriteria van de AVG voldaan.

[32] Ten overvloede zij opgemerkt dat op het moment dat de inhoud van de blokken voor geautoriseerde gebruikers eenmaal zichtbaar is, de hash (van het vorige blok) in de header geen privacyrechtelijke consequenties meer heeft. Het gaat in dat geval immers om een hash van een vorig blok met een inhoud die toch al voor gebruikers zichtbaar is.
[33] Zie hierover verder onderdeel IV, randnrs. 4.3.15 e.v. van dit rapport

- Ook de *niet-geautoriseerde gebruikers* verwerken persoonsgegevens. Hoewel zij de inhoud van het blok niet kunnen zien, verwerken zij wel de versleutelde en/of gehashte inhoud van het blok. Zoals hiervoor toegelicht, wordt er in dit rapport van uitgegaan dat ook versleutelde/gehashte persoonsgegevens, persoonsgegevens zijn. Ook ten aanzien van niet-geautoriseerde gebruikers wordt dus aan de materiële toepassingscriteria van de AVG voldaan.

IV. Het blok bevat (een hash van) gegevens die niet herleidbaar zijn tot een natuurlijke persoon. Het kan hier gaan om technische metingen van medische apparaten, financiële gegevens van ziekenhuizen, geaggregeerde statistische gegevens of (andere) daadwerkelijk anonieme gegevens.

De AVG is in deze situatie niet van toepassing op de gegevens in het blok. De gegevens in het blok zijn namelijk niet herleidbaar tot een natuurlijke persoon en aldus ook geen persoonsgegevens.

V. Het blok bevat een (al dan niet versleutelde en/of gehashte) on-chain verwijzing naar (bijzondere) persoonsgegevens die buiten de blockchain staan opgeslagen (off-chain*).*

Het komt dikwijls voor dat het blok slechts een link of verwijzing naar persoonsgegevens bevat die off-chain staan opgeslagen (ook wel: een pointer). Denk aan de situatie dat een link op de blockchain wordt geplaatst naar resultaten van bepaalde medische onderzoeken die door een collega-ziekenhuis zijn verricht. Als het gebruik van links op een zodanige wijze kan worden vormgeven dat de inhoud van de link geen persoonsgegevens bevat zal de AVG niet van toepassing zijn op de inhoud van de transactie.[34] Voor zover de inhoud van de link wél persoonsgegevens bevat (de link bevat bijvoorbeeld de naam van de patiënt) zal de AVG wél van toepassing zijn.[35]

De Public Key

Het blok zal een vermelding bevatten van de public key van de verzender. De public key wordt per transactie van de gebruiker aan de ontvangende gebruikers meegezonden. De public key is een unieke sleutel die is gekoppeld aan de gebruiker en die bestaat uit een lange reeks getallen en cijfers.

[34] Hierbij zij opgemerkt dat een transactie – ook bij het gebruik van pointers – altijd de (gehashte) public key van de verstrekkende gebruiker zal bevatten. De AVG is van toepassing op de in de transactie opgenomen gehashte private key van de gebruiker. Het feit dat de private key aldus blijvend wordt verwerkt, lijkt echter geen wezenlijke issues met zich mee te brengen. Er doet zich bij het verwerken van de private key geen (wezenlijke) problemen voor bij de naleving van de vereisten van de AVG.
[35] Vanzelfsprekend is de AVG wel van toepassing op de persoonsgegevens die offline zijn opgeslagen en zal voor de verwerking daarvan bijvoorbeeld een grondslag moeten bestaan.

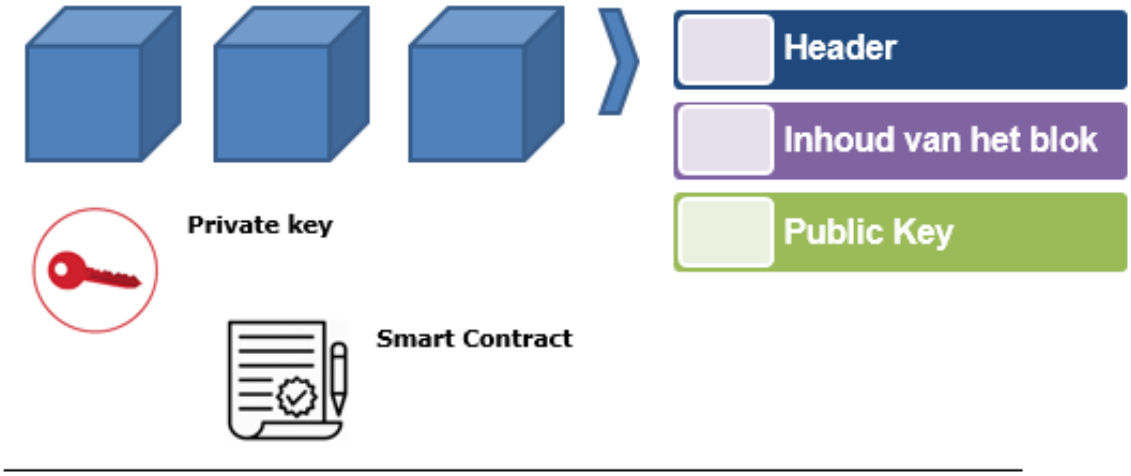
In dit rapport wordt aangenomen dat de public key een persoonsgegeven *kan* vormen voor zover de gebruiker daarvan een natuurlijke persoon is. De public key is in dat geval namelijk (indirect) herleidbaar tot een natuurlijke persoon en daarmee een persoonsgegeven.

Dit zal veelal anders zijn in de situatie dat de gebruiker van de public key *geen* natuurlijke persoon is, maar een rechtspersoon (bijv. een ziekenhuis, een huisartsenpost of een verzekeraar). Gegevens over rechtspersonen zijn (doorgaans) geen persoonsgegevens.[36] Als de public key niet (indirect) herleidbaar is tot een natuurlijke persoon, zal de AVG niet van toepassing zijn.

Overige persoonsgegevens die op de blockchain kunnen worden verwerkt

2.3.4 Naast de persoonsgegevens die kunnen worden verwerkt *in* de blokken, is het ook mogelijk dat elders op de blockchain persoonsgegevens worden verwerkt. Zo zou het bijvoorbeeld mogelijk kunnen zijn dat er persoonsgegevens worden verwerkt als private key of in een smart contract.

Schematische weergave van de volledige blockchain



De Private Key

Iedere gebruiker van de blockchain beschikt over een private key. De private key van de gebruiker is een geheime sleutel die is gekoppeld met de public key van de gebruiker. De gebruiker kan met zijn private key de inhoud van de transacties binnen de blockchain - voor zover hij daartoe geautoriseerd is - ontsleutelen. Doordat de private key is gekoppeld aan de individuele gebruiker, kan deze private key ook een persoonsgegeven vormen over de gebruiker, mits de private key is te herleiden naar een natuurlijke persoon. De private key komt doorgaans echter niet op de blockchain terecht. Daarvan uitgaande

[36] Voor zover duidelijk is dat bij een public key bij een specifieke medeweker van de rechtspersoon "hoort", zal de public key een persoonsgegeven over de betreffende medewerker vormen.

worden er met (het bestaan van) de private key als zodanig geen persoonsgegevens *op de blockchain* verwerkt.

Het is mogelijk dat de private key is gekoppeld aan een rechtspersoon (bijv. een ziekenhuis). In dat geval staat de private key in beginsel niet in verband met een natuurlijke persoon en is van een persoonsgegeven geen sprake. [37]

Het Smart contract
Smart contracts zijn toepassingen die op een blockchain geplaatst kunnen worden. Zoals reeds toegelicht in deel I van dit rapport, is een smart contract een stuk programmeercode waarin een handeling afhankelijk is gemaakt van het voltrekken van één of meer gebeurtenissen. Het is in wezen een deterministische computerprogramma: gegeven een bepaalde input en bepaalde beginwaarden zal het altijd dezelfde output genereren.

Hoewel in de meeste gevallen het smart contract slechts deterministische regels bevat voor de blockchain, is het mogelijk dat in het smart contract persoonsgegevens zijn opgenomen. Deze situatie doet zich voor indien de deterministische regels persoonsgebonden zijn.[38]

Relevante uitzondering: zuiver persoonlijke of huishoudelijke activiteit

2.3.5 Hiervoor is opgemerkt dat aan de materiële toepassingscriteria wordt voldaan als binnen de blockchain persoonsgegevens worden verwerkt. Daarop geldt één (voor dit rapport relevante) uitzondering: de AVG is niet van toepassing op de verwerking van persoonsgegevens door natuurlijke personen bij de uitoefening van een zuiver persoonlijke of huishoudelijke gebruik.[39] Het gaat hier om verwerkingen van persoonsgegevens die geen enkel verband houden met een beroeps- of handelsactiviteit. Voorbeelden daarvan zijn het (voor eigen gebruik) bijhouden van adresbestanden, het gebruik van social media en online activiteiten in de context van social media.[40] Commerciële partijen die aan natuurlijke personen de middelen verschaffen om persoonsgegevens voor persoonlijke of huishoudelijke activiteiten te verwerken, vallen uiteraard wél onder de reikwijdte van de AVG.

2.3.6 Individuele natuurlijke personen die de blockchain gebruiken voor zuiver persoonlijk gebruik zijn niet gebonden zijn aan de regels van de AVG als zij persoonsgegevens

[37] Zie de eerdere bespreking van de public key.
[38] Hierbij kan gedacht worden aan de situatie waarbij in het smart contract is opgenomen dat indien situatie A ten aanzien van een bepaalde persoon B zich voordoet, persoon C en D daarvan een specifieke melding ontvangen. Het gaat daarbij om persoonsgebonden deterministische regels die zijn opgenomen in het smart contract omdat de personen genoemd worden in het smart contract. De vermelding van deze personen in het smart contract is een persoonsgegeven.
[39] Artikel 2, tweede lid, aanhef en onder c, AVG. De term 'persoonlijke of huishoudelijke doeleinden' in de zin van die bepaling ziet op de activiteit van de persoon die persoonsgegevens verwerkt, niet op de persoon wiens gegevens worden verwerkt. Zie onder meer HvJ EU 10 juli 2018, C-25/17, ECLI:NL:C:2018:551, rov. 40 en HvJ EU 11 december 2014, C-212/213, ECLI:NL:2014:2428, rov. 31 en 33.
[40] Overweging 18 van de AVG.

verwerken. Dit ligt bijvoorbeeld anders voor (degenen die werkzaam zijn bij) de bestuursorganen en rechtspersonen die de blockchain gebruiken en/of beheren. Er zal dan (veelal) geen sprake zijn van verwerking voor zuiver persoonlijke of huishoudelijke doeleinden. Zodra zij persoonsgegevens verwerken, is ten aanzien van hen al snel aan de materiële toepassingscriteria van de AVG voldaan.

Tussenconclusie

Bij het verwerken van gegevens in een blockchain zal al snel sprake zijn van een verwerking van persoonsgegevens, en zal dus snel aan de materiële eisen voor toepasselijkheid van de AVG worden voldaan.[41] Om te kunnen vaststellen of binnen de (beoogde) blockchain persoonsgegevens worden verwerkt, dient aan de hand van deze paragraaf te worden nagelopen of de volgende onderdelen van de blockchain persoonsgegevens bevatten:

- *De header van het blok;*
- *De inhoud van het blok;*
- *De public key die is opgenomen in het blok;*
- *De private key;*
- *Het smart contract.*

Aanbevelingen voor het ontwerp van de blockchain

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. Een belangrijk voordeel van deze benadering is dat de AVG niet van toepassing is op de inhoud van de transacties (met uitzondering van de in de transactie opgenomen hash van de public key).

Zoals in het verdere vervolg van dit rapport aan bod zal komen, heeft dit diverse voordelen.

De gebruikers blockchain hoeven ten aanzien van de gegevens in de transacties niet te worden aangemerkt als verwerkingsverantwoordelijken of verwerker.[42]

De gebruikers van de blockchain hoeven dan ook geen wettelijke grondslag te hebben voor het verwerken van de inhoud van iedere transacties. Ze zullen slechts een wettelijke grondslag nodig hebben voor het verwerken van (i) de (gehashte) public key van de gebruikers op de blockchain en (ii) de persoonsgegevens die buiten de blockchain om worden verwerkt.[43]

[41] Als de gebruiker een natuurlijke persoon is die de persoonsgegevens voor zuiver persoonlijke of huishoudelijke activiteiten verwerkt, zal de AVG op die persoon (veelal) niet van toepassing zijn. Gedacht kan worden aan de zorgbehoevende die gebruikt maakt van Mijn Zorg Log.
[42] Zie voor een nadere toelichting op deze begrippen deel III, paragraaf 3.3.
[43] Zie Deel IV van dit rapport

Daar komt bovendien bij dat gebruikers – gelet op de beperkte set aan persoonsgegevens die op de blockchain worden verwerkt (feitelijk slechts de public key) - sneller voldoen aan de materiele vereisten van de AVG (in het bijzonder het beginsel van dataminimalisatie, het beginsel van opslagbeperking en privacy by design en default).[44]

Tot slot maakt het gebruik van pointers het mogelijk om – via het ontoegankelijk maken van de gegevens – (zoveel mogelijk) uitvoering te geven aan de rechten van de betrokkenen, in het bijzonder het verwijderingsrecht.[45]

Let op: het gebruik van pointers maakt niet dat AVG in zijn geheel niet meer van toepassing is op de blockchain.[46]

2.4 Territoriale reikwijdte AVG

2.4.1 Nadat is vastgesteld dat aan de materiële toepassingscriteria van de AVG is voldaan, moet ook nog worden bezien of aan de territoriale eisen is voldaan. Is dat het geval, dan is de AVG van toepassing. De territoriale reikwijdte van de AVG is geregeld in artikel 3 van de AVG. Toegespitst op blockchain is de AVG van toepassing op:

- de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een gebruiker van de blockchain[47] in de Europese Unie, ongeacht of de verwerking in de Europese Unie plaatsvindt (artikel 3, eerste lid, AVG);
- de verwerking van persoonsgegevens van betrokkenen[48] die zich in de Unie bevinden, door een buiten de Europese Unie gevestigde gebruiker van de blockchain[49], wanneer de verwerking verband houdt met;
  (a) het aanbieden van goederen of diensten aan deze betrokkenen in de Europese Unie, ongeacht of daarvoor een betaling van de betrokkenen is vereist; of
  (b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt (artikel 3, tweede lid, AVG).

[44] Zie Deel V van dit rapport.
[45] Zie Deel VI van dit rapport.
[46] Allereerst zal in de transactie altijd een gehashte public key zichtbaar zijn, ook bij het gebruik van pointers. De AVG is in zoverre dus wel van toepassing. Het is bovendien mogelijk dat op de blockchain ook persoonsgegevens buiten de inhoud van de transacties om worden verwerkt, bijvoorbeeld ten behoeve van het uitvoeren van het smart contract of het uitvoeren van het consensusmodel. De AVG is in dat geval van toepassing op de aanvullende persoonsgegevens die buiten de transacties worden verwerkt. Zowel ten aanzien van het verwerken van de public key, als het verwerken van de additionele gegevens buiten de transacties geldt echter dat zich geen (wezenlijke) problemen voordoen bij het naleven van de vereisten van de AVG.
[47] Dit kan een verwerkingsverantwoordelijke of een (sub)verwerker zijn. Zie Deel III voor een nadere toelichting op het onderscheid tussen een verwerkingsverantwoordelijke en een (sub)verwerker.
[48] De natuurlijke persoon op wie een persoonsgegeven betrekking heeft, zoals de patiënt / zorgbehoevende.
[49] Dit kan een verwerkingsverantwoordelijke of een (sub)verwerker zijn. Zie Deel III voor een nadere toelichting op het onderscheid tussen een verwerkingsverantwoordelijke en een (sub)verwerker.

Vestiging in de EU (artikel 3, eerste lid, AVG)

2.4.2 Van een 'vestiging' in de zin van artikel 3 AVG is sprake op het moment dat een publieke of private partij duurzaam is gevestigd binnen de Europese Unie. Dit kan aldus een overheidsinstantie zijn, zoals het Zorginstituut Nederland, of een vestiging van een private partij, zoals een ziekenhuis, zorgkantoor of verzekeraar. De rechtsvorm van de vestiging, of het nu gaat om bijkantoor of dochteronderneming met rechtspersoonlijkheid, is daarbij niet doorslaggevend. Een duurzame vestiging veronderstelt het effectief en daadwerkelijk uitoefenen van activiteiten. In de Europese rechtspraak wordt dit begrip ruim uitgelegd. Al bij één enkele vertegenwoordiger kan sprake zijn van een duurzame vestiging. Doorslaggevend is dat diegene met een voldoende mate van duurzaamheid en met behulp van de nodige middelen de verlening van de concrete dienst in de lidstaat mogelijk maakt.[50] Het begrip vestiging heeft betrekking op iedere vorm van activiteit die via een duurzame vestiging wordt uitgeoefend, 'zelfs geringe, reële en daadwerkelijke' activiteiten die via de vestiging worden uitgeoefend. De AVG is van toepassing indien de verwerking van de persoonsgegevens door de gebruiker van de blockchain plaatsvindt in het kader van de activiteiten van de vestiging. Ook dit betreft een ruim criterium. Niet is vereist dat de betrokken verwerking van persoonsgegevens wordt verricht door de betrokken vestiging zelf, maar enkel dat deze wordt verricht in 'het kader van de activiteiten' daarvan.

2.4.3 Kort en goed leidt artikel 3, eerste lid, AVG ertoe dat alle gebruikers van een blockchain die zijn gevestigd binnen de EU onder de territoriale reikwijdte van de AVG vallen. Bij blockchains in de zorg zal deze situatie zich in verreweg de meeste gevallen voordoen. Vooralsnog zijn de meeste blockchains in de zorg immers nationaal georiënteerd. De ziekenhuizen, verzekeraars, apotheken etc. die gebruik maken van de blockchain zullen in dat geval gevestigd zijn binnen Nederland en dus vallen onder de territoriale reikwijdte van de AVG (artikel 3, eerste lid, AVG). Het is voor de territoriale toepasselijkheid van de AVG in dit geval niet relevant waar de node van de gebruiker fysiek staat. Zoals volgt uit artikel 3, eerste lid, AVG, hoeft de verwerking niet binnen de EU plaats te vinden. Ook als een Nederlandse gebruiker in het kader van diens vestiging in Nederland (of een andere lidstaat) gebruik maakt van een "buitenlandse blockchain" (en de nodes staan buiten de EU), zal de verwerking die plaatsvindt, vallen onder de territoriale reikwijdte van de AVG.

> ***Voorbeeld - Gebruik buitenlandse blockchain***
> *Een in Nederland gevestigde gebruiker (bijvoorbeeld een apotheek) maakt gebruik van een private, (permissioned) blockchain die wordt beheerd door een buiten de EU gevestigde partij (bijv. een Amerikaans farmaceutisch bedrijf). De verwerking binnen de blockchain door de Nederlandse gebruiker valt overeenkomstig artikel 3, eerste lid, AVG binnen de territoriale reikwijdte van de AVG. Dit geldt zelfs voor zover de nodes in het buitenland zouden*

[50] Overweging 22 en 23 AVG. Zie EDBP, Guidelines 3/2018 on the territorial scope of the GDPR (artikel 3), p. 6.

staan, of de gegevens op de nodes op servers in het buitenland zouden zijn opgeslagen.

2.4.4 Omgekeerd is het niet ondenkbaar dat in Nederland beheerde blockchains in de zorg toegankelijk zijn of zullen worden voor buitenlandse gebruikers. Hierbij kan gedacht worden aan blockchains van:

- internationale samenwerkingsverbanden van ziekenhuizen, waarbij een deel van de ziekenhuizen binnen de EU, maar ook een deel van de ziekenhuizen buiten de EU is gevestigd;
- internationale medische farmaceutische onderzoeken, waarbij meerdere partijen zijn betrokken;
- ontwikkelingshulpprojecten waarbij Nederlandse teams in het buitenland medische hulp aanbieden;
- buitenlandse verzekeraars met bijkantoren binnen de EU.

2.4.5 Doet een dergelijke situatie zich voor, dan zal aan de hand van artikel 3, eerste lid, AVG beoordeeld moeten worden of de buitenlandse gebruikers van de blockchain vallen onder de territoriale reikwijdte van de AVG. Dit zal per concreet geval beoordeeld moeten worden.

Persoonsgegevens hebben betrekking op betrokkenen binnen de EU (artikel 3, tweede lid, AVG)

2.4.6 Indien een gebruiker van een blockchain buiten de EU is gevestigd, en de gebruiker valt *buiten* de territoriale reikwijdte van artikel 3, eerste lid, AVG, dan zal in geval van blockchains in de zorg - in verreweg de meeste gevallen - de AVG tóch van toepassing kunnen zijn, ervan uitgaande dat ook aan de materiële toepasselijkheidseisen wordt voldaan.

2.4.7 Artikel 3, tweede lid, aanhef en onder a, AVG bepaalt dat de AVG ook van toepassing is op het aanbieden van goederen of diensten aan betrokkenen in de EU[51] door niet in de EU gevestigde partijen, ongeacht of daarvoor een betaling is vereist. Deze bepaling is ook relevant voor blockchains in de zorg. Blockchains in de zorg zullen vaak worden gebruikt voor het aanbieden van (medische) diensten of producten aan personen *binnen* de EU. Dergelijke blockchains vallen binnen de territoriale reikwijdte van de AVG, ongeacht of de gebruiker van de blockchain is gevestigd binnen de EU.

Voorbeeld – Internationale klinische onderzoeken
Een Indiaas farmaceutisch bedrijf, zonder vestiging of activieiten in de EU, sponsort klinische onderzoeken in Nederlandse en Belgische ziekenhuizen naar een nieuw medicijn. De meerderheid van de patiënten van de klinische onderzoeken is gevestigd in Nederland. De resultaten van de klinische onderzoeken worden gedeeld via een private permissioned blockchain. Ervan

[51] Het gaat daarbij dus om zowel Europese burgers, als buitenlanders die zich binnen de EU bevinden.

uitgaande dat het Indiase bedrijf en de deelnemende ziekenhuizen (via hun node) toegang hebben tot de blockchain en zich op de blockchain persoonsgegevens (over de onderzochte personen) bevinden, zal er sprake zijn van de verwerking van persoonsgegevens. De nodes staan verspreid over België, Nederland en India. Er is aldus sprake van de verwerking van persoonsgegevens binnen de EU en buiten de EU (India). De Nederlandse en Belgische ziekenhuizen vallen onder de reikwijdte van de AVG, aangezien zij gevestigd zijn binnen de EU (artikel 3, eerste lid, AVG). Ook het Indiase farmaceutische bedrijf valt binnen de reikwijdte van de AVG, nu de persoonsgegevens op de blockchain betrekking hebben op personen die zich binnen de EU (Nederland en België) bevinden (artikel 3, tweede lid, aanhef en onder a, AVG).[52]

2.5 Conclusie deel II

2.5.1 De AVG is van toepassing op een blockchain indien aan zowel de materiële als territoriale eisen is voldaan. Aan de materiële eis is voldaan als gebruikers persoonsgegevens op de blockchain verwerken en zij dat niet doen als natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit.[53] Van het verwerken van persoonsgegevens is al snel sprake. Het versleutelen en/of hashen van de persoonsgegevens op de blockchain, maakt in de meeste gevallen niet dat geen persoonsgegevens meer worden verwerkt. Dergelijke technieken zijn eerder te zien als privacyverhogende maatregelen. Ten aanzien van de meeste gebruikers van een blockchain zal (ook) worden voldaan aan de territoriale eisen voor toepasselijkheid van de AVG.

[52] Dit betreft een variatie op een voorbeeld dat de EDPB (voorbeeld 20) aanhaalt in zijn Richtlijn 3/2018. Zie EDBP, Guidelines 3/2018 on the territorial scope of the GDPR (artikel 3), p. 11.
[53] Dit betekent dat de AVG in beginsel bijvoorbeeld niet van toepassing zal zijn op de zorgbehoevende die van Mijn Zorg Log gebruik maakt.

3 WIE VERWERKEN PERSOONSGEGEVENS OP DE BLOCKCHAIN?

3.1 Inleiding

3.1.1 Indien op grond van deel II wordt vastgesteld dat de blockchain persoonsgegevens bevat en de AVG van toepassing is, is vervolgens de vraag *wie* deze persoonsgegevens verwerken. Dit zijn in ieder geval (de nodes van) de *geautoriseerde gebruikers*, oftewel:

- de gebruikers die door middel van de blockchain een transactie met daarin persoonsgegevens aan (een deel van) de andere geautoriseerde gebruikers verzenden, en;
- de gebruikers die de transactie ontvangen en bevoegd zijn om de inhoud van het blok te raadplegen.

3.1.2 Het is voor het antwoord op de vraag of de ontvangende gebruiker persoonsgegevens verwerkt niet van belang of deze naast leesrechten ook beschikt over schrijfrechten. Het enkele raadplegen van de persoonsgegevens in het blok vormt al een verwerking van persoonsgegevens.

3.1.3 In dit rapport wordt zekerheidshalve tot uitgangspunt genomen dat ook de *niet-geautoriseerde* gebruikers persoonsgegevens verwerken.[54] Hoewel zij als niet-geautoriseerde gebruikers de inhoud van bepaalde blokken (de blokken waarvoor zij niet-geautoriseerd zijn) niet kunnen raadplegen, verwerken zij namelijk wel de hash van de inhoud van de blokken.[55]

> Zoals in het vorige deel is besproken, wordt er, gelet op de opinie van de Artikel-29 Werkgroep, in dit rapport zekerheidshalve vanuit gegaan dat een hash een (gepseudonimiseerd) persoonsgegeven is.

3.2 Toepasselijkheid van deel III op de blockchain

3.2.1 Dit deel van het rapport is met name relevant voor blockchains waarbij (bijzondere) persoonsgegevens in transacties op de blockchain worden verwerkt.

3.2.2 In het vorige deel is belicht dat het sterk de voorkeur verdient om de gegevens op de blockchain te beperken tot pointers naar off-chain persoonsgegevens, waarbij de pointers geen persoonsgegevens bevatten.[56] Een belangrijk voordeel van deze

[54] Het onderscheid tussen niet-geautoriseerde en geautoriseerde gebruikers zal zich slechts voordoen bij permissioned blockchains, aangezien slechts in permissioned blockchains autorisaties kunnen worden toebedeeld.
[55] In dit rapport wordt in het midden gelaten of de niet-geautoriseerde gebruiker een node heeft die niet meedoet aan het consensus-mechanisme (een zogenoemde participating of light node) of dat die gebruiker een node heeft die *wel* aan het consensus-mechanisme meedoet (een zogenoemde validating of full node) en in dat kader persoonsgegevens verwerkt, nu de niet-geautoriseerde gebruiker de betreffende persoonsgegevens toch wel, in gehashte vorm, zal verwerken als de transactie aan de blockchain wordt toegevoegd.
[56] Bij deze opties vindt de feitelijke verwijdering van persoonsgegevens off-chain plaats.

benaderingen is dat de AVG niet van toepassing is op de inhoud van de transacties. De gebruikers hoeven ten aanzien van de gegevens in de transacties niet te worden aangemerkt als verwerkingsverantwoordelijken of verwerker (zie voor een nadere toelichting op deze begrippen paragraaf 3.3 van dit deel). De gebruikers hoeven dan ook geen wettelijke grondslag te hebben voor het verwerken van de inhoud van iedere transactie. Ze zullen slechts een wettelijke grondslag nodig hebben voor het verwerken van (i) de (gehashte) public key van de gebruikers op de blockchain en (ii) de persoonsgegevens die zij (bijv. met behulp van een pointer op de blockchain) off-chain met elkaar uitwisselen (zie deel IV van dit rapport).

3.2.3 Worden er toch (gehashte en versleutelde) persoonsgegevens geplaatst op de blockchain, dan is de AVG ook van toepassing op de inhoud van de transacties. Elke gebruiker van de blockchain moet in dat geval worden aangemerkt als verwerkingsverantwoordelijke of verwerker. De gebruikers moeten bovendien voor ieder persoonsgegeven dat (gehasht) in een transactie op de blockchain wordt geplaatst een wettelijke grondslag hebben om dat persoonsgegeven te verwerken. In veel gevallen zal een dergelijke wettelijke grondslag voor een deel van de gebruikers (namelijk de gebruikers die een transactie niet mogen zien, maar de persoonsgegevens in de transactie wel in gehashte vorm verwerken) echter ontbreken. In dit deel van het rapport zal worden onderzocht in hoeverre dit punt kan worden ondervangen door de niet-geautoriseerde gebruikers aan te merken als (sub)verwerkers voor de geautoriseerde gebruikers die persoonsgegevens op de blockchain plaatsen.

> Aangezien het vrijwel is uitgesloten dat elke gebruiker van de blockchain een wettelijke grondslag heeft voor het verwerken van alle persoonsgegevens die in transacties op de blockchain worden geplaatst, wordt in dit rapport tot uitgangspunt genomen dat de persoonsgegevens die toch[57] in de transacties worden verwerkt, altijd gehasht moeten worden, zodat op zijn minst wordt voorkomen dat niet-geautoriseerde gebruikers de inhoud van de transacties kunnen raadplegen.

3.3 Wie is verwerkingsverantwoordelijke en wie (sub)verwerker?

3.3.1 De AVG maakt bij het verwerken van persoonsgegevens onderscheid tussen de verwerkingsverantwoordelijke en de (sub)verwerker. Daar wordt hierna verder op ingegaan.

De verwerkingsverantwoordelijke

3.3.2 De verwerkingsverantwoordelijke speelt in het stelsel van de AVG een centrale rol. De verwerkingsverantwoordelijke draagt de verantwoordelijkheid dat de verwerking van persoonsgegevens op de blockchain rechtmatig – en aldus in overeenstemming met de

[57] Dus in ieder geval de public key van de gebruiker indien met pointers wordt gewerkt en eventuele aanvullende persoonsgegevens indien niet met pointers wordt gewerkt, maar in de transacties op de blockchain (aanvullende) persoonsgegevens worden verwerkt.

vereisten van de AVG – plaatsvindt.[58] Het is primair de verwerkingsverantwoordelijke die bij strijdig handelen met de AVG het risico loopt op sancties van de Autoriteit Persoonsgegevens ('AP'). Het is van belang om vast te stellen wie binnen de blockchain optreedt of optreden als verwerkingsverantwoordelijke(n).

3.3.3 Een verwerkingsverantwoordelijke is degene die, alleen of samen met anderen, het doel en de middelen van de verwerking van persoonsgegevens vaststelt.[59]

> Met het bepalen van het doel van de verwerking wordt bedoeld dat de verwerkingsverantwoordelijke de zeggenschap heeft over waarom de persoonsgegevens worden verwerkt en voor welke concrete doelen de persoonsgegevens zullen worden ingezet. Het vaststellen van het doel van de verwerking is een exclusieve bevoegdheid van de verwerkingsverantwoordelijke.
>
> Met het vaststellen van de middelen van de verwerking wordt gedoeld op het vaststellen van de wijze waarop de verwerking plaats zal vinden, kortom: hoe worden de persoonsgegevens verwerkt ten behoeve van het vastgestelde doel.

3.3.4 Indien twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en de middelen van de verwerking bepalen, wordt gesproken van 'gezamenlijke verwerkingsverantwoordelijken'.[60]

De geautoriseerde gebruikers als verwerkingsverantwoordelijke(n) van de blockchain

3.3.5 Een vaak gestelde vraag in blockchain-verband is welke gebruikers van de blockchain kunnen worden aangemerkt als verwerkingsverantwoordelijken. Het aanwijzen van een verwerkingsverantwoordelijke leidt bij een blockchain vaak tot moeilijkheden. Het gedecentraliseerde karakter van een blockchain maakt dat geen duidelijke partij kan worden aangewezen die de beslissende zeggenschap heeft over de verwerkingen die binnen de blockchain plaatsvinden. Verschillende benaderingen zijn denkbaar:

- **Benadering I** - iedere (node van de) gebruiker van de blockchain is een verwerkingsverantwoordelijke, ook ten aanzien van de inhoud van transacties waartoe hij niet is geautoriseerd[61];
- **Benadering II** - een (node van de) gebruiker van de blockchain is pas verwerkingsverantwoordelijke op het moment dat deze daadwerkelijk geautoriseerd is om de inhoud van de betreffende transacties te raadplegen en/of te wijzigen.

[58] Zie voor die vereisten de delen 3 en 4 van dit rapport.
[59] Artikel 4 aanhef en onder 7, AVG.
[60] Artikel, 26, eerste lid, AVG.
[61] De redenering daarbij is dat de nodes gezamenlijk bepalen of een transactie kan worden toegevoegd en dus invloed uitoefenen op het doel en de middelen van de verwerking.

3.3.6 De Europese privacytoezichthouders hebben (vooralsnog) geen duidelijkheid verschaft over de vraag welke gebruikers van een blockchain handelen als verwerkingsverantwoordelijken. De benadering dat iedere gebruiker van de blockchain wordt aangemerkt als verwerkingsverantwoordelijke (benadering I) zal in de praktijk vaak kunnen leiden tot privacyrechtelijke vragen. De voornaamste vraag bij het aanwijzen van alle gebruikers van de blockchain als verwerkingsverantwoordelijken, is of zij wel allemaal een eigen wettelijke grondslag hebben voor de verwerking van de gehashte persoonsgegevens op de blockchain. Goed denkbaar is dat dat, afhankelijk van wat er op de blockchain wordt gezet en welke gebruikers daarin participeren, niet altijd zo is.

> Denk bijvoorbeeld aan de situatie dat een zorgverzekeraar en zorgaanbieder medische gegevens uitwisselen over een patiënt, maar de apotheek – die ook participeert op de blockchain – die gegevens ook kan zien in gehashte vorm, terwijl de gegevens niet voor de apotheek bestemd zijn. De apotheek beschikt niet over een wettelijke grondslag om de gehashte persoonsgegevens te verwerken.

3.3.7 Dit punt zou niet spelen als de niet-geautoriseerde gebruikers (achter de nodes) ten aanzien van de gehashte persoonsgegevens in de transacties waarvoor zij niet zijn geautoriseerd, zijn aan te merken als verwerker van de wél geautoriseerde gebruikers (benadering II). In dat geval, dus als verwerker, zouden zij de grondslag van de wel geautoriseerde gebruikers kunnen overnemen. Voordeel daarvan is dat de niet-geautoriseerde gebruikers als verwerker hun wettelijke grondslag voor het verwerken van de gehashte persoonsgegevens kunnen ontlenen aan de wettelijke grondslagen van de geautoriseerde verwerkingsverantwoordelijken.[62]

3.3.8 Zoals hierna zal worden toegelicht, zijn er goede argumenten voor deze laatste benadering. Verdedigbaar is dat alleen de (nodes van de) geautoriseerde gebruikers verwerkingsverantwoordelijke zijn voor de transacties waarvoor zij geautoriseerd zijn.[63] Tegen de achtergrond van het voorgaande wordt in dit rapport tot uitgangspunten genomen dat:

---

[62] Er is ook nog een benadering denkbaar, waarbij de niet-geautoriseerde gebruikers verwerkingsverantwoordelijken, noch verwerker zijn. Er zou dan betoogd moeten worden dat (de nodes van) niet-geautoriseerde gebruikers te vergelijken zijn met telecommunicatie- of elektronsiche postdiensten, die slechts berichten doorgeven ten behoeve van anderen. De (Europese) wetgever en de Europese toezichthouders beschouwen telecommunicatie- of elektronische postdiensten niet als verwerkingsverantwoordelijken of verwerkers ten aanzien van de (persoonsgegevens in de) inhoud van de berichten die zij doorgeven. Dergelijke diensten zijn slechts verwerkingsverantwoordelijke ten aanzien van de aanvullende gegevens die zij ten behoeve van het verzending van de berichten verwerken. Het is echter onzeker is of (nodes van) niet-geautoriseerde gebruikers inderdaad gelijk zouden kunnen worden gesteld aan telecom- en postdiensten. Zie ook randnummer 3.3.27.

[63] Deze opvatting lijkt in lijn met de opvatting in een whitepaper van de Franse privacy toezichthouder (de Commission Nationale Informatique & Libertés 'CNIL') waarin de CNIL stelt dat het enkele minen onvoldoende is om te spreken van een verwerkingsverantwoordelijke node. Zie CNIL, 'blockchain: Solutions for a responsible use of the blockchain in the context of personal data', p. 2 t/m 4.

- (de node van) de geautoriseerde gebruiker verwerkingsverantwoordelijke is voor de persoonsgegevens die hij op de blockchain plaatst[64];
- (de node van) de geautoriseerde gebruiker verwerkingsverantwoordelijke is voor de persoonsgegevens ten aanzien waarvan hij is geautoriseerd om ze te raadplegen, wijzigen en/of verwijderen.[65]

(hierna gezamenlijk aangeduid als: de geautoriseerde verwerkingsverantwoordelijken)

3.3.9 Dit zal anders zijn ten aanzien van een geautoriseerde gebruiker die – buiten de blockchain om – al verwerker was voor een partij (bijvoorbeeld een ziekenhuis) en die die verwerkerswerkzaamheden nu voortzet met gebruikmaking van de blockchain. In dat geval zal die partij vermoedelijk verwerker blijven voor het ziekenhuis ("geautoriseerde verwerkers"). Verdedigbaar is, zoals gezegd, dat ook niet-geautoriseerde gebruikers zijn aan te merken als verwerkers, zolang zij persoonsgegevens alleen in gehashte vorm verwerken (zie daarover de volgende paragraaf vanaf randnr. **Fout! Verwijzingsbron niet gevonden.**).

Tussenconclusie
De (nodes van) geautoriseerde gebruikers van een blockchain kunnen worden onderverdeeld in geautoriseerde verwerkingsverantwoordelijken en geautoriseerde verwerkers.

Verwerkingsverantwoordelijken
De geautoriseerde gebruiker van de blockchain is een gebruiker die zelfstandig bepaalt of hij persoonsgegevens op de blockchain verwerkt en voor welke doelen hij dat doet.

Meer concreet wordt in dit rapport tot uitgangspunt genomen dat:
- (de node van) de geautoriseerde gebruiker als verwerkingsverantwoordelijke optreedt voor de persoonsgegevens die hij op de blockchain heeft geplaatst;
- (de node van) de geautoriseerde gebruiker verwerkingsverantwoordelijke is voor de persoonsgegevens in de blokken die hij kan raadplegen, wijzigen en/of verwijderen.

Geautoriseerde verwerkers
Geautoriseerde verwerkers zijn de externe partijen die in opdracht van een of meer van de geautoriseerde verwerkingsverantwoordelijken deelnemen aan de blockchain en ten behoeve van hen persoonsgegevens op de blockchain

[64] Tenzij dat een gebruiker is op wie de AVG niet van toepassing is, bijvoorbeeld omdat de verstrekking plaatsvindt in het kader van een persoonlijke activiteit. Denk aan de transactie die op de blockchain wordt gezet door een zorgbehoevende.
[65] Zie de vorige voetnoot. Verder: het kan hier dus gaan om enkel het recht om de inhoud van het blok te raadplegen, maar kan ook meer omvatten, waaronder het wijzigen of verwijderen van het blok. Zie over wijzigen en verwijderen paragraaf 6.4 van dit rapport.

verwerken.
Geautoriseerde verwerkers moeten worden onderscheiden van niet-geautoriseerde gebruikers. De niet-geautoriseerde gebruikers zijn de gebruikers die als verwerker kunnen worden aangemerkt voor de gehashte persoonsgegevens in de transacties waarvoor zij niet zijn geautoriseerd.

Verplichtingen van de (gezamenlijke) verwerkingsverantwoordelijken

3.3.10 Zoals hiervoor is gebleken, zullen er in iedere blockchain (zowel private als public blockchains) meerdere verwerkingsverantwoordelijke gebruikers zijn. Deze verwerkingsverantwoordelijke gebruikerszijn enerzijds *individueel* verantwoordelijk voor de persoonsgegevens die zij via de blockchain verstrekken en de persoonsgegevens ten aanzien waarvan zij lees- en (mogelijk) schrijfrechten hebben. Anderzijds zijn de verwerkingsverantwoordelijke gebruikers *gezamenlijk* verantwoordelijk voor onder meer de betrouwbaarheid en veiligheid van de blockchain. Het uitoefenen van gezamenlijke verwerkingsverantwoordelijkheid kan – mede gelet op het grote aantal verwerkingsverantwoordelijken en eventuele conflicterende belangen - leiden tot problemen. Zo kan de grote hoeveelheid aan verwerkingsverantwoordelijken leiden tot discussies over de respectievelijke verplichtingen van de verwerkingsverantwoordelijken die gebruikmaken van de blockchain, met als resultaat een impasse in de besluitvorming. Daarnaast kan het grote aantal verwerkingsverantwoordelijke gebruikers aan de zijde van de betrokkenen leiden tot onduidelijkheid over tot wie zij zich moeten richten om hun (privacy)rechten uit te oefenen. Om de hiervoor beschreven problemen te ondervangen, is het van belang dat de verwerkingsverantwoordelijke gebruikers voorafgaand aan het gebruik van de blockchain hun onderlinge verplichtingen en de wijze waarop de betrokkenen hun rechten kunnen uitoefenen vastleggen. De verwerkingsverantwoordelijke gebruikers zullen de volgende maatregelen moeten treffen.

I. Het opstellen van een onderlinge regeling (artikel 26 AVG)

3.3.11 De verwerkingsverantwoordelijke gebruikers zijn allereerst op grond van artikel 26, eerste lid, AVG verplicht om een zogenoemde *'onderlinge regeling'* vast te stellen. Een onderlinge regeling is een door de gezamenlijke verwerkingsverantwoordelijke vastgesteld document waarin zij hun respectievelijke verantwoordelijkheden ten aanzien van de naleving van de AVG vastleggen. De onderlinge regeling dient met name afspraken te bevatten over de uitoefening van de rechten van de betrokkenen en de informatieverplichting. In de onderlinge regeling – die als een onderdeel van de bredere governance zou kunnen worden gezien – zullen de verwerkingsverantwoordelijke gebruikers onder meer moeten vaststellen:

- de inhoud van de privacyverklaring, de wijze van het beschikbaar stellen van de privacyverklaring en de procedure voor het wijzigen en actualiseren van de privacyverklaring;

- tot wie de betrokkenen zich kunnen wenden indien zij hun rechten willen uitoefenen (bijv. hun inzage-, rectificatie- of verwijderingsrecht) en hoe uitvoering aan dergelijke verzoeken wordt gegeven;
- op welke wijze de verwerkingsverantwoordelijke gebruikers zullen handelen in geval van een datalek;
- welke procedures moeten worden doorlopen om deel te kunnen nemen aan de blockchain, op welke wijze en door wie wordt beslist of een partij (niet langer) wordt toegelaten en wie die (beëindiging van de) toegang verwezenlijkt;
- de te stellen beveiligingseisen, op welke wijze beslissingen worden genomen over veranderingen in de beveiliging en over de controle op getroffen beveiligingsmaatregelen;
- op welke wijze de verwerkingsverantwoordelijke gebruikers beslissingen nemen over veranderingen in de beveiliging van de blockchain, het smart contract of het consensusmodel;
- welke bewaartermijnen zullen worden gehanteerd en hoe deze bewaartermijnen zullen worden nageleefd;
- wie het aanspreekpunt is in geval van een eventueel onderzoek van de AP;
- hoe de regeling bekend wordt gemaakt aan de betrokkenen.

3.3.12 Om aan de betrokkenen duidelijkheid te verschaffen over tot wie zij zich moeten richten om hun rechten uit te oefenen, zouden de verwerkingsverantwoordelijke gebruikers kunnen overwegen om voor de blockchain een *contactpunt* voor betrokkenen aan te wijzen. Ook het oprichten van een dergelijk contactpunt zal moeten worden opgenomen in de onderlinge regeling.[66]

3.3.13 De inhoud van de onderlinge regeling zal aan de betrokkenen beschikbaar moet worden gesteld. Als gezegd zullen de verwerkingsverantwoordelijke gebruikers heldere afspraken moeten maken over de wijze van het beschikbaar stellen van de onderlinge regeling aan betrokkenen. Denkbaar is dat de verwerkingsverantwoordelijke gebruikers de onderlinge regeling via een gezamenlijke website beschikbaar maken. Een andere optie is dat één van de verwerkingsverantwoordelijke gebruikers (namens de andere verwerkingsverantwoordelijke gebruikers die gebruik maken van de blockchain) de betrokkenen een fysieke kopie van de onderlinge regeling verstrekt voordat de gegevens van de betrokkenen op de blockchain worden verwerkt (bijv. aan de start van de behandeling of bij opname van de patiënt). Belangrijk is tot slot dat de verwerkingsverantwoordelijke gebruikers bij iedere wijziging van de inhoud van de onderlinge regeling, de betrokkenen opnieuw een kopie van de onderlinge regeling verstrekken.

[66] Dit laat overigens onverlet dat betrokkenen – ondanks de gemaakte afspraken in de onderlinge regeling – het recht behouden om hun rechten ten opzichte van de individuele verwerkingsverantwoordelijke uit te oefenen. Het voorgaande volgt uit artikel 26, derde lid, AVG.

II. De noodzaak van het aanwijzen van een super user

3.3.14 Hoewel een onderlinge regeling zoals bedoeld in artikel 26 AVG duidelijkheid zal *kunnen* scheppen over de onderlinge verplichtingen van de verwerkingsverantwoordelijke gebruikers die gebruikmaken van de blockchain, neemt een onderlinge regeling nooit elke onduidelijkheid weg. Daar komt bovendien bij dat een grote hoeveelheid aan verwerkingsverantwoordelijke gebruikers kan leiden tot (langlopende) discussies over wie voor welke verwerkingen binnen de blockchain verantwoordelijk is. Tot slot kunnen discussie ontstaan over het gezamenlijk uitvoering geven aan eventuele verzoeken van betrokkenen of autoriteiten.

3.3.15 Om mogelijke discussies en conflicten te voorkomen, zouden de verwerkingsverantwoordelijke gebruikers kunnen overwegen 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. De super user kan het beheer van de blockchain voor zijn rekening nemen. Daarbij kan worden gedacht aan het beslissen over de toelating van nieuwe gebruikers van de blockchain, de uitgifte van public keys en het verwijderen van persoonsgegevens op de blockchain, een en ander conform de door de verwerkingsverantwoordelijke gebruikers gemaakte afspraken.

3.3.16 Doordat de gezamenlijke bevoegdheden van de verwerkingsverantwoordelijke gebruikers en het beheer van de blockchain worden ondergebracht bij de super user is het voor de betrokkenen duidelijk tot wie zij zich kunnen richten en kan de super user namens de gezamenlijke verwerkingsverantwoordelijke gebruikers beslissingen nemen, zonder dat daarover afzonderlijk hoeft te worden gediscussieerd. De super user is bevoegd om uitvoering te geven aan de in de onderlinge regeling geregelde onderwerpen, in het bijzonder om gevolg te geven aan verzoeken van de betrokkenen. De oprichting van een super user gaat verder dan het oprichten van een contactpunt, aangezien de super user daadwerkelijk een deel van de taken van de individuele gezamenlijke verwerkingsverantwoordelijke gebruikers ten behoeve van hen en in hun naam uitoefent.

3.3.17 Bovengenoemde aanpak zou in lijn zijn met eerdere adviezen van de Artikel-29 Werkgroep en de AP ten aanzien van (zorg)portals. In het verleden hebben de Artikel-29 Werkgroep en de AP geoordeeld dat zodra een platform of portal door een (zeer) groot aantal gezamenlijke verwerkingsverantwoordelijke gebruikers wordt beheerd, de gezamenlijke verwerkingsverantwoordelijke gebruikers in beginsel verplicht zijn om één beheerder (als gezamenlijk verwerkingsverantwoordelijke) aan te stellen die het beheer op zich neemt. De reden daarvoor is dat het anders voor de betrokkenen die gebruik maken van de portal volledig onduidelijk is tot wie van de gezamenlijke

verwerkingsverantwoordelijke gebruikers zij zich moeten richten.[67] Een nationaal voorbeeld betreft het Landelijk Schakelpunt.[68] Op advies van de AP hebben de duizend gezamenlijke verwerkingsverantwoordelijken besloten om een gezamenlijke rechtspersoon op te richten die het beheer op zich nam: de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ).[69]

3.3.18 Of en zo ja, in hoeverre de gezamenlijke verwerkingsverantwoordelijke gebruikers daadwerkelijk *verplicht* zijn tot het oprichten/benoemen van een super user, zal afhankelijk zijn van het aantal verwerkingsverantwoordelijke gebruikers. Eerder genoemde adviezen van de AP en de Artikel-29 Werkgroep zagen op situaties met veel verwerkingsverantwoordelijken. Hieruit lijkt te volgen dat bij een private blockchain met een beperkt aantal gebruikers, een onderlinge regeling met een contactpunt voor de betrokkenen mogelijk al voldoende zal zijn. Waar de precieze grens ligt bij het gebruik van blockchain, is niet met zekerheid te zeggen. De AP en de overige Europese privacy toezichthouders hebben zich hier nog niet over uitgelaten. Wel heeft de Franse privacy toezichthouder (CNIL) in blockchain-context op de mogelijkheid gewezen om een gezamenlijke rechtspersoon op te richten die namens gebruikers beslissingen neemt (oftewel een super user).[70]

Tussenconclusie – Verwerkingsverantwoordelijken van de blockchain
Geautoriseerde gebruikers die persoonsgegevens op de blockchain plaatsen, en geautoriseerde gebruikers die de transactie met daarin die persoonsgegevens ontvangen en bevoegd zijn om de inhoud daarvan te raadplegen en/of te wijzigen, zijn aan te merken als (gezamenlijke) verwerkingsverantwoordelijke gebruikers voor die persoonsgegevens.

[67] Vgl. Artikel 29-Werkgroep, 'Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker'', p. 28: "Voorbeeld 16: In een lidstaat stelt een overheidsinstantie een nationaal informatiecentrum in voor de uitwisseling van patiëntengegevens tussen zorgaanbieders. Door het grote aantal voor de verwerking verantwoordelijken – tienduizenden – ontstaat voor de betrokkenen (patiënten) een dermate onduidelijke situatie dat de bescherming van hun rechten in het geding komt. Voor betrokkenen is het namelijk onduidelijk tot wie zij zich kunnen richten met klachten, vragen en verzoeken om informatie, rectificatie en toegang tot persoonsgegevens. Bovendien is de overheidsinstantie verantwoordelijk voor de feitelijke opzet van de verwerking en de wijze waarop deze wordt gebruikt. Daarom moet worden geconcludeerd dat de overheidsinstantie die het datacentrum instelt als gezamenlijk voor de verwerking verantwoordelijk moet worden beschouwd, en tevens als aanspreekpunt voor verzoeken van betrokkenen." Zie tevens het hierna te bespreken voorbeeld van het Landelijk Schakelpunt.
[68] Het Landelijk Schakelpunt is een netwerk waarmee zorgaanbieders medische gegevens van hun patiënten digitaal met elkaar kunnen delen.
[69] Het ging bij het Landelijk Schakelpunt om een zorgportal die het NICTIZ had ontwikkeld en die zou worden beheerd door de gezamenlijke verwerkingsverantwoordelijke zorgaanbieders (het betrof hier duizenden zorgaanbieders). De gezamenlijke zorgaanbieders waren van plan om het Landelijke Schakelpunt door een verwerker te laten beheren. De Autoriteit Persoonsgegevens achtte dit plan onacceptabel. Door het grote aantal zorgaanbieders (duizenden) zou het voor de betrokkenen niet duidelijk zijn bij wie zij terecht zouden kunnen met hun klachten. Daar kwam bovendien bij dat de gezamenlijke zorgaanbieders naar verwachting niet in staat zouden zijn om het doel en de middelen van de gegevensverwerking te bepalen. Het AP zag in deze situatie twee oplossingen. Het meest voor de hand lag volgens de AP het creëren van een wettelijke grondslag voor de betreffende verwerkingsverantwoordelijke. Als alternatief werd genoemd het oprichten van een rechtspersoon, waarin alle participerende zorgaanbieders zouden zijn vertegenwoordigd en die verantwoordelijk zouden worden voor het Landelijk Schakelpunt. Vgl. De brieven van het CBP aan NICTIZ van 11 oktober 2005 (kenmerk z2005-0878) en 11 juli 2005 (z2005-0505). Destijds is gekozen voor het oprichten van een rechtspersoon: de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ).
[70] Zie CNIL, 'Blockchain: Solutions for a responsible use of the blockchain in the context of personal data', p. 2: "When a group of participants decide to carry out processing operations with a common purpose, the CNIL recommends to identify beforehand the data controller. For example, the participants may create a legal person in the form of an association or economic interest group. They may also choose to identify one participant who makes decisions for the ground and to designate the said participant as a data controller."

De geautoriseerde verwerkingsverantwoordelijken moeten worden onderscheiden van de geautoriseerde verwerkers. De geautoriseerde verwerkers zijn de externe partijen die in opdracht van een of meer van de geautoriseerde verwerkingsverantwoordelijken deelnemen aan de blockchain en ten behoeve van hen persoonsgegevens verwerken op de blockchain. Deze situatie zal zich (bijvoorbeeld) voordoen indien een partij buiten de blockchain om al verwerker was voor een partij (bijvoorbeeld een ziekenhuis) en de verwerker zijn verwerkerswerkzaamheden voortzet met gebruikmaking van de blockchain. In dat geval zal die partij vermoedelijk verwerker blijven (voor het ziekenhuis).

De gezamenlijke verwerkingsverantwoordelijken van de blockchain zijn op grond van artikel 26, eerste lid, AVG verplicht tot het vaststellen van een onderlinge regeling waarin hun respectieve verplichtingen ten aanzien van de verwerking op een transparante wijze worden vastgelegd.

Bij een groot aantal gezamenlijke verwerkingsverantwoordelijken kan het volgens de Europese privacy toezichthouders (waaronder de AP) verplicht zijn om één super user aan te wijzen, die een deel van de taken van de gezamenlijke verwerkingsverantwoordelijken uitvoert.

Het vaststellen van een onderlinge regeling en het aanwijzen van een super user vereist dat gebruikers met elkaar in overleg treden en heldere afspraken maken. Dit lijkt bij een public, permissionless blockchain een vrijwel onmogelijke exercitie. In dit licht bezien, verdient het dan ook de voorkeur om voor blockchains in de zorg waarin persoonsgegevens worden verwerkt te kiezen voor een private, permissioned blockchain, óók zodat daadwerkelijk uitvoering kan worden gegeven aan de afspraken die zijn opgenomen in de onderlinge regeling. De keuze voor een private, permissioned blockchain is van verder van belang gelet op:
- de regels voor internationale doorgifte[71];
- het vereiste van een wettelijke grondslag voor het verwerken van persoonsgegevens[72];
- het uitvoering kunnen geven aan de rechten van de betrokkene[73];
- het beginsel van dataminimalisatie.[74]

[71] Slechts bij een besloten blockchain kan voorafgaand aan de toetreding tot de blockchain worden vastgesteld in hoeverre een toetredende gebruiker zich buiten de EU bevindt en zo ja, of de daarbij optredende internationale doorgifte van persoonsgegevens op grond van de AVG toelaatbaar is (zie deel V, paragraaf 5.3 van dit rapport).
[72] Niet iedere gebruiker zal een wettelijke grondslag hebben voor het verwerken van alle persoonsgegevens die door gebruikers op de blockchain worden geplaatst. Om dit te ondervangen, dient het mogelijk te zijn om specifieke gebruikers te autoriseren om de transactie te raadplegen. Niet-geautoriseerde gebruikers zouden slechts de hash van deze gegevens mogen verwerken, mits zijn kunnen worden aangemerkt als verwerkers. Het toebedelen van autorisaties kan slechts plaatsvinden binnen een private, permissioned blockchain.
[73] Slechts in een private, permissioned blockchain zal duidelijk zijn wie de gebruikers van de blockchain zijn, zodat onderling afspraken kunnen worden gemaakt wie en op welke wijze uitvoering moet worden gegeven aan verzoeken van betrokkenen.
[74] Het beginsel van dataminimalisatie houdt (mede) in dat het aantal gebruikers van de blockchain beperkt blijft tot het strikt noodzakelijke. Slechts bij een besloten blockchain kan invloed worden uitgeoefend op de gebruikers die mogen worden toegelaten tot de blockchain. Zie voor een nadere toelichting randnrs. 3.3.28 van dit Deel.

Een private, permissioned blockchain is bovendien noodzakelijk om aan de super user (voor zover deze is aangesteld) taken toe te kunnen bedelen. In het verdere vervolg van dit rapport wordt er vanuit gegaan dat sprake is van een private permissioned blockchain.

3.3.19 Tot zover de rol van de geautoriseerde gebruikers als verwerkingsverantwoordelijken en de maatregelen die zij voorafgaand aan het gebruik van de blockchain zullen moeten treffen. In de volgende paragraaf wordt nader ingegaan op de vraag hoe de nodes van de niet-geautoriseerde gebruikers van de blockchain kunnen worden aangemerkt onder de AVG.

De (sub)verwerker

3.3.20 De verwerker is degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.[75] De verwerker ontleent zijn bevoegdheid om persoonsgegevens te verwerken aan de bevoegdheid van de verwerkingsverantwoordelijke die hem inschakelt. De bevoegdheden van een verwerker moeten zijn vastgelegd in een verwerkersovereenkomst.[76]

3.3.21 Kenmerkend voor een verwerker is dat de verwerker:

- een externe natuurlijke persoon, rechtspersoon, overheidsinstantie, dienst of orgaan is, die geen onderdeel vormt van de verwerkingsverantwoordelijke, en;
- persoonsgegevens voor de verwerkingsverantwoordelijke verwerkt – en dus niet voor zichzelf.[77]

3.3.22 Voor de kwalificatie van verwerker is bepalend of de partij aanwijzingen van de verwerkingsverantwoordelijke dient op te volgen met betrekking tot de verwerking van persoonsgegevens. Zo ja, dan is de partij een verwerker. Uitgangspunt is dat de verwerker niet mag afwijken van de afspraken die in de verwerkersovereenkomst met de verwerkingsverantwoordelijke zijn gemaakt. Dat betekent overigens niet dat de verwerker op detailniveau aanwijzingen van de verwerkingsverantwoordelijke moet ontvangen en volgen over de gegevensverwerking, maar (in ieder geval) wel voor zover het gaat om het doel van de verwerking en de wezenlijke aspecten van de middelen voor de verwerking.[78]

[75] Artikel 4, aanhef en onder 8, AVG.
[76] Artikel 28, derde lid, AVG.
[77] Op het moment dat een verwerker verwerkingen voor zichzelf (of in strijd met de instructies van de verwerkingsverantwoordelijke) verricht, en aldus feitelijk handelt als verwerkingsverantwoordelijke, zal de verwerker (voor dat deel) worden aangemerkt als verwerkingsverantwoordelijke.
[78] Vgl. Artikel 29-Werkgroep, 'Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker"', 16 februari 2010, p. 29.

3.3.23 De verwerker kan met voorafgaande toestemming van de verwerkingsverantwoordelijke een subverwerker inschakelen. Met de (sub)verwerker moet een (sub)verwerkersovereenkomst worden gesloten.[79]

3.3.24 Op het moment dat de verwerker een zelfstandige en bepalende rol krijgt bij het vaststellen van de doelen en/of de middelen van de verwerking, zal de verwerker niet langer als verwerker kwalificeren, maar als verwerkingsverantwoordelijke.[80] Een belangrijke consequentie daarvan is dat de verwerker niet langer zijn wettelijke grondslag voor het verwerken van de (gehashte) persoonsgegevens op de blockchain kan ontlenen aan de wettelijke grondslag van de verwerkingsverantwoordelijke die hem heeft ingeschakeld. Als verwerkingsverantwoordelijke dient hij immers een zelfstandige wettelijke grondslag te hebben voor het verwerken van de gehashte persoonsgegevens. Het probleem is dat een dergelijke wettelijke grondslag vaak zal ontbreken. In dat geval zal sprake zijn van een onrechtmatige verwerking, met onder meer als gevolg een risico op hoge boetes van de AP.

3.3.25 In een private permissioned blockchain zullen ook niet-geautoriseerde gebruikers gebruikmaken van de blockchain. Anders dan (de nodes van) de geautoriseerde gebruikers van de blockchain, hebben de niet-geautoriseerde gebruikers geen toegang tot (leesbare) persoonsgegevens in de blokken. Verdedigbaar is dat het verwerken van de (voor hen gehashte) persoonsgegevens op de blockchain - en het minen dat eventueel plaatsvindt via de node van de niet-geautoriseerde gebruiker[81] - in wezen plaatsvindt ten behoeve van het vergroten van – zo is althans de gedachte en dat wordt in dit rapport ook tot uitgangpunt genomen – de betrouwbaarheid en de veiligheid van de transactie. Doordat de niet-geautoriseerde gebruikers de gehashte persoonsgegevens ten behoeve van de geautoriseerde gebruikers verwerken, zou gesteld kunnen worden dat de niet-geautoriseerde gebruikers zijn aan te merken als verwerkers.

3.3.26 Hieronder volgt een nadere toelichting.

Zijn (de nodes van) de niet-geautoriseerde gebruikers van de blockchain aan te merken als verwerkers?

3.3.27 Er is discussie mogelijk over de vraag of (de nodes van) niet-geautoriseerde gebruikers – die als gezegd alleen gehashte persoonsgegevens zullen verwerken – handelen als (mede)verwerkingsverantwoordelijken of als verwerkers. Daarbij kunnen de volgende benaderingen worden onderscheiden:

[79] Zie randnr. 3.3.30 van dit rapport.
[80] Vgl. Artikel 29-Werkgroep, 'Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker"', 16 februari 2010, p. 29; Art. 29 Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), adopted on 22 November 2006
[81] Als zij een validating node hebben.

Benadering I - (de nodes van) niet-geautoriseerde gebruikers zijn (mede)verwerkingsverantwoordelijken.

Enerzijds zou betoogd kunnen worden dat de nodes van de niet-geautoriseerde gebruikers handelen als mede-verwerkingsverantwoordelijken. De nodes beschikken immers over een kopie van de blockchain en de (validating) nodes hebben een medebepalende rol bij het minen van nieuwe blokken.[82]

Benadering II - (de nodes van) niet-geautoriseerde gebruikers zijn verwerkers.

Anderzijds zou betoogd kunnen worden dat (de nodes van) niet-geautoriseerde gebruikers gehashte persoonsgegevens verwerken ten behoeve van de geautoriseerde gebruiker van de blockchain en aldus optreden als (sub)verwerkers.[83] Een belangrijk voordeel van deze benadering is, als gezegd, dat de nodes van niet-geautoriseerde gebruikers niet over een afzonderlijke wettelijke grondslag hoeven te beschikken om de persoonsgegevens te verwerken, maar zij de wettelijke grondslag kunnen overnemen van de verwerkingsverantwoordelijken voor wie zij verwerker zijn.

Benadering III – (de nodes) van niet-geutoriseerde gebruikers zijn verwerkingsverantwoordelijken, noch verwerkers

Tot slot is ook een derde benadering denkbaar, waarbij de niet-geautoriseerde gebruikers verwerkingsverantwoordelijken, noch verwerker zijn. Er zou dan betoogd moeten worden dat (de nodes van) niet-geautoriseerde gebruikers te vergelijken zijn met telecommunicatie- of elektronsiche postdiensten, die slechts berichten doorgeven ten behoeve van anderen. De (Europese) wetgever en de Europese toezichthouders beschouwen telecommunicatie- of elektronische postdiensten niet als verwerkingsverantwoordelijken of verwerkers ten aanzien van de (persoonsgegevens in de) inhoud van de berichten die zij doorgeven. Dergelijke diensten zijn slechts verwerkingsverantwoordelijke ten aanzien van de aanvullende gegevens die zij ten behoeve van het verzending van de berichten verwerken.[84] Vertaald naar de blockchain zou dit betekenen dat (i)

[82] De Franse privacy toezichthouder acht dat laatste echter onvoldoende voor de conclusie dat sprake is van verwerkingsverantwoordelijkheid. Zie CNIL, 'blockchain: Solutions for a responsible use of the blockchain in the context of personal data', p. 2 t/m 4.
[83] Als verwerker voor de geautoriseerde verwerkingsverantwoordelijken en als sub-verwerker voor de geautoriseerde verwerkers.
[84] Zie overweging 47 van de (vervallen) Privacyrichtlijn: "Overwegende dat, wanneer een bericht dat persoonsgegevens bevat, wordt verzonden via een telecommunicatie- of elektronische postdienst waarvan het enige doel is dit soort berichten door te geven, het de person is van wie het bericht uitgaat, en niet degene die de dienst aanbiedt, die normaliter zal worden beschouwd als verantwoordelijk voor de verwerking van de in het bericht vervatte persoonsgegevens; dat evenwel de personen die deze diensten aanbieden normaliter zullen worden beschouwd als verantwoordelijk voor de verwerking van de aanvullende persoonsgegevens die

niet-geautoriseerde gebruikers geen grondslag hoeven te hebben om de gehashte transacties te verwerken en (ii) evenmin verwerkersovereenkomsten hoeven te worden gesloten met de niet-geautoriseerde gebruikers van de blockchain. Aangezien het echter onzeker is of (nodes van) niet-geautoriseerde gebruikers inderdaad gelijk zouden kunnen worden gesteld aan telecom- en postdiensten, zal deze benadering in het verdere vervolg van dit rapport onbesproken worden gelaten.

3.3.28 Hoewel de AP of de gezamenlijke Europese privacy toezichthouders zich hierover nog niet hebben uitgelaten, lijkt de tweede opvatting goed verdedigbaar. De (nodes van de) niet-geautoriseerde gebruikers hebben slechts een beperkte rol bij het bepalen van het doel en de middelen van de verwerkingen van persoonsgegevens binnen de blockchain waartoe zij niet-geautoriseerd zijn. Zij hebben geen toegang tot de onderliggende persoonsgegevens, maar verwerken enkel de hash van de persoonsgegevens. De verwerkingsverantwoordelijken zijn gebaat bij de verwerking van de hash door de niet-geautoriseerde gebruikers. Doordat de informatie op de blockchain ook (gehasht) staat opgeslagen op de nodes van niet-geautoriseerde gebruikers, vergroot dat – zo is althans de gedachte en dat wordt in dit rapport ook tot uitgangspunt genomen – de veiligheid en betrouwbaarheid van de gegevens die via de blockchain worden uitgewisseld. De nodes van niet-geautoriseerde gebruikers dragen aldus bij aan een veiligere uitwisseling van persoonsgegevens tussen de geautoriseerde gebruikers en dat doen zij vóór (‘*ten behoeve van*’) die geautoriseerde gebruikers. Het gegeven dat de nodes van de niet-geautoriseerde gebruikers de integriteit van transacties tussen geautoriseerde gebruikers vergroot, vormt daarmee een aanwijzing dat de verwerking via de nodes van niet-geautoriseerde gebruikers *ten behoeve van* de geautoriseerde gebruikers plaatsvindt.

De invloed van het type node van de gebruiker
Een relevante vraag is of het type node van de gebruiker van invloed is op het kunnen aanmerken van een niet-geautoriseerde gebruiker als verwerker. Het onderscheid tussen een validating/full node en een participating/light node lijkt echter niet relevant, nu ook de participating node uiteindelijk de (veilige en betrouwbare) gegevensuitwisseling tussen geautoriseerde gebruikers faciliteert, reeds omdat ook zij over een kopie van de (voor hen (deels) gehashte) blockchain beschikken, hetgeen borgt dat de inhoud van de blockchain niet eenzijdig kan worden gewijzigd.

Aandachtspunt: Het beginsel van dataminimalisatie
Een aandachtspunt bij een groot aantal verwerkers die gebruikmaken van de blockchain is het beginsel van dataminimalisatie (nader uitgewerkt in deel V, randnummer 5.4.7 e.v. van dit rapport). Het beginsel van dataminimalisatie betekent dat de verwerking van persoonsgegevens beperkt moet zijn tot het

noodzakelijk zijn voor de werking van de dienst”. Zie daarnaast Artikel 29-Werkgroep, ‘Advies 1/2010 over de begrippen ‘voor de verwerking verantwoordelijke’ en ‘verwerker’, p. 11.

strikt noodzakelijke. Onderdeel van de noodzakelijkheid van de verwerking is dat de groep van personen en instanties die de persoonsgegevens op de blockchain verwerken, is beperkt tot het strikt noodzakelijke.

De inzet van een groot aantal verwerkers zou in strijd kunnen komen met het beginsel van dataminimalisatie. Op het moment dat het laten toetreden van (nog meer) niet-geautoriseerde gebruikers geen toegevoegde waarde (meer) heeft voor de veiligheid van de uitwisseling van persoonsgegevens, kan de vraag rijzen of de inzet van zoveel verwerkers nog wel noodzakelijk is. Of een dergelijke situatie daadwerkelijk leidt tot een schending van het beginsel van dataminimalisatie is momenteel niet duidelijk. Rechtspraak hierover ontbreekt en ook de Europese privacy toezichthouders hebben zich hier nog niet over uitgelaten.

Om het risico op een schending van het beginsel van dataminimalisatie te verkleinen, doen gebruikers er verstandig aan om bij het ontwerp van de blockchain ontwerpkeuzes te maken die borgen dat het aantal niet-geautoriseerde gebruikers beperkt blijft tot het strikt noodzakelijke. Zo is het raadzaam om per patiënt / verzekerde een persoonlijke blockchain te hanteren, om zodoende de groep gebruikers van de blockchain (en het aantal niet-geautoriseerde gebruikers) te beperken tot de gebruikers die in een relatie staan tot de betreffende patiënt/verzekerde.

Het sluiten van een verwerkersovereenkomst

3.3.29 Voor zover de niet-geautoriseerde gebruikers inderdaad optreden als (sub)verwerkers voor de geautoriseerde gebruikers, zal een (sub)verwerkersovereenkomst moeten worden gesloten. Deze verwerkersovereenkomst dient te worden gesloten vóórdat de node van de niet-geautoriseerde gebruiker wordt toegelaten tot de blockchain. Het zou aanbeveling verdienen om gezamenlijk tot een standaardverwerkersovereenkomst te komen die door alle gebruikers ondertekend wordt.[85] Daarbij is dan de gedachte dat de gebruikers – voor zover zij (ten aanzien van bepaalde transacties) niet geautoriseerd zullen zijn – als (sub)verwerker optreden voor de wel-geautoriseerde gebruikers. De verwerkingsverantwoordelijken zullen (mede in de onderlinge regeling) een toetredingsprocedure moeten vormgeven die borgt dat iedere toetredende gebruiker de standaardverwerkersovereenkomst ondertekent (voor zover die gebruiker zal optreden als niet-geautoriseerde gebruiker).

3.3.30 In de verwerkersovereenkomst dient tenminste te zijn geregeld dat:

[85] Daarmee wordt voorkomen dat er verschillende en mogelijk zelfs tegenstrijdige afspraken ontstaan tussen de verwerkers die gebruikmaken van de blockchain.

(i) de geautoriseerde verwerkersverantwoordelijken die individuele zeggenschap hebben over de gehashte persoonsgegevens die de niet-geautoriseerde gebruikers verwerken, en;

(ii) (de nodes van) de niet-geautoriseerde gebruikers de gehashte persoonsgegevens voor geen enkel andere doel zullen verwerken dan om de geautoriseerde verwerkingsverantwoordelijken en verwerkers in staat te stellen persoonsgegevens via de blockchain te verwerken, inclusief wat dat precies inhoudt (zoals ten aanzien van het punt welk consensusprotocol in acht moet worden genomen, als sprake is van een niet-geautoriseerde gebruiker met een validating node).

3.3.31 De verwerkersovereenkomst dient verder in ieder geval de volgende onderdelen te bevatten:

- een garantie van de verwerker met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van de AVG voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd (artikel 28, eerste lid, AVG);
- een beschrijving van het onderwerp, de duur, de aard en het doel van de verwerkingen die plaatsvinden binnen de blockchain (artikel 28, derde lid, aanhef AVG);
- een beschrijving van het soort persoonsgegevens dat binnen de blockchain verwerkt wordt (artikel 28, derde lid, aanhef AVG);
- een beschrijving van de categorieën van betrokkenen waarop de persoonsgegevens die verwerkt worden zien (artikel 28, derde lid, aanhef AVG);
- de verplichting dat de verwerker de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, tenzij een unierechtelijke of lidstaatrechtelijke bepaling tot verwerking verplicht, in welk geval de verwerker de verwerkingsverantwoordelijke voorafgaand aan de verwerking van dat wettelijke voorschrift in kennis stelt (tenzij die wetgeving die kennisgeving om gewichtige redenen van algemeen belang verbiedt) (artikel 28, derde lid, aanhef en onder a AVG);
- de verplichting dat de verwerker waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen (oftewel de personen die namens de verwerker kunnen inloggen op de node) zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting tot vertrouwelijkheid zijn gebonden (artikel 28, derde lid, aanhef en onder b AVG);

- de verplichting dat de verwerker passende technische en organisatorische beveiligingsmaatregelen treft (artikel 28, derde lid, aanhef en onder c jo. artikel 32 AVG);
- de verplichting dat de verwerker zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke geen subverwerker mag inschakelen. En de verplichting dat, in het geval van algemene schriftelijke toestemming, de verwerker de verwerkingsverantwoordelijke inlicht over beoogde veranderingen inzake de toevoeging of vervanging van subverwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid heeft om bezwaar te maken (artikel 28, derde lid, aanhef en onder d jo. artikel 28, tweede lid, AVG);
- de verplichting de verwerker met subverwerkers een rechtsgeldige verwerkersovereenkomst sluit met daarin dezelfde verplichtingen als waaraan de verwerker jegens de verwerkingsverantwoordelijke is gebonden (artikel 28, derde lid, aanhef en onder d jo. artikel 28, vierde lid, AVG).
- de verplichting dat de verwerker, rekening houdend met de aard van de verwerking, de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verleent bij het vervullen van diens plicht om verzoeken tot uitoefening van de in hoofdstuk III van de AVG vastgestelde rechten van de betrokkene te beantwoorden (artikel 28, derde lid, aanhef en onder e, AVG;
- de verplichting dat de verwerker de verwerkingsverantwoordelijke bijstand verleent bij het voldoen aan zijn verplichting om uiterlijk binnen 72 uur na ontdekking een datalek te melden bij de Autoriteit Persoonsgegevens op de wijze als beschreven in artikel 33 AVG en om een datalek te melden aan de betrokkene overeenkomstig op de wijze als beschreven in artikel 34 AVG (artikel 28, derde lid, aanhef en onder f jo. artikel 33 en 34 AVG);
- de verplichting dat de verwerker de verwerkingsverantwoordelijke bijstand verleent bij het uitvoeren van de gegevensbeschermingseffectbeoordeling als bedoeld in artikel 35 AVG (artikel 28, derde lid, aanhef en onder f jo. artikel 35 AVG);
- de verplichting dat de verwerker de verwerkingsverantwoordelijke bijstand verleent bij het uitvoeren van een voorafgaande raadpleging als bedoeld in artikel 36 AVG (artikel 28, derde lid, aanhef en onder f jo. artikel 36 AVG);
- de verplichting dat de verwerker, afhankelijk van de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wist of terugbezorgt en bestaande kopieën verwijdert, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht (artikel 28, derde lid, aanhef en onder g AVG);
- de verplichting dat de verwerker om de verwerkingsverantwoordelijke alle informatie ter beschikking te stellen die nodig is om de nakoming van de in

artikel 28 AVG neergelegde verplichtingen aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke of een door de verwerkingsverantwoordelijke gemachtigde controleur mogelijk te maken en eraan bij te dragen (artikel 28, derde lid, aanhef en onder h AVG);

- de verplichting dat de verwerker en eenieder die onder diens gezag handelt de persoonsgegevens uitsluitend in opdracht van de verwerkingsverantwoordelijke verwerkt (artikel 29 AVG).

3.4 Aandachtspunt bij het toebedelen van de rollen van de gebruikers: geen doorkruising van de wettelijk vastgestelde bevoegdheidsverdelingen

3.4.1 Een aandachtspunt bij het toebedelen van de rollen van de gebruikers van de blockchain, zijn de wettelijk vastgestelde bevoegdheidsverdelingen. Het is mogelijk dat een bijzondere (zorgspecifieke) wet expliciet instanties of personen aanwijst als verwerkingsverantwoordelijke of verwerker. Het gebruik van de blockchain mag er niet toe leiden dat een instantie die wettelijk is aangewezen als verwerkingsverantwoordelijke of verwerker na ingebruikname van de blockchain een rol krijgt toebedeeld (geautoriseerde of niet-geautoriseerde gebruiker) die niet past bij de wettelijk vastgestelde rol. Een op grond van de Jeugdwet aangewezen verwerkingsverantwoordelijke zal aldus als geautoriseerde verwerkingsverantwoordelijke moeten optreden voor zover het gaat om verwerkingen van persoonsgegevens ten aanzien waarvan die partij in de Jeugdwet is aangewezen als verwerkingsverantwoordelijke.

> ***Praktijkvoorbeeld***
> *Een voorbeeld is artikel 8.4.2 van de Jeugdwet waarin de Sociale verzekeringsbank (SVB) wordt aangewezen als verwerkingsverantwoordelijke voor het verwerken van persoonsgegevens van jeugdigen en hun ouders, voor zover dat noodzakelijk is voor – kort gezegd – de budgetbeheertaken van de SVB. De SVB zal bij toetreden van een blockchain gericht op (onder meer) het budgetbeheer, ten aanzien van die budgetbeheer-taken in ieder geval moeten worden toegelaten als geautoriseerde verwerkingsverantwoordelijke. Een door de Jeugdwet aangewezen verwerker zou moeten worden aangemerkt als:*
> - *geautoriseerde verwerker van de persoonsgegevens in de transacties die hij in opdracht en ten behoeve van de verwerkingsverantwoordelijke mag verwerken, en als;*
> - *niet-geautoriseerde gebruiker ten aanzien van de gehashte persoonsgegevens in de overige transacties.*

3.4.2 Het verdient aanbeveling om in de onderlinge regeling tussen de verwerkingsverantwoordelijke gebruikers van de blockchain te komen tot een controleproces waarmee wordt gewaarborgd dat wettelijk aangewezen partijen bij

toetreding tot de blockchain rollen krijgen die in overeenstemming zijn met de hun wettelijk toebedeelde taken.

3.5 De bouwer(s) van de blockchain: verwerkingsverantwoordelijke, verwerker of geen van beiden?

3.5.1 Een veel voorkomende vraag bij de kwalificatie van gebruikers als verwerkingsverantwoordelijke of verwerker, is in hoeverre de betrokkenheid van een partij bij de bouw van de blockchain relevant is voor het aanmerken van die partij als verwerkingsverantwoordelijke. Kernvraag is of de betrokkenheid van een partij bij het ontwerp en de bouw van de blockchain ertoe leidt dat die partij (mede) het doel en de middelen van de verwerking binnen de blockchain heeft bepaald en reeds daardoor zou moeten worden aangemerkt als verwerkingsverantwoordelijke.

3.5.2 Het is aannemelijk dat de betrokkenheid bij de bouw van een blockchain niet zonder meer ertoe leidt dat een partij (gezamenlijke) verwerkingsverantwoordelijke wordt voor de verwerkingen die plaatsvinden binnen de blockchain. Of dat het geval is, is geheel afhankelijk van de rol die de betreffende partij zal spelen *nadat* de blockchain in gebruik wordt genomen. De volgende situaties kunnen worden onderscheiden.

> ***Situatie I – De partij is betrokken geweest bij de bouw van de blockchain, maar heeft geen rol bij het verwerken van persoonsgegevens na ingebruikname van de blockchain.***
>
> *In deze situatie is de bouwer weliswaar betrokken geweest bij de bouw van de blockchain, maar vervult de bouwer geen rol bij het verwerken van persoonsgegevens nadat de blockchain in gebruik is genomen. Hierbij kan worden gedacht aan een blockchain die in opdracht van bijv. een ziekenhuis is ontworpen en vervolgens is overgedragen aan de opdrachtgever (het ziekenhuis). De blockchain is als het ware volledig overgedragen. Doordat de bouwer geen persoonsgegevens verwerkt, zal de bouwer noch verwerker, noch verwerkingsverantwoordelijke zijn.*
>
> *Daarbij is van belang dat het enkele feit dat hij bij de bouw van de blockchain ontwerpkeuzes heeft gemaakt en de facto de standaard heeft bepaald, op zichzelf niet maakt dat hij daardoor als verwerkingsverantwoordelijke moet worden aangemerkt. Het zijn immers nog steeds de verwerkingsverantwoordelijke gebruikers van de blockchain die bepalen dat zij gebruik willen maken van de blockchain en voor welke doelen.*

> ***Situatie II – De bouwer is betrokken geweest bij de bouw van de blockchain, en voert na ingebruikname van de blockchain taken uit waarbij persoonsgegevens worden verwerkt.***

Doordat de bouwer in het kader van de aan hem opgedragen (beheer)taken[86] persoonsgegevens verwerkt ten behoeve van de verwerkingsverantwoordelijke gebruikers van de blockchain, zal de betreffende partij optreden als verwerker.

De omstandigheid dat de bouwer het ontwerp van de blockchain zelfstandig heeft vormgegeven, en aldus feitelijk de middelen van de verwerking heeft bepaald, maakt de bouwer naar alle waarschijnlijkheid nog geen verwerkingsverantwoordelijke. De Artikel 29-Werkgroep acht toelaatbaar dat een verwerker een 'take it or leave it' aanbod doet aan de verwerkingsverantwoordelijke(n) die van zijn systeem gebruik wil(len) maken. De verwerker mag daarbij gebruik maken van een (door hem gebruikte) standaard verwerkersovereenkomst waarin is vastgesteld op welke wijze hij zijn diensten inricht en welke hardware en software hiervoor zal worden gebruikt.[87] Ook de omstandigheid dat de verwerker een grotere machtspositie heeft dan de (gezamenlijke) verwerkingsverantwoordelijke(n), maakt volgens de Artikel 29-Werkgroep niet dat de verwerker daarom kwalificeert als verwerkingsverantwoordelijke.[88]

Bovengenoemde uitgangspunten zullen – zo is de verwachting – ook gelden voor blockchains. Hieruit lijkt te volgen dat een bouwer van een blockchain door middel van een 'take it or leave it' aanbod een blockchain kan aanbieden en voor de verwerkingsverantwoordelijke kan beheren, zonder dat hij daarmee kwalificeert als verwerkingsverantwoordelijke. Belangrijke voorwaarde daarbij is dat het 'take it or leave it' aanbod geen afbreuk doet aan de vrijheid van de gezamenlijke verwerkingsverantwoordelijken om (na ingebruikname van de blockchain) het doel van de verwerking binnen de blockchain te bepalen en te bepalen welke gegevens worden verwerkt en hoe lang deze worden bewaard.

Situatie III – De partij is betrokken geweest bij de bouw van de blockchain, gebruikt de blockchain vervolgens als (niet-)geautoriseerde gebruiker, maar voert geen beheertaken uit

In het geval de bouwer betrokken is geweest bij de bouw van de blockchain en die partij de blockchain vervolgens ook gaat gebruiken als geautoriseerde respectievelijk niet-geautoriseerde gebruiker, dan zal de partij naar alle waarschijnlijkheid optreden als verwerkingsverantwoordelijke voor zover hij geautoriseerd is, en als verwerker voor zover dat niet het geval is.[89] De betrokkenheid van die partij bij de bouw van de blockchain zal daar geen verandering in brengen.

Situatie VI – De partij is betrokken geweest bij de bouw van de blockchain, gebruikt de blockchain vervolgens als (niet-) geautoriseerde gebruiker en voert wel beheertaken uit

[86] Bijvoorbeeld het uitvoeren van de beveiliging van de blockchain en het beheren van de server waar de node op draait
[87] Een goed voorbeeld hiervan is cloudopslagproviders, die vrijwel standaard gebruik maken van 'take it or leave it' verwerkersovereenkomsten.
[88] Zie Artikel 29-Werkgroep, 'Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker'', p. 30.
[89] Zie voorgaande paragrafen.

In deze variant heeft de betreffende bouwer een dubbelrol. Voor zover hij optreedt als geautoriseerde gebruiker zal hij naar alle waarschijnlijkheid verwerkingsverantwoordelijke zijn en voor zover hij optreedt als de niet-geautoriseerde gebruiker zal hij handelen als verwerker.[90] Hij zal ook als verwerker optreden uit hoofde van zijn beheertaken. De te sluiten verwerkersovereenkomst(en) zal (zullen) aan die situatie recht moeten doen.

3.6 Conclusie

3.6.1 Geautoriseerde gebruikers die persoonsgegevens op de blockchain plaatsen, en geautoriseerde gebruikers die de transactie ontvangen en bevoegd zijn om de inhoud van het blok te raadplegen, wijzigen en/of verwijderen, zijn aan te merken als (gezamenlijke) verwerkingsverantwoordelijken voor die persoonsgegevens, tenzij zij zouden kwalificeren als geautoriseerde verwerkers.

3.6.2 De gezamenlijke verwerkingsverantwoordelijken van de blockchain zijn op grond van artikel 26, eerste lid, AVG verplicht tot het vaststellen van een onderlinge regeling waarin hun respectieve verplichtingen ten aanzien van de verwerking op een transparante wijze worden vastgelegd.

3.6.3 Bij een groot aantal gezamenlijke verwerkingsverantwoordelijken kan het volgens de Europese privacy toezichthouders verplicht zijn om één super user aan te wijzen, die een deel van de taken van de gezamenlijke verwerkingsverantwoordelijken uitvoert.

3.6.4 Het vaststellen van een onderlinge regeling en het aanwijzen van een super user vereist dat gebruikers met elkaar in overleg treden en heldere afspraken maken. Dit lijkt bij een public, permissionless blockchain een vrijwel onmogelijke exercitie. In dit licht bezien, verdient het dan ook de voorkeur om óók voor blockchains in de zorg waarin persoonsgegevens worden verwerkt te kiezen voor een private, permissioned blockchain, zodat daadwerkelijk uitvoering kan worden gegeven aan de afspraken die zijn opgenomen in de onderlinge regeling. Een private, permissioned blockchain is verder onder meer noodzakelijk om aan de super user (voor zover deze is aangesteld) bevoegdheden toe te kunnen bedelen. In het verdere vervolg van dit rapport wordt er dan ook vanuit gegaan dat sprake is van een private permissioned blockchain.

3.6.5 De geautoriseerde verwerkingsverantwoordelijken moeten worden onderscheiden van de geautoriseerde verwerkers. De geautoriseerde verwerkers zijn de externe partijen die in opdracht van een of meer van de geautoriseerde verwerkingsverantwoordelijken deelnemen aan de blockchain en ten behoeve van hen persoonsgegevens verwerken op de blockchain. Deze situatie zal zich (bijvoorbeeld) voordoen indien een partij buiten de blockchain om al verwerker was voor een partij (bijvoorbeeld een ziekenhuis) en de verwerker zijn verwerkerswerkzaamheden voortzet met

[90] Zie voorgaande paragrafen.

gebruikmaking van de blockchain. In dat geval zal die partij vermoedelijk verwerker blijven (voor het ziekenhuis).

3.6.6 Hoewel hierover discussie mogelijk is, is het verdedigbaar om niet-geautoriseerde gebruikers ten aanzien van de persoonsgegevens in de transacties waarvoor zij niet zijn geautoriseerd aan te merken als (sub)verwerkers, nu zij slechts in beperkte mate het doel en de middelen van die persoonsgegevens bepalen en – zo is althans de gedachte en dat wordt in dit rapport ook tot uitgangspunt genomen – deze grotendeels ten behoeve van de veilige en betrouwbare uitwisseling tussen geautoriseerde gebruikers verwerken.

3.6.7 Voor zover de niet-geautoriseerde gebruikers inderdaad optreden als (sub)verwerkers voor de geautoriseerde gebruikers, zal een (sub)verwerkersovereenkomst moeten worden gesloten. Deze verwerkersovereenkomst dient te worden gesloten, vóórdat de node van de niet-geautoriseerde gebruiker wordt toegelaten tot de blockchain. De verwerkingsverantwoordelijken zullen (mede in de onderlinge regeling) een toetredingsprocedure moeten vormgeven die borgt dat iedere toetredende gebruiker de standaardverwerkersovereenkomst ondertekent (voor zover die gebruiker zal optreden als niet-geautoriseerde gebruiker). Het zou aanbeveling verdienen om gezamenlijk tot een standaardverwerkersovereenkomst te komen die door alle gebruikers ondertekend wordt. Daarbij is dan de gedachte dat de gebruikers – voor zover zij (ten aan zien van bepaalde transacties) niet geautoriseerd zullen zijn – als (sub)verwerker optreden voor de wel-geautoriseerde gebruikers.

3.6.8 In de verwerkersovereenkomst dient ten minste te zijn geregeld dat (i) de geautoriseerde verwerkingsverantwoordelijken de zeggenschap hebben over de gehashte persoonsgegevens die de niet-geautoriseerde gebruikers verwerken en (ii) de nodes van de niet-geautoriseerde gebruikers de gehashte persoonsgegevens voor geen enkel andere doel zullen verwerken, dan om de geautoriseerde verwerkingsverantwoordelijken en verwerkers in staat te stellen persoonsgegevens via de blockchain te verwerken, inclusief wat dat precies inhoudt (zoals ten aanzien van het punt welk consensusprotocol in acht moet worden genomen, als sprake is van een niet-geautoriseerde gebruiker met een validating node). De verwerkersovereenkomst dient verder in ieder geval een aantal andere onderdelen te bevatten zoals beschreven in de artikelen 28 en 29 van de AVG (zie randnrs. 3.3.30 e.v. van dit rapport).

3.6.9 Het komt geregeld voor dat een bijzondere (zorgspecifieke) wet instanties of personen aanwijst als verwerkingsverantwoordelijke of verwerker. Het gebruik van de blockchain mag er niet toe leiden dat een instantie die wettelijk is aangewezen als verwerkingsverantwoordelijke of verwerker na ingebruikname van de blockchain een rol krijgt (geautoriseerde of niet-geautoriseerde gebruiker) die niet past bij die wettelijk vastgestelde rol.

3.6.10 Afhankelijk van de rol die de bouwer van (delen van) de blockchain vervult, zal de bouwer kwalificeren als verwerkingsverantwoordelijke, verwerker of als niets.

4 WETTELIJKE GRONDSLAGEN VOOR HET VERWERKEN VAN PERSOONSGEGEVENS

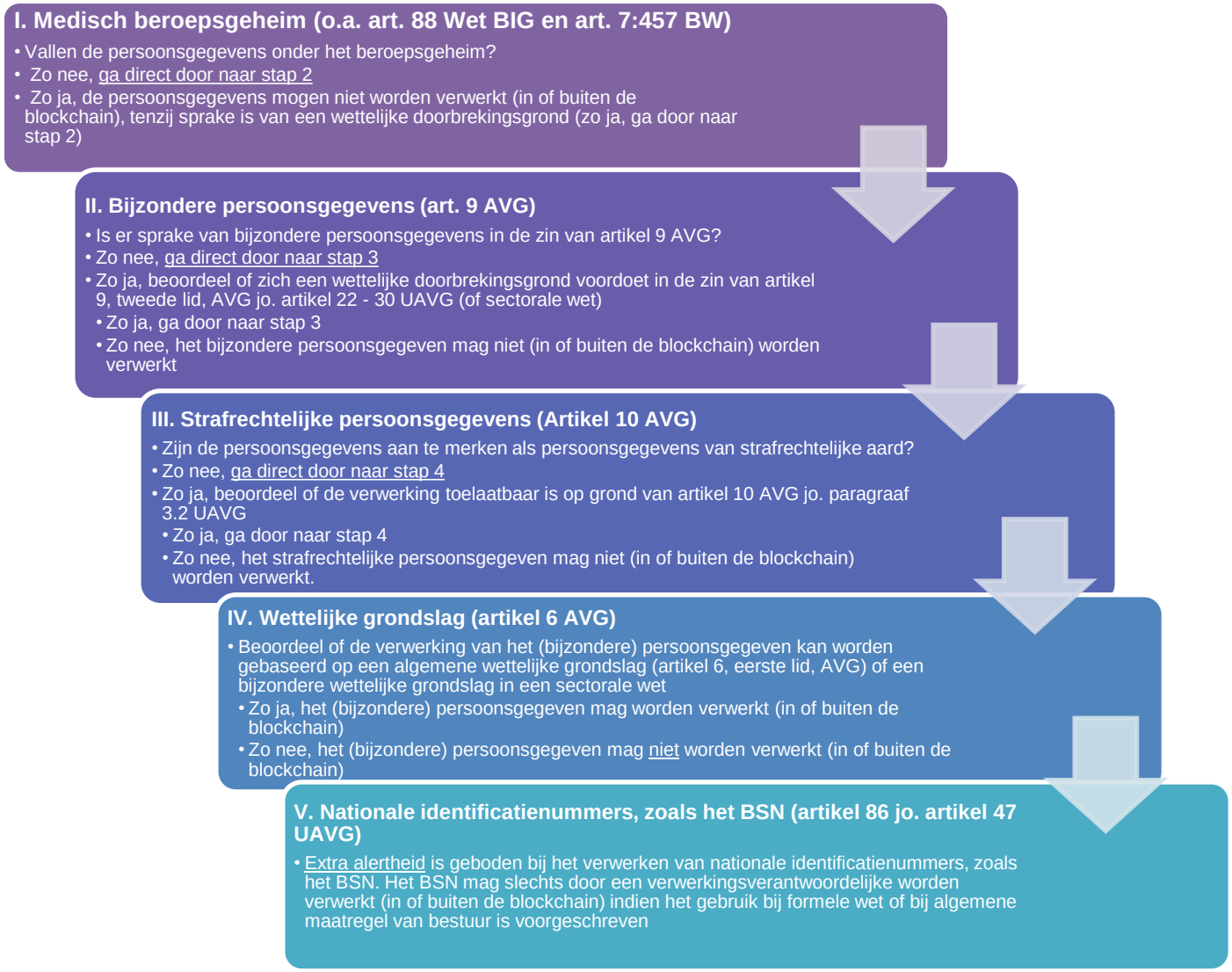
4.1 Inleiding

4.1.1 Zodra is vastgesteld dat binnen de blockchain persoonsgegevens worden verwerkt (deel II van dit rapport) en de geautoriseerde gebruikers zijn geïdentificeerd (deel III van dit rapport), dient per verwerkingsverantwoordelijke gebruiker te worden vastgesteld of en zo ja in hoeverre een wettelijke grondslag bestaat voor het verwerken van (bijzondere) persoonsgegevens in de transacties. Om dit te kunnen vaststellen, moeten de volgende deelvragen worden beantwoord:

1. Vallen de persoonsgegevens onder een (medisch) beroepsgeheim en zo ja, doet zich een wettelijke grond op basis waarvan die deze geheimhoudingsplicht zou kunnen worden doorbroken?
2. Voor zover er sprake is van het verwerken van bijzondere persoonsgegevens (bijv. medische gegevens, genetische gegevens of biometrische gegevens), doet zich voor de verwerking daarvan een wettelijke doorbrekingsgrond voor?
3. Voor zover er persoonsgegevens van strafrechtelijke aard worden verwerkt (bijv. in aanvulling op medische gegevens), is daar een wettelijke grondslag voor?
4. Kan de verwerking van de (bijzondere) persoonsgegevens op de blockchain worden gebaseerd op een (algemene of bijzondere) wettelijke grondslag?[91]
5. Worden er op de blockchain nationale identificatienummers (zoals het burgerservicenummer) verwerkt? Zo ja, is het gebruik daarvan voorgeschreven bij een formele wet of bij algemene maatregel van bestuur?

4.1.2 De hierboven beschreven stappen kunnen schematisch als volgt worden samengevat.

[91] Vgl. voor de voorgaande volgorde *Kamerstukken II* 2017-2018, 34814, nr. 3, p. 30. "Het kan zich voordoen dat in een geval waarin op grond van artikel 30 het verbod om medische gegevens te verwerken niet van toepassing is, het medische beroepsgeheim toch aan de gegevensverwerking in de weg kan staan. Dit betekent dat verstrekking van gezondheidsgegevens eerst moet worden getoetst aan de regels voor doorbreking van het medisch beroepsgeheim. Pas wanneer verstrekking van gezondheidsgegevens niet in strijd is met het medisch beroepsgeheim, komt men toe aan toetsing aan het onderhavige artikel. Als daaraan is voldaan (een beroep op de uitzondering op het algemene verbod van artikel 9, eerste lid, van de verordening is mogelijk), dan moet nog een grondslag aanwezig zijn in de zin van artikel 6 van de verordening."



4.2 Toepasselijkheid van dit deel

4.2.1 Dit deel is van toepassing op zowel:

(i) blockchains waarbij gebruik wordt gemaakt van pointers die zelf geen persoonsgegevens bevatten (en waarbij er aldus *geen* persoonsgegevens op de blockchain worden geplaatst), als op;

(ii) blockchains waarbij (gehashte) persoonsgegevens op de blockchain worden geplaatst.

4.2.2 In beide gevallen dient de verwerkingsverantwoordelijke aan de hand van het hierboven beschreven stappenplan vast te stellen of de verwerking van persoonsgegevens (in of buiten de blockchain) mag plaatsvinden.

4.3 Nadere bespreking doorbrekingsgronden en wettelijke grondslagen

4.3.1 Hieronder volgt een nadere toelichting op de afzonderlijke stappen.

I. Het medische beroepsgeheim

4.3.2 Het is bij blockchains in de zorg allereerst van belang dat wordt vastgesteld of de verwerkingsverantwoordelijke gebruikers van de blockchain zijn gebonden aan een (medisch) beroepsgeheim. Is dat het geval, dan zal de verwerkingsverantwoordelijke gebruiker geen persoonsgegevens van de patiënt[92] kenbaar mogen maken aan derden, tenzij deze verwerking kan worden gebaseerd op een wettelijke doorbrekingsgrond. Hieronder volgt een nadere toelichting.

4.3.3 Zorgverleners en zorgaanbieders[93] zijn gebonden aan de geheimhoudingsplicht van artikel 88 Wet BIG en artikel 7:457 BW (hierna: 'het (medisch) beroepsgeheim').

> Vgl. Artikel 88 Wet BIG:
>
> 'Een ieder is verplicht geheimhouding in acht te nemen ten opzichte van al datgene wat hem bij het uitoefenen van zijn beroep op het gebied van de individuele gezondheidszorg als geheim is toevertrouwd, of wat daarbij als geheim te zijner kennis is gekomen en waarvan hij het vertrouwelijke karakter moest begrijpen.'
>
> Vgl. Artikel 7:457 BW:
>
> '(…) de hulpverlener (draagt) zorg dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden (…) worden verstrekt dan met toestemming van de patiënt.'

4.3.4 Onder de geheimhoudingplicht van artikel 88 Wet BIG vallen alle BIG-geregistreerde zorgverleners (waaronder artsen, verpleegkundigen, GGZ-psychologen, tandartsen en fysiotherapeuten). Het medische beroepsgeheim in artikel 7:457 BW is ruimer dan het beroepsgeheim in de Wet BIG, aangezien ook niet-geregistreerde zorgverleners onder de reikwijdte van deze bepaling vallen.[94] De strekking van beide geheimhoudingsbepalingen is hetzelfde: zorgverleners zijn gebonden aan hun

---

[92] In artikel 7:457 BW wordt degene die zorg ontvangt, aangeduid als 'patiënt'. Degene die jeugdhulp ontvangt wordt onder de Jw aangeduid als 'jeugdige'. De Wmo 2015 hanteert de term 'cliënt'. De Zvw en de Wlz spreken van 'verzekerde'. Voor zover het gaat om de verwerking van persoonsgegevens van deze personen, wordt op grond van de AVG gesproken van 'betrokkene'.

[93] In artikel 7:457 BW wordt gesproken van 'hulpverlener'. In de praktijk wordt ook wel gesproken van zorgverleners en zorgaanbieders. In het verdere vervolg van dit rapport zal steeds worden gesproken van 'zorgverleners'.

[94] Een zorgverlener kan zowel een natuurlijke persoon als een rechtspersoon zijn die een geneeskundig beroep of bedrijf uitoefent. Voorbeelden van natuurlijke personen die een geneeskundig beroep uitoefenen zijn een arts, tandarts, verloskundige, psychotherapeut en paramedicus. Voorbeelden van een rechtspersoon die een geneeskundig bedrijf uitoefent zijn ziekenhuizen, verpleeghuizen of andere zorginstellingen.

beroepsgeheim. Slechts met toestemming van de patiënt mag de informatie over de patiënt aan een ander kenbaar worden gemaakt.

4.3.5 Als 'een ander' wordt, voor zover van belang, niet gezien degene die rechtstreeks betrokken is bij de verlening van de uitvoering van de behandelingsovereenkomst en degene die optreedt als vervanger van de (jeugd)hulpverlener, voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden (artikel 7:457, tweede lid, BW).[95] Het dient hierbij te gaan om andere zorgverleners die ingeschakeld zijn en daadwerkelijk werkzaamheden verrichten bij de verlening van de specifieke hulp aan de patiënt. Wanneer bijvoorbeeld aan één patiënt tegelijkertijd drie vormen van zorg worden verleend, zal in dat geval in beginsel sprake zijn van drie zorgverleners met elk hun eigen expertise en hulpverleningstraject. Elk van die zorgverleners is zelf gehouden een dossier in te richten, van een gezamenlijk dossier kan geen sprake zijn. Zij dienen er ieder voor zich voor te zorgen dat geen gegevens uit het dossier worden verstrekt aan anderen. De ene zorgverlener mag dus geen gegevens uit het dossier verstrekken aan een van de andere twee zorgverleners. Die zijn immers niet rechtstreeks betrokken bij de verlening van die specifieke zorg.

4.3.6 Aan een collega – BIG-geregistreerd of niet – waarmee de zorgverlener in de uitvoering van die specifieke zorg samenwerkt in het kader van dezelfde behandelrelatie, kan hij wél gegevens verstrekken over de betrokken patiënt of inzage geven in het dossier. Ook dan geldt echter nog wel de regel dat dit slechts is toegestaan voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden. Gedacht kan worden aan de situatie dat een collega-vakgenoot met het oog op de goede verlening van de specifieke geneeskundige behandeling geraadpleegd wordt (voor zover dat niet anoniem *kan).*

4.3.7 Het beroepsgeheim strekt zich eveneens uit tot de medewerkers van de zorgverlener (assistenten en secretaresses).[96] Voor hen geldt een afgeleid beroepsgeheim. Het beroepsgeheim van de zorgverlener is niet beperkt tot medische informatie, maar ziet op alle informatie die de patiënt aan de zorgverlener heeft toevertrouwd. Het kan aldus gaan om medische gegevens, maar ook over niet-medische gegevens, waaronder privéomstandigheden (bijv. de gezinssituatie). Ook het enkele gegeven dat een patiënt een afspraak heeft of een behandeling heeft ondergaan valt onder het beroepsgeheim.

[95] Vgl. artikel 9, aanhef en onder h, AVG jo. artikel 30, tweede lid, aanhef en onder a, UAVG, dat bepaalt dat het verbod om persoonsgegevens betreffende iemands gezondheid te verwerken niet van toepassing is indien de verwerking geschiedt door hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene, dan wel het beheer van de betreffende instelling of beroepspraktijk noodzakelijk is.
[96] HR 30 juni 2017, ECLI:NL:HR:2017:1205.

Aanvullende geheimhoudingsbepaling Jeugdwet (artikel 7.3.11 Jw)
De Jeugdwet kent een (aanvullende) geheimhoudingsbepaling die zich specifiek richt op jeugdhulpverleners.[97] *De (jeugd)hulpverlener mag slechts aan een ander inlichtingen over de jeugdige geven en inzage in of afschrift van het betreffende dossier verstrekken als de jeugdige*[98] *daar toestemming voor verleent aan de (jeugd)hulpverlener (art. 7.3.11, eerste lid, Jw).*[99] *Artikel 7.3.11 Jw is een soortgelijke bepaling als artikel 7:457 BW, maar is specifiek toegespitst op de jeugdhulpverlener/jeugdige.*

Doorbreking van het beroepsgeheim

4.3.8 Het beroepsgeheim en de daaruit voortvloeiende geheimhoudingsverplichting kan in bepaalde gevallen doorbroken worden. De volgende doorbrekingsgronden kunnen worden onderscheiden:

a) Uitdrukkelijke toestemming van de patiënt;
b) Wettelijke verplichting of wettelijk recht;
c) Conflict van plichten.[100]

Ad (a) Uitdrukkelijke toestemming van de patiënt

4.3.9 Het beroepsgeheim van de zorgverlener vervalt indien de patiënt heeft ingestemd met doorbreking daarvan. Deze toestemming dient dan wel uitdrukkelijk te zijn gegeven. De patiënt dient expliciete, gerichte toestemming te geven alvorens gegevens mogen worden verstrekt. Dit betekent dat de patiënt moet weten met welk doel welke gegevens aan wie worden verstrekt. In de wet is niet voorgeschreven dat de toestemming schriftelijk[101] moet worden gegeven, maar dit verdient vanuit privacyrechtelijk perspectief wel de voorkeur. Vaak wordt daarbij gebruik gemaakt van schriftelijke of elektronische toestemmingsformulieren. Toestemmingsformulieren met een te brede of algemene toestemmingsvraag zijn doorgaans onvoldoende basis voor het verstrekken van specifieke, privacygevoelige gegevens en voor doorbreking van de geheimhoudingsplicht.[102]

---

[97] Artikel 7.3.11, eerste lid, Jeugdwet: "Onverminderd artikel 7.3.2, derde lid, tweede volzin, draagt de jeugdhulpverlener zorg, dat aan anderen dan de betrokkene geen inlichtingen over de betrokkene dan wel inzage in of afschrift van het dossier worden verstrekt dan met toestemming van de betrokkene. Indien verstrekking plaatsvindt, geschiedt deze slechts voor zover daardoor de persoonlijke levenssfeer van een ander niet wordt geschaad. De verstrekking geschiedt zonder inachtneming van beperkingen, indien het bij of krachtens de wet bepaalde daartoe verplicht."
[98] In bepaalde gevallen is de toestemming van bijvoorbeeld de met het gezag belaste ouders vereist. Zie artikel 7.3.15 Jw / 7:465 BW.
[99] Indien verstrekking plaatsvindt, mogen alleen gegevens worden verstrekt voor zover daardoor de persoonlijke levenssfeer van een ander niet wordt geschaad.
[100] Zowel het civiele recht als het stafrecht kennen eigen aanvullende doorbrekingsgronden. Het civiele recht kent de aanvullende doorbrekingsgrond 'zwaarwegend algemeen belang' (zie bijv. HR 20 april 2001, ECLI:NL:HR:2001:AB1201). Ook het strafrecht kent een aanvullende doorbrekingsgrond. Een zorgverlener kan in 'zeer uitzonderlijke omstandigheden' *geen* beroep doen op het verschoningsrecht tegenover de rechter, politie of justitie (zie HR 28 februari 2012, NJ 2012, 537).
[101] Onder schriftelijk vastleggen valt onder meer het elektronisch vragen en vastleggen van de toestemming van de patiënt.
[102] Zie voor de nadere eisen die bij toestemming gelden randnrs. 4.3.17 e.v. van dit rapport.

4.3.10 Terzijde: de sectorale wetgeving kent diverse wettelijke bepalingen die voorschrijven dat de uitdrukkelijke toestemming van de patiënt vereist is voor het verstrekken van gegevens door een zorgverlener met een beroepsgeheim aan een derde. Zie bijvoorbeeld: artikel 9.1.2, tweede lid, Wlz dat bepaalt dat de verzekerde uitdrukkelijke toestemming moet verlenen voor het door het CIZ en de zorgaanbieder onderling verstrekken van diens (gezondheids)gegevens.

Ad (b) Wettelijke verplichting/recht

4.3.11 De zorgverlener mag zijn geheimhoudingsverplichting doorbreken indien een wettelijk voorschrift hiertoe verplicht of dat toelaat.[103] Voorafgaande toestemming van de patiënt is in een dergelijk geval niet vereist. Voorbeelden van dergelijke wettelijke verplichtingen/rechten zijn:

- het delen van de persoonsgegevens met de rechtstreeks bij de behandeling betrokken personen en de vervanger van de hulpverlener (artikel 7:457, tweede lid, BW);
- het – onder omstandigheden[104] – gebruiken van de persoonsgegevens van de patiënt ten behoeve van wetenschappelijk onderzoek en statistiek (artikel 7:458 BW);
- het geven van inzage in een dossier ten behoeve van materiële controle en/of fraudeonderzoek bij en aangaande jeugdhulpaanbieders (artikel 7.4.0, eerste lid, Jw jo. paragraaf 6b Regeling Jw)[105];
- het door een jeugdhulpaanbieder verstrekken van informatie aan het college die noodzakelijk is voor de uitvoering van de taken van de gemeente op grond van de Jw (artikel 7.4.0, tweede lid, Jw);
- het op grond van de Wlz verplicht aan elkaar verstrekken van persoonsgegevens, waaronder gezondheidsgegevens, door Wlz-uitvoerders, zorgaanbieders, het CAK en het CIZ, dan wel het verlenen van inzage of het ter beschikking stellen van een afschrift voor zover dit noodzakelijk is voor de in artikel 9.1.2 genoemde doeleinden (artikel 9.1.2, eerste lid, Wlz), bijv. het nemen van indicatiebesluiten door het CIZ.

Ad (c) Conflict van plichten

4.3.12 Een andere situatie waarin de zorgverlener zijn beroepsgeheim mag doorbreken is als hij verkeert in een 'conflict van plichten'. De doorbrekingsgrond 'conflict van plichten' betreft een uitzonderlijke situatie en kan het best worden begrepen als een overmachtssituatie. Het moet gaan om een noodtoestand, waarbij sprake is van een zodanig zwaarwegend algemeen belang dat de zorgverlener zich – ter voorkoming van

[103] Artikel 7:475, eerste lid, BW.
[104] Zie randnr. 4.3.50 van dit rapport.
[105] Het proces van materiële controle en detailcontrole is met strikte privacywaarborgen omgeven. Een van die waarborgen is dat de onderzoeken slechts (in opdracht van het college) mogen worden verricht door of onder verantwoordelijkheid van een persoon op wie het medisch beroepsgeheim van toepassing is.

ernstige schade voor de patiënt of een ander – verplicht voelt om zijn geheimhouding te doorbreken. De Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst ('KNMG') heeft diverse voorwaarden geformuleerd waaraan voldaan moet worden om een beroep te kunnen doen op de doorbrekingsgrond 'conflict van plichten':

> "Om een beroep te kunnen doen op het 'conflict van plichten' moeten in beginsel alle onderstaande voorwaarden zijn vervuld:
> - alles is in het werk gesteld om eerst toestemming van de patiënt te verkrijgen;
> - de arts verkeert in gewetensnood door het handhaven van de zwijgplicht [het beroepsgeheim];
> - er is geen andere weg om het probleem op te lossen dan door het doorbreken van de zwijgplicht;
> - Als de arts de zwijgplicht niet doorbreekt, levert dat voor een ander ernstige schade op;
> - het is vrijwel zeker dat die schade kan worden voorkomen of beperkt door de zwijgplicht te doorbreken;
> - het beroepsgeheim wordt zo min mogelijk geschonden. Slechts direct relevante gegevens mogen verstrekt worden;
> - Indien het mogelijk is, moet de arts aan de patiënt melden dat hij de gegevens aan een ander heeft verstrekt."[106]

4.3.13 Voor zover de zorgverlener (i) met uitdrukkelijke toestemming, (ii) met een beroep op een wettelijke voorschrift of (iii) op grond van een conflict van plichten zijn beroepsgeheim mag doorbreken, zal de zorgverlener de persoonsgegevens van de patiënt (in of buiten de blockchain) beschikbaar mogen stellen aan de betreffende derde. De feitelijke toegang kan plaatsvinden via een (gehashte) pointer die in een transactie op de blockchain wordt geplaatst. Door het loggen van de doorbreking van het medisch beroepsgeheim op de blockchain kan voor de patiënt inzichtelijk worden gemaakt wanneer (en mogelijk zelfs om welke reden) het medisch beroepsgeheim is doorbroken.

4.3.14 Er zijn situaties denkbaar dat niet kenbaar mag worden gemaakt aan de patiënt dat het beroepsgeheim is doorbroken (bijvoorbeeld ter voorkoming van een strafbaar feit). In deze situatie geldt uiteraard dat er geen vermelding mag worden opgenomen op de blockchain, althans geen vermelding die door de patiënt kan worden geraadpleegd.

---

[106] Vgl. KNMG Richtlijn 'Omgaan met medische gegevens' (8 september 2016), p. 61; zie tevens Centraal Tuchtcollege voor de Gezondheidszorg 7 november 2013, C-2013/199, rov. 4.3.

II. Bijzondere persoonsgegevens

4.3.15 Zoals reeds toegelicht in deel II van dit rapport, zullen blockchains in de zorg in veel gevallen ook bijzondere persoonsgegevens bevatten. Voor bijzondere persoonsgegevens geldt dat de verwerkingsverantwoordelijke zich moet kunnen beroepen op een doorbrekingsgrond. De algemene doorbrekingsgronden staan beschreven in artikel 9 AVG en de artikelen 22 tot en met 33 van de Uitvoeringswet AVG ('UAVG'). In aanvulling hierop bevatten sectorale wetten veelal bijzondere doorbrekingsgronden voor specifieke gevallen (onder meer de Wmo 2015, de Jw, de Wlz en de Zvw). Het gaat het bestek van dit rapport te buiten om alle afzonderlijke doorbrekingsgronden te behandelen. Hieronder volgt een niet-uitputtende bespreking van de doorbrekingsgronden die voor blockchains in de zorg het meest relevant zullen zijn. Het gaat daarbij kort gezegd om de volgende algemene doorbrekingsgronden:

(a) de betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking van zijn bijzondere persoonsgegevens (artikel 9, tweede lid, aanhef en onder a, AVG);

(b) de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en het socialezekerheids- en socialebeschermingsrecht, voor zover zulks is toegestaan bij Unierecht of lidstatelijk recht of bij een collectieve overeenkomst op grond van lidstatelijk recht die passende waarborgen voor de grondrechten en de fundamentele belangen van de betrokkene biedt (artikel 9, tweede lid, aanhef en onder b, AVG);

(c) de verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven (artikel 9, tweede lid, aanhef en onder c, AVG);

(d) de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene (artikel 9, tweede lid, aanhef en onder g, AVG);

(e) de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van

gezondheidszorgstelsels en -diensten of sociale stelsels en diensten (artikel 9, tweede lid, aanhef en onder h, AVG);

(f) de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim (artikel 9, tweede lid, aanhef en onder i, AVG);

(g) de verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, eerste lid, AVG op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de belangen van de betrokkene (artikel 9, tweede lid, aanhef en onder j, AVG).

Ad (a) Uitdrukkelijke toestemming[107]

4.3.16 Een doorbrekingsgrond die veelvuldig in de zorg wordt ingeroepen voor het verwerken van bijzondere persoonsgegevens is de 'uitdrukkelijke toestemming'. Deze wettelijke doorbrekingsgrond wordt in specifieke wettelijke bepalingen expliciet aangehaald als voorwaarde voor het verstrekken van gezondheidsgegevens. Zie onder meer:

- artikel 5.1.1, vierde lid, Wmo dat bepaalt dat het college, voor zover de betrokkene daarvoor zijn uitdrukkelijke toestemming heeft verleend, bevoegd is gezondheidsgegevens te verwerken onder meer indien dat noodzakelijk is voor de beoordeling van de behoefte van de cliënt aan ondersteuning van zijn participatie of zelfredzaamheid, dan wel opvang of beschermd wonen voor zover dat noodzakelijk is voor de aan de gemeente opgedragen Wmo-taken;
- artikel 5.2.5, eerste lid, Wmo dat bepaalt dat een zorgaanbieder met uitdrukkelijke toestemming van de betrokkene bevoegd is om uit eigen beweging en desgevraagd verplicht is aan het college (gezondheids)gegevens te verstrekken van een verzekerde die zorg als omschreven in de Zvw ontvangt of heeft ontvangen en in aanvulling of in aansluiting daarop aangewezen kan zijn op een maatwerkvoorziening, voor zover dat noodzakelijk is voor de uitvoering van de Wmo-taken van de zorgaanbieder;

[107] Artikel 9, tweede lid, aanhef en onder a AVG jo. artikel 22, tweede lid, aanhef en onder a, UAVG.

- artikel 9.1.2, tweede lid, Wlz dat bepaalt dat voor zover de verzekerde daartoe uitdrukkelijk toestemming heeft verleend, het CIZ en een zorgaanbieder elkaar kosteloos persoonsgegevens, waaronder gezondheidsgegevens, verstrekken;
- artikel 9.1.3, derde lid, Wlz dat bepaalt dat het college en de Wlz-uitvoerder elkaar met uitdrukkelijke toestemming van de betrokkene kosteloos de persoonsgegevens van de verzekerde, waaronder gezondheidsgegevens, verstrekken, voor zover de gegevens noodzakelijk zijn voor de onderlinge afstemming van de Wlz en de Wmo of Jw of voor het voorkomen van dubbele verstrekkingen.

4.3.17 Van rechtsgeldige toestemming in de zin van de AVG is sprake indien de toestemming van de betrokkene (i) vrijelijk, (ii) specifiek, (iii) geïnformeerd en (iv) op een ondubbelzinnige wijze is verkregen.

i. 'Vrijelijk'

4.3.18 De eerste voorwaarde, *vrijelijke* toestemming, houdt in dat de betrokkene daadwerkelijk een vrije keuze moet hebben of hij toestemming geeft voor de verwerking van zijn persoonsgegevens. Een belangrijke voorwaarde daarbij is dat de betrokkene geen nadelige gevolgen ondervindt indien hij zijn toestemming weigert of intrekt.[108]

Aandachtspunt: Overheidsorganen & toestemming
De Europese privacy toezichthouders[109], waaronder de AP zijn kritisch over het vragen van toestemming door overheidsorganen.[110] Zij zijn van oordeel dat overheidsorganen in beginsel geen beroep kunnen doen op de wettelijke grondslag 'toestemming'.[111] Doordat de burger in veel gevallen in een afhankelijkheidsrelatie jegens de overheid verkeert, zal de burger zich niet vrij voelen om zijn toestemming te weigeren, zo is de gedachte. Hierdoor is van vrije toestemming geen sprake. Hiermee is niet gezegd dat een overheidsorgaan onder geen beding de toestemmingsgrondslag persoonsgegevens zal kunnen verwerken, maar terughoudendheid en een kritische blik of inderdaad sprake kan zijn van 'vrije' toestemming is wel op zijn plaats.[112]

Het voorgaande is met name relevant in het sociaal domein, waar de gemeente betrokken is bij de toeleiding naar voorzieningen (bijvoorbeeld in het kader van de

[108] Vgl. Overwegingen 42 AVG: "Toestemming mag niet worden geacht vrijelijk te zijn verleend indien de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen." Zie tevens: Artikel-29 Werkgroep, 'Guidelines on consent under Regulation 2016/679' van 10 april 2018, WP259 rev. 01, p. 5-6.
[109] De Europese privacy toezichthouders zijn verenigd in de European Data Protection Board. Voordat de AVG van toepassing was, was dit nog de Artikel-29 Werkgroep.
[110] Artikel-29 Werkgroep, Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679, WP259, p. 6 e.v.
[111] Dit volgt ook rechtstreeks uit de AVG. Zie overweging 43 van de AVG: "In een specifiek geval wanneer er sprake is van een duidelijke wanverhouding tussen de betrokkene en de verwerkingsverantwoordelijke, met name wanneer de verwerkingsverantwoordelijke een overheidsinstantie is, en dit het onwaarschijnlijk maakt dat de toestemming in alle omstandigheden van die specifieke situatie vrijelijk is verleend.".
[112] Zie overweging 43 van de AVG.

Wmo en de Jeugdwet). De AP heeft geoordeeld dat de toestemming van de betrokkene géén grondslag kan vormen voor de verwerking van persoonsgegevens door de gemeente ten behoeve van de intake in het sociaal domein, waaronder de toeleiding naar voorzieningen uit de Wmo en de Jeugdwet.[113] De burger staat namelijk in een afhankelijkheidsrelatie tot de gemeente. Het weigeren van toestemming voor de gegevensverwerking zal veelal gevolgen hebben voor het verkrijgen van de door de betrokkene gewenste voorziening. Kort en goed lijkt het verstandig ervan uit te gaan dat overheidsorganen die betrokken zijn bij (toeleiding naar) zorgverlening slechts (bijzondere) persoonsgegevens mogen verwerken op de blockchain voor zover zij de verwerking kunnen baseren op een andere wettelijke grondslag.

4.3.19 Belangrijk is tot slot dat de toestemming *apart* moet worden gevraagd. Het verzoek om toestemming mag niet zijn verstopt in bijvoorbeeld de algemene voorwaarden of een contract. Het verzoek om toestemming voor de verwerking van persoonsgegevens moet duidelijk te onderscheiden zijn.[114]

ii. 'Specifiek'

4.3.20 De tweede voorwaarde voor het verkrijgen van rechtsgeldige toestemming is dat de toestemming gespecificeerd moet zijn: er moet om specifieke, gerichte toestemming worden gevraagd. Het toestemmingsformulier moet zo zijn vormgegeven dat de betrokkene zijn toestemming per gebruiker van de blockchain, per doel en per type persoonsgegevens kan differentiëren.[115] De doeleinden mogen niet zodanig vaag zijn dat zij na het verkrijgen van toestemming ruimer zouden kunnen worden geïnterpreteerd.

iii. 'Geïnformeerd'

4.3.21 De derde voorwaarde voor het verkrijgen van rechtsgeldige toestemming is dat sprake moet zijn van *geïnformeerde* toestemming. De betrokkene dient voorafgaand aan het verlenen van zijn toestemming uitvoerig te zijn geïnformeerd over de beoogde verwerking, zodat hij een geïnformeerde beslissing kan nemen of hij al dan niet zijn toestemming verleent. De (gezamenlijke) verwerkingsverantwoordelijken binnen de blockchain zullen voorafgaand in ieder geval de volgende informatie moeten verschaffen voor het verkrijgen van rechtmatige toestemming:

(a) de identiteit van de (mede) verwerkingsverantwoordelijke(n);
(b) het doel van iedere verwerking waarvoor toestemming wordt gevraagd;
(c) de (aard van de) gegevens waar de toestemming betrekking op heeft;

[113] Zie AP, Onderzoeksrapport 'Gegevensverwerking gemeente Nijmegen bij toeleiding naar hulp' van 15 februari 2018, p. 11.
[114] Vgl. Artikel 7, vierde lid, AVG jo. overweging 43 AVG.
[115] Daarbij kan gebruik worden gemaakt van afzonderlijke (digitale) formulieren per gebruiker of één formulier waarin meerdere opties en gebruikers zijn opgenomen.

(d) het bestaan van het recht van de betrokkene om zijn toestemming te allen tijde kosteloos in te trekken;

(e) (indien van toepassing) informatie over het gebruik van de persoonsgegevens voor geautomatiseerde besluitvorming in de zin van artikel 22 AVG, waaronder profilering[116], en tot slot;

(f) (indien van toepassing) de mogelijke risico's ten gevolge van doorgifte van de persoonsgegevens aan een land buiten de EU ten aanzien waarvan geen adequaatheidsbesluit is genomen, dan wel adequate waarborgen in de zin van artikel 46 AVG gelden.[117]

4.3.22 De Artikel-29 Werkgroep benadrukt in haar Richtlijn inzake toestemming[118] ten aanzien van punt (a) en (c) dat ook andere verwerkingsverantwoordelijke organisaties genoemd moeten worden bij het vragen om toestemming in het geval (i) de gevraagde toestemming wordt ingeroepen door meerdere (gezamenlijke) verwerkingsverantwoordelijken of (ii) de gegevens worden doorgegeven aan of verwerkt door andere verwerkingsverantwoordelijken die een beroep willen doen op de oorspronkelijk toestemming.[119]

4.3.23 De hierboven beschreven lijst is niet uitputtend. Afhankelijk van de omstandigheden en de context van de specifieke beoogde verwerking, is het mogelijk dat nadere informatie is vereist. Enige indicatie wanneer daarvan sprake is, wordt door de Artikel-29 Werkgroep niet gegeven. Voor zover het gaat om blockchains in de zorg zullen de verwerkingsverantwoordelijke gebruikers van de blockchain de betrokkene in ieder geval moeten informeren over het feit dat de persoonsgegevens via een blockchain zullen worden uitgewisseld (eventueel met nadere informatie over de werking van de blockchain).

4.3.24 De AVG schrijft niet voor op welke wijze de hiervoor genoemde informatie moet worden gegeven. De wijze waarop om toestemming wordt gevraagd is vormvrij. Dit neemt niet weg dat bepaalde kwaliteitseisen gelden ten aanzien van de inhoud van de informatie. Zo moet het verzoek om toestemming in een begrijpelijke en gemakkelijke toegankelijke vorm en in duidelijke en eenvoudige taal worden gepresenteerd.[120]

---

[116] Zie hierover paragraaf 5.2 van dit rapport.
[117] De informatie die aan de betrokkene zal moeten worden verschaft zal grotendeels al (moeten) zijn opgenomen in de privacyverklaring van de verwerkingsverantwoordelijke gebruikers. De Artikel-29 Werkgroep acht het toelaatbaar dat in de tekst van het verzoek om toestemming wordt verwezen naar de privacyverklaring of cookieverklaring. Zie. Artikel-29 Werkgroep, 'Guidelines on consent under Regulation 2016/679' van 10 april 2018, WP259 rev. 01, p. 13.
[118] Zie. Artikel-29 Werkgroep, 'Guidelines on consent under Regulation 2016/679' van 10 april 2018, WP259 rev. 01.
[119] De Artikel 29-Werkgroep benadrukt dat de (categorieën) ontvangers niet hoeven te worden genoemd om rechtmatige toestemming te verkrijgen. Dit laat echter onverlet dat een verwerkingsverantwoordelijke op grond van de informatieverplichtingen van artikelen 13 en 14 AVG verplicht is inzicht te geven in de ontvangers of categorieën ontvangers, waaronder andere verwerkingsverantwoordelijken. Zie Artikel-29 Werkgroep, 'Guidelines on consent under Regulation 2016/679' van 10 april 2018, WP259 rev. 01, p. 14.
[120] Artikel 7, tweede lid, AVG.

iv. 'Ondubbelzinnig'

4.3.25 De laatste voorwaarde voor het verkrijgen van rechtsgeldige toestemming is dat de toestemming ondubbelzinnig – door middel van een actieve handeling – moet zijn geuit. Er dient kortom altijd sprake te zijn van een 'opt-in'. De wijze waarop dit moet gebeuren, is in principe vormvrij. Het actief kunnen aankruisen van een vakje is in de ogen van de Europese privacy toezichthouders voldoende.[121]

Aanvullende voorwaarden

4.3.26 Voor zover 'uitdrukkelijke toestemming' een doorbrekingsgrond kan vormen voor de verwerking van persoonsgegevens op de blockchain, geldt als aanvullende voorwaarde dat:

- de verwerkingsverantwoordelijke kan aantonen wanneer en op welke wijze hij toestemming van de betrokkene heeft verkregen voor het verwerken van de persoonsgegevens, bijvoorbeeld door middel van het bijhouden van een 'toestemmingenregister'[122]. Vertaald naar de blockchain: het bewijs dat toestemming is verleend zou op de blockchain kunnen worden gelogd, en;
- de betrokkene de mogelijkheid moet krijgen om zijn toestemming gemakkelijk weer in te trekken. Zoals gezegd zullen op de blockchain maatregelen moeten worden getroffen die bewerkstelligen dat het intrekken van de toestemming daadwerkelijk tot effect heeft dat de betreffende gebruikers van de blockchain niet langer toegang hebben tot de betreffende gegevens van de betrokkene.[123]

4.3.27 De vraag rijst hoe betrokkenen toestemming zouden kunnen geven voor het verwerken van hun persoonsgegevens op de blockchain. De meest werkbare optie zou zijn dat de betrokkene door middel van een (gedigitaliseerd) toestemmingsformulier zijn toestemming gedifferentieerd (per verwerkingsverantwoordelijke) kan verlenen. Deze toestemming dient te worden verleend voordat de verwerkingsverantwoordelijken toegang krijgen tot de (betreffende) persoonsgegevens op de blockchain.

4.3.28 De (door de betrokkene) geautoriseerde gebruikers van de blockchain zullen uiteraard op de hoogte moeten zijn van de door de betrokkene toebedeelde autorisaties. Gebruikers moeten immers weten welke persoonsgegevens zij via de blockchain met welke andere gebruikers en voor welke doelen mogen delen. Het informeren van de gebruikers over de door de betrokkene verleende toestemmingen zou plaats kunnen vinden door hen inzage te verlenen in het ingevulde toestemmingsformulier. Daarbij zou geborgd moeten worden dat de gebruikers slechts inzage krijgen in het voor hen

[121] Een al aangevinkt vakje dat kan worden uitgezet (een 'opt-out') is niet voldoende.
[122] Uit dit toestemmingenregister zou moeten blijken (i) hoe toestemming is verkregen, (ii) wanneer en waarvoor de toestemming is verleend en (iii) de informatie die ten tijde van het verkrijgen van de toestemming door de verwerkingsverantwoordelijke is verstrekt.
[123] Zie over het verwijderen van persoonsgegevens uit de blockchain randnr. 5.4.32 van dit rapport.

relevante deel van het toestemmingsformulier (oftewel de autorisaties die op hen betrekking hebben).

4.3.29 Het hanteren van een door de betrokkene ingevuld toestemmingsformulier zal niet voldoende zijn. Het moet voor de betrokkene daarnaast mogelijk zijn om op een later moment (alsnog) toestemming te verlenen aan nieuwe gebruikers van de blockchain. Bovendien moet de betrokkene de mogelijkheid hebben om gedurende de verwerking zijn toestemming per afzonderlijke gebruiker in trekken of te wijzigen.[124] Om dit mogelijk te maken zal een functie moeten worden ingebouwd die de betrokkene in staat stelt om per gebruiker autorisaties in te trekken of te wijzigen.

4.3.30 Het is van belang dat nieuwe deelnemers niet kunnen terugkijken over de periode dat zij nog niet aan de blockchain deelnamen, tenzij de betrokkene daarvoor toestemming verleent. Daarnaast dient te worden gewaarborgd dat de gebruikers niet langer mogen deelnemen aan de blockchain indien de betrokkene zijn toestemming intrekt, bijvoorbeeld door via het smart contract te regelen dat het intrekken van de toestemming er (automatisch) toe leidt dat de gebruiker geen toegang meer kan krijgen tot de blockchain.

4.3.31 Tot slot een belangrijke nuancering. Het intrekken van toestemming door de betrokkene hoeft er niet per definitie toe te leiden dat de betreffende gebruiker niet meer bevoegd zou zijn om bijzondere persoonsgegevens (via de blockchain) te verwerken. Het is goed mogelijk dat de betreffende gebruiker de verwerking kan baseren op een andere doorbrekingsgrond dan toestemming. Het intrekken van de toestemming heeft in dat geval geen gevolgen voor de rechtmatigheid van de verwerking. De vraag zou hierbij overigens wel zijn of niet beter al in eerste instantie van de andere doorbrekingsgrond gebruik zou kunnen worden gemaakt.

> ***Aandachtspunt: wettelijke vertegenwoordigers van de betrokkene***
> *De toestemming dient in beginsel door de betrokkene te worden gegeven, tenzij de betrokkene (i) de leeftijd van zestien jaar nog niet heeft bereikt, (ii) onder curatele staat of (iii) ten behoeve van de betrokkene een bewind of mentorschap is ingesteld. In dat geval is in beginsel[125] de toestemming van de wettelijke vertegenwoordiger vereist (artikel 5, eerste en tweede lid, UAVG).[126] Het voorgaande kan – naast in de AVG – specifiek in de sectorale wetgeving geregeld zijn. Zo bepaalt artikel 7.3.15, eerste lid, Jw dat de voogd of de ouder van een jeugdige die jonger is dan 12 namens de jeugdige toestemming kan geven. Artikel 7.3.15, tweede lid, Jw bevat een soortgelijke bepaling voor een ten behoeve van*

[124] Met 'wijzigen' wordt bedoeld het door de betrokkene aanbrengen van wijzigingen in de aard of omvang van de gegevens die mogen worden verwerkt door de geautoriseerde gebruiker of het uitbreiden of beperken van de personen met wie de gebruiker persoonsgegevens mag uitwisselen.
[125] Dit is anders bij hulp- en adviesdiensten die rechtstreeks en kosteloos aan een minderjarige of een onder curatele gestelde worden aangeboden. Voor verwerkingen die in dat kader plaatsvinden kan de minderjarige of onder curatele gestelde wel toestemming geven. Zie artikel 5, vijfde lid, UAVG.
[126] In geval een betrokkene onder curatele staat, dan wel ten behoeve de betrokkene een bewind of mentorschap is ingesteld, geldt de relativering dat het moet gaan om een aangelegenheid waarvoor de betrokkene onbekwaam dan wel onbevoegd is. Zie artikel 5, tweede lid, UAVG.

de jeugdige aangestelde curator of mentor. De wettelijk vertegenwoordiger heeft de bevoegdheid om de toestemming te allen tijde in te trekken (artikel 5, derde lid, Uitvoeringswet AVG). De verwerkingsverantwoordelijke zal zich ervan moeten vergewissen dat een derde daadwerkelijk bevoegd is om te handelen als wettelijk vertegenwoordiger.

Ad (b) De verwerking is noodzakelijk voor de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht[127]

4.3.32 Op grond van artikel 9, tweede lid, aanhef en onder b, AVG mogen bijzondere persoonsgegevens worden verwerkt indien dit noodzakelijk is met het oog op het uitvoeren van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht. Deze doorbrekingsgrond dient een basis te hebben in het Europese of nationale recht of dient te volgen uit een nationale collectieve overeenkomst die passende waarborgen voor de grondrechten en fundamentele belangen van de betrokkene biedt.

4.3.33 De Nederlandse wetgever heeft hieraan, voor wat betreft gezondheidsgegevens, onder meer invulling gegeven door middel van artikel 30, eerste lid, UAVG. Dit artikel bepaalt dat het verbod om gezondheidsgegevens te verwerken niet van toepassing is indien de verwerking geschiedt door bestuursorganen, pensioenfondsen, werkgevers of instellingen die te hunnen behoeve werkzaam zijn en voor zover de verwerking noodzakelijk is voor de uitvoering van sociale zekerheidsstelsels, meer specifiek voor:

(a) een goede uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene, of;

(b) de re-integratie of begeleiding van werknemers of uitkeringsgerechtigden in verband met ziekte of arbeidsongeschiktheid.

4.3.34 Met name onderdeel a van artikel 30, eerste lid, UAVG zal relevant zijn voor blockchains in de zorg, omdat dit een doorbrekingsgrond vormt voor bestuursorganen of door hen ingeschakelde instellingen om, voor zover dit noodzakelijk is voor de uitvoering van de sociale zekerheid, gezondheidsgegevens te verwerken, bijvoorbeeld om te bepalen of een bepaalde voorziening noodzakelijk is. Het kan daarbij gaan om materiële voorzieningen of verstrekkingen die samenhangen met de gezondheidstoestand van de betrokkene, zoals speciale voorzieningen in een woning in verband met een lichamelijke handicap. Regelingen voor dergelijke voorzieningen

[127] Artikel 9, tweede lid aanhef en onder b AVG jo. artikel 30, eerste lid, UAVG.

vallen onder de noemer ‘aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene’. Mogelijke voorbeelden zijn:

- artikel 5.1.1 Wmo bepaalt dat het college bevoegd is tot het verwerken van onder meer gezondheidsgegevens die noodzakelijk zijn voor de beoordeling van de behoefte aan ondersteuning van de participatie of zelfredzaamheid van de cliënt en noodzakelijk zijn voor de uitvoering van de in artikel 5.1.1. Wmo genoemde taken van het college;

- artikel 5.1.2 Wmo bepaalt dat een aanbieder die een maatwerkvoorziening levert en een derde aan wie ten laste van een persoonsgebonden budget betalingen worden gedaan, bevoegd is tot het verwerken van gezondheidsgegevens, voor zover dit noodzakelijk is voor het leveren van de diensten, hulpmiddelen, woningaanpassingen en andere maatregelen waartoe hij zich jegens het college dan wel de cliënt heeft verbonden;
- artikel 9.1.2 Wlz dat bepaalt dat Wlz-uitvoerders, zorgaanbieders, het CAK en het CIZ elkaar kosteloos persoonsgegevens, waaronder gegevens over de gezondheid, verstrekken, voor zover dat noodzakelijk is voor de in artikel 9.1.2 genoemde taken (onder meer het nemen van indicatiebesluiten door het CIZ).

4.3.35 Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld. Doel daarvan is om te kunnen komen tot een precisering van de noodzakelijkheidseis met het oog op de verwerking van gezondheidsgegevens in de sociale zekerheid.[128]

4.3.36 De nationale wetgever heeft in artikel 30, vierde lid, UAVG bepaald dat persoonsgegevens over iemands gezondheid in beginsel alleen mogen worden verwerkt door personen met een geheimhoudingsplicht die voortvloeit uit hoofde van ambt, beroep, wettelijk voorschrift of overeenkomst. Artikel 30, vierde lid, UAVG bepaalt daarnaast dat op personen die niet zijn gebonden aan een geheimhoudingsplicht, maar die op grond van artikel 30, eerste tot en met derde lid, UAVG wél bevoegd zijn tot het verwerken van gezondheidsgegevens, een ‘gelijkwaardige geheimhoudingsplicht’ rust. Deze gelijkwaardige geheimhoudingsplicht is niet absoluut. De personen zijn bevoegd om op grond van een wettelijke plicht of als uit hun taak de noodzaak daartoe voortvloeit, gezondheidsgegevens te delen met andere personen die op grond van artikel 30 UAVG bevoegd zijn tot het verwerken van gezondheidsgegevens.

[128] Artikel 30, zesde lid, UAVG. Vgl. *Kamerstukken II* 2017/18, 34 851, nr. 2, p. 99.

Ad (c) De verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene, mits de betrokkene fysiek of juridisch niet in staat is om zijn toestemming te geven[129]

4.3.37 De verwerking van bijzondere persoonsgegevens op de blockchain is daarnaast toegestaan als de verwerking noodzakelijk is voor de bescherming van een vitaal belang, oftewel een belang dat voor het leven van de betrokkene of dat van een ander natuurlijke persoon van essentieel belang is. Deze grond moet beperkt worden geïnterpreteerd: er moet een dringende medische noodzaak zijn om de gegevens van de betrokkene te verwerken. Bij vitale belangen kan gedacht worden aan het verwerken van persoonsgegevens die noodzakelijk zijn voor humanitaire doelen, waaronder het monitoren van epidemieën en de verspreiding daarvan of verwerking van persoonsgegevens in humanitaire noodsituaties, zoals natuurrampen of door de mens veroorzaakte rampen.[130] Als voorwaarde voor deze doorbrekingsgrond geldt dat de betrokkene fysiek (bijv. bewusteloos) of juridisch (bijv. handelingsonbekwaam) niet in staat is zijn toestemming te geven.

> Een voorbeeld van een situatie waarin een vitaal belang van de betrokkene zou kunnen rechtvaardigen dat persoonsgegevens in een blockchain worden verwerkt, is de situatie dat een betrokkene een ongeluk krijgt, daardoor in een bewusteloze toestand komt te verkeren en een hulpverlener met spoed (medische) gegevens moet raadplegen die op de blockchain staan opgeslagen.

Ad (d) De verwerking is noodzakelijk om een reden van zwaarwegend algemeen belang[131]

4.3.38 De verwerking van bijzondere persoonsgegevens is verder toelaatbaar indien op grond van het Europese recht of het nationale recht in het kader van een zwaarwegend algemeen belang[132] een wettelijke uitzondering is gecreëerd voor de verwerking daarvan. Daarbij geldt als voorwaarde dat (i) de wettelijke bepaling evenredig is met het nagestreefde doel, (ii) de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en (iii) passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en fundamentele belangen van de betrokkene.

4.3.39 Voorbeelden van nationale doorbrekingsgronden die de Nederlandse wetgever op grond van artikel 9, eerste lid, aanhef en onder g, AVG heeft gecreëerd zijn de hierna te bespreken uitzonderingen voor de verwerking van genetische gegevens (artikel 28 UAVG) en biometrische gegevens (artikel 29 UAVG).

---

[129] Artikel 9, tweede lid, aanhef onder c, AVG jo. artikel 22, tweede lid, aanhef en onder c, AVG.
[130] Overweging 46 van de AVG.
[131] Artikel 9, eerste lid, aanhef en onder g, AVG.
[132] Een voorbeeld van een zwaarwegend algemeen belang is bijvoorbeeld een zwaarwegend geneeskundig belang of wetenschappelijke of statistische belangen.

4.3.40 Ook de sectorale wetten bevatten wettelijke grondslagen die kunnen worden aangemerkt als doorbrekingsgronden in de zin van artikel 9, eerste lid, aanhef en onder g, AVG. Zie bijvoorbeeld:

- artikel 8.4.2, eerste lid, Jw dat bepaalt dat de Sociale verzekeringsbank bevoegd is tot het verwerken van persoonsgegevens van de jeugdige en zijn ouders, waaronder persoonsgegevens over de gezondheid, die noodzakelijk zijn voor het verrichten van betalingen en het budgetbeheer van onder meer het persoonsgebonden budget, voor zover deze op rechtmatige wijze zijn verkregen en noodzakelijk zijn voor het uitvoeren van de jeugdwet-taken van de SVB;
- artikel 5.1.3, tweede lid, Wmo dat bepaalt dat onder meer het CAK bevoegd is tot het verwerken van gezondheidsgegevens van de cliënt die noodzakelijk zijn voor de vaststelling en inning van een bijdrage als bedoeld in artikel 2.1.4 en 2.1.5 van de Wmo, voor zover deze zijn verkregen op grond van artikel 5.2.1, 5.2.2 of 5.2.3 en noodzakelijk zijn voor de uitvoering van artikel 2.1.4 of 2.1.5;
- artikel 9.1.2, eerste lid, aanhef en onder d, Wlz dat bepaalt dat Wlz-uitvoerders, zorgaanbieders, het CAK en het CIZ elkaar kosteloos gezondheidsgegevens verstrekken voor zover dat noodzakelijk is voor onder meer de beoordeling van de Wlz-uitvoerder of de zorg op verantwoorde wijze kan worden verleend met een persoonsgebonden budget;
- artikel 5.2.2 Wmo dat bepaalt dat een aanbieder die een maatwerkvoorziening levert bevoegd is uit eigen beweging, persoonsgegevens van de cliënt, waaronder bijzondere persoonsgegevens, te verstrekken aan het college voor zover dat noodzakelijk is voor de uitvoering van de gemeentelijke wmo-taken van het college;
- artikel 87, eerste lid, Zvw dat bepaalt dat een zorgaanbieder die aan een verzekerde zorg of andere diensten heeft verleend, persoonsgegevens, waaronder gegevens over de gezondheid, verstrekt aan de zorgverzekeraar ten einde de kosten van de verleende zorg/diensten rechtstreeks bij de zorgverzekeraar in rekening te brengen. Voorwaarde is wel dat die gegevens noodzakelijk zijn voor de uitvoering van de zorgverzekering of de Zvw;
- artikel 7.4.0, eerste lid, onderdeel a, Jw dat onder meer bepaalt dat het college of door het college aangewezen personen persoonsgegevens mogen verwerken van de jeugdige of zijn ouders, waaronder het BSN van de jeugdige én bijzondere persoonsgegevens, voor zover dat noodzakelijk is voor de toeleiding naar, advisering over, bepaling van of het inzetten van een voorziening op het gebied van de jeugdhulp.

Ad (e) De verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten[133]

4.3.41 Een voor de zorg zeer relevante doorbrekingsgrond is artikel 9, tweede lid, aanhef en onder h, AVG. Op grond van deze bepaling kan het verbod om bijzondere persoonsgegevens – waaronder gezondheidsgegevens – te verwerken worden doorbroken indien de verwerking noodzakelijk is voor:

- doeleinden van preventie of arbeidsgeneeskunde voor de beoordeling van arbeidsgeschiktheid van de werknemer;
- medische diagnosen;
- het verstrekken van gezondheidszorg of sociale diensten of behandelingen, dan wel;
- het beheren van gezondheidszorgstelsels en –diensten of sociale stelsels en diensten.

4.3.42 De uitzondering moet bij Europese of nationale wet worden bepaald of de verwerking kan plaatsvinden uit hoofde van de (behandelings)overeenkomst die is gesloten tussen de patiënt en de zorgverlener.

4.3.43 Ook deze wettelijke doorbrekingsgrond is nader uitgewerkt in de UAVG en de sectorale wetgeving. Artikel 30, tweede lid, UAVG bevat een nadere doorbrekingsgrond voor de verwerking van gezondheidsgegevens door hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening (onderdeel a) en verzekeraars (onderdeel b).

4.3.44 Uit de uitzondering van artikel 30, derde lid, aanhef en onder a, UAVG volgt dat gezondheidsgegevens niet alleen mogen worden verwerkt door ziekenhuizen en andere medische instellingen, maar ook door instanties op het terrein van maatschappelijke dienstverlening. Voorbeelden van dergelijke instanties zijn volgens de wetgever verzorgingshuizen en instanties voor jeugdzorg. Het is daarnaast mogelijk dat individuele hulpverleners die niet bij voornoemde instellingen werkzaam zijn, maar bijvoorbeeld een zelfstandige praktijk uitoefenen, gezondheidsgegevens verwerken.

4.3.45 De verwerking van gezondheidsgegevens zal steeds alleen mogen plaatsvinden, voor zover een goede behandeling van de betrokkene dit noodzakelijk maakt of wanneer dat voor het beheer van de desbetreffende instelling of voorziening noodzakelijk is.[134]

---

[133] Artikel 9, tweede lid, aanhef en onder h, AVG jo. artikel 30, tweede lid, UAVG.
[134] Vgl. *Kamerstukken II* 2017/18, 34 851, nr. 2, p. 98: "Het begrip 'beheer' dient in dit onderdeel te worden uitgelegd als het waarborgen van de kwaliteit van de verleende zorg, intercollegiale toetsing door hulpverleners onderling (kwaliteitsbeheer) en de betaling van rekeningen voor medische behandeling. Dit laatste geldt zowel voor een instelling als bijvoorbeeld een ziekenhuis als een beroepspraktijk van een individuele hulpverlener."

4.3.46 Artikel 9, derde lid, AVG jo. artikel 30, vierde lid, UAVG noemt nog als belangrijke beperking dat de bijzondere persoonsgegevens slechts mogen worden verwerkt voor zover dit plaatsvindt onder de verantwoordelijkheid van een beroepsbeoefenaar die aan het beroepsgeheim is gebonden of tot geheimhouding is verplicht.[135]

Andere bijzondere persoonsgegevens in aanvulling op de gezondheidsgegevens

4.3.47 Het vijfde lid van artikel 30 UAVG bepaalt tot slot dat bepaalde personen en instanties die op grond van artikel 30, eerste lid, aanhef en onder a, UAVG gezondheidsgegevens mogen verwerken, voor zover noodzakelijk, in aanvulling daarop ook andersoortige bijzondere persoonsgegevens mogen verwerken. Het gaat hier om de hiervoor beschreven specifieke situatie waarin in het belang van een goede geneeskundige behandeling en verzorging van patiënten in aanvulling op gezondheidsgegevens ook andere bijzondere persoonsgegevens moeten worden verwerkt. Hierbij kan gedacht worden aan persoonsgegevens over godsdienst of levensovertuiging (omdat dit bijvoorbeeld direct invloed kan hebben op het behandelplan van een patiënt) of gegevens over iemands seksuele leven (omdat deze gegevens in een bepaalde context als medisch relevant kunnen worden aangemerkt).[136]

4.3.48 De uitzondering van artikel 30, derde lid, aanhef en onder b, AVG staat toe dat verzekeraars in herverzekeringen, levensverzekeringen, natura-uitvaartverzekeringen en schadeverzekeringen[137] in het kader van de uitvoering van de verzekeringsovereenkomst gezondheidsgegevens verwerken voor zover dit noodzakelijk is voor:

- de beoordeling van het door de verzekeraar te verzekeren risico en de betrokkene geen bezwaar heeft gemaakt, of;
- de uitvoering van de overeenkomst van verzekering dan wel het assisteren bij het beheer en de uitvoering van de verzekering.

4.3.49 Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld voor verwerkingen die vallen onder artikel 30, derde lid, aanhef en onder onderdeel b, AVG. Doel daarvan is om te kunnen komen tot een precisering van de noodzakelijkheidseis met het oog op de verwerking van gezondheidsgegevens ten behoeve van de uitvoering van de verzekeringsovereenkomst.[138]

Ad (f) De verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid[139]

4.3.50 Artikel 9, tweede lid, aanhef en onder i, AVG kan eveneens een relevante doorbrekingsgrond vormen voor het verwerken van bijzondere persoonsgegevens. Op

[135] Zie voor een uitgebreide bespreking van de geheimhoudingsplicht randnr. 4.3.2 van dit deel.
[136] Zie *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 115.
[137] Voorbeelden van schadeverzekeringen zijn de zorgverzekering en de ongevallenverzekering.
[138] Artikel 30, zesde lid, UAVG.
[139] Artikel 9, tweede lid, aanhef en onder i, AVG.

grond van deze bepaling geldt het verbod om bijzondere persoonsgegevens te verwerken niet, indien de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van volksgezondheid.[140] Als voorbeelden noemt de bepaling (i) de bescherming tegen ernstige grensoverschrijdende gevaren voor de volksgezondheid of (ii) het waarborgen van hoge veiligheid- en kwaliteitsnormen van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen. Deze uitzondering moet volgen uit het Europese of nationale recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name het beroepsgeheim.

Ad (g) De verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden[141]

4.3.51 Tot slot vormt artikel 9, tweede lid, aanhef onder j, AVG jo. artikel 24 UAVG een relevante doorbrekingsgrond voor het verwerken van bijzondere persoonsgegevens in de zorg. Bijzondere persoonsgegevens mogen ten behoeve van wetenschappelijk[142] of historisch[143] onderzoek of statistische[144] doeleinden worden verwerkt indien:

(a) de verwerking noodzakelijk is met het oog op een wetenschappelijk of historische onderzoek of statistische doeleinden;
(b) het onderzoek een algemeen belang dient;
(c) het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost[145]; en

[140] Zie Overweging 54 van de AVG: "In dit verband dient „volksgezondheid" overeenkomstig de definitie van Verordening (EG) nr. 1338/2008 van het Europees Parlement en de Raad te worden uitgelegd als alle elementen in verband met de gezondheid, namelijk gezondheidstoestand, inclusief morbiditeit en beperkingen, de determinanten die een effect hebben op die gezondheidstoestand, de behoeften aan gezondheidszorg, middelen ten behoeve van de gezondheidszorg, de verstrekking van en de universele toegang tot gezondheidszorg, alsmede de uitgaven voor en de financiering van de gezondheidszorg, en de doodsoorzaken."
[141] Artikel 9, tweede lid, aanhef en onder j, AVG jo. artikel 24 UAVG.
[142] Wetenschappelijk onderzoek moet ruim worden opgevat. Het kan gaan om technologische ontwikkeling en demonstratie, fundamenteel onderzoek, toegepast onderzoek en uit particuliere middelen gefinancierd onderzoek. Wetenschappelijke onderzoeksdoeleinden omvatten ook studies op het gebied van de volksgezondheid die in het algemeen belang worden gedaan. Hierbij gelden enkele voorwaarden. Vgl. Overweging 159 van de AVG: "Om als verwerking van persoonsgegevens met het oog op wetenschappelijk onderzoek te worden aangemerkt, moet de verwerking aan specifieke voorwaarden voldoen, met name wat betreft het publiceren of anderszins openbaar maken van persoonsgegevens voor wetenschappelijke onderzoeksdoeleinden. Indien de resultaten van wetenschappelijk onderzoek, met name op het gebied van gezondheid, aanleiding geven tot verdere maatregelen in het belang van de betrokkene, zijn met het oog op deze maatregelen de algemene regels van deze verordening van toepassing." Daar komt bovendien bij dat wetenschappelijke onderzoeken ook moeten voldoen aan andere toepasselijke wetgeving, zoals die over klinische proeven.
[143] Vgl. Overweging 160 van de AVG: "Wanneer persoonsgegevens met het oog op historisch onderzoek worden verwerkt, dient deze verordening ook voor verwerking met dat doel te gelden. Dit dient ook historisch onderzoek en onderzoek voor genealogische doeleinden te omvatten, met dien verstande dat deze verordening niet van toepassing mag zijn op overleden personen."
[144] Onder 'statistische doeleinden' wordt volgens overweging 162 van de AVG verstaan: "het verzamelen en verwerken van persoonsgegevens die nodig zijn voor statistische onderzoeken en voor het produceren van statistische resultaten. Die statistische resultaten kunnen ook voor andere doeleinden worden gebruikt, onder meer voor wetenschappelijke onderzoeksdoeleinden. Het statistische oogmerk betekent dat het resultaat van de verwerking voor statistische doeleinden niet uit persoonsgegevens, maar uit geaggregeerde gegevens bestaat, en dat dit resultaat en de persoonsgegevens niet worden gebruikt als ondersteunend materiaal voor maatregelen of beslissingen die een bepaalde natuurlijke persoon betreffen."
[145] Hieruit volgt dat uitdrukkelijke toestemming in beginsel de voorkeur heeft. Voldoende is dat de betrokkene toestemming geeft voor onderzoeken op een specifiek onderzoeksterrein. Vgl. *Kamerstukken II* 2017/18, 34 851, nr. 2, p. 42: "Het is vaak niet mogelijk op het ogenblik waarop de persoonsgegevens worden verzameld, het doel van de gegevensverwerking voor wetenschappelijke onderzoeksdoeleinden volledig te omschrijven.

(d) bij de uitvoering van het onderzoek is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

4.3.52 Zoals volgt uit artikel 89, eerste lid, AVG en overweging 156 van de AVG dienen de passende waarborgen ervoor te zorgen dat technische en organisatorische maatregelen worden getroffen om met name de inachtneming van het beginsel van gegevensminimalisering te verzekeren. Op de verwerkingsverantwoordelijke rust de verplichting om eerst te bezien of het mogelijk is om het onderzoek uit te voeren op een wijze dat de betrokkenen niet of niet langer geïdentificeerd kunnen worden. Is dit niet mogelijk dan is de verwerking niettemin mogelijk, mits uiteraard wordt voldaan aan de hiervoor (achter randnr. 4.3.51) beschreven voorwaarden en (overige) passende waarborgen zijn getroffen, zoals de pseudonimisering van de persoonsgegevens.

4.3.53 Uit artikel 9, eerste lid, aanhef en onder j, AVG jo. artikel 89 AVG jo. Archiefwet volgt verder nog dat bijzondere persoonsgegevens mogen worden verwerkt met het oog op archivering in het algemeen belang. Ook voor deze archivering geldt dat passende waarborgen getroffen moeten worden.[146]

Zorgspecifieke doorbrekingsgrond voor statistische en wetenschappelijke medische onderzoeken (artikel 7:458 BW)

4.3.54 Het is mogelijk dat het statistisch of wetenschappelijk onderzoek ziet op medische gegevens waarop een medisch beroepsgeheim rust. Zoals hiervoor toegelicht, is in dat geval niet alleen een doorbrekingsgrond vereist voor het verwerken van de bijzondere persoonsgegevens, maar dient er ook een doorbrekingsgrond te zijn voor het opheffen van het beroepsgeheim.

4.3.55 Voor wetenschappelijke en statistische onderzoeken op het gebied van volksgezondheid vormt artikel 7:458, eerste lid, BW een grond voor de doorbreking van het medisch beroepsgeheim.

4.3.56 Artikel 7:458, eerste lid, BW bepaalt dat het – zonder toestemming van de patiënt – verstrekken van inlichtingen over de patiënt of het verlenen van inzage in het medisch dossier van de patiënt ten behoeve van statistisch of wetenschappelijk onderzoek op het gebied van volksgezondheid is toegestaan, indien:

Daarom moet de betrokkene worden toegestaan toestemming te geven voor bepaalde terreinen van het wetenschappelijk onderzoek waarbij erkende ethische normen voor wetenschappelijk onderzoek in acht worden genomen. De betrokkene moet de gelegenheid krijgen om zijn toestemming alleen te geven voor bepaalde onderzoeksterreinen of onderdelen van onderzoeksprojecten, voor zover het voorgenomen doel dit toelaat."

[146] Zie vorige alinea.

(a) het vragen van toestemming in redelijkheid niet mogelijk is[147] en zodanige waarborgen zijn getroffen dat de persoonlijke levenssfeer van de patiënt niet onevenredig wordt geschaad[148], of;

(b) het vragen van toestemming, gelet op de aard en het doel van het onderzoek, in redelijkheid niet kan worden verlangd en de hulpverlener zorg heeft gedragen dat de gegevens in zodanige vorm worden verstrekt dat herleiding tot de individuele natuurlijke persoon redelijkerwijs wordt voorkomen.[149]

4.3.57 Daarnaast gelden de aanvullende voorwaarden dat:

(a) het onderzoek een algemeen belang dient;
(b) het onderzoek niet zonder de desbetreffende gegevens kan worden uitgevoerd;
(c) de betrokken patiënt tegen een verstrekking geen uitdrukkelijk bezwaar heeft gemaakt, en tot slot;
(d) in het dossier een aantekening wordt gehouden van de verstrekking ten behoeve van het wetenschappelijk of statistisch onderzoek op het gebied van volksgezondheid.

Ad (h) Genetische gegevens[150]

4.3.58 Artikel 28 UAVG bevat diverse doorbrekingsgronden voor het verwerken van genetische gegevens.[151] Genetische gegevens zijn persoonsgegevens met betrekking tot de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon. Deze genetische kenmerken moeten blijken uit een biologisch monster van de persoon in kwestie.[152] Aangezien genetische gegevens niet alleen betrekking hebben op de

[147] Voorbeelden die in de parlementaire geschiedenis worden aangehaald zijn onder meer de situaties dat (i) historisch wetenschappelijk onderzoek wordt verricht en de adressen van de personen niet meer te achterhalen zijn (*Kamerstukken II* 1989/90, 21561, 3, p. 40), (ii) het te belastend is voor de ex-patiënt om opnieuw met zijn ziekte te worden geconfronteerd (*Kamerstukken II* 1989/90, 21561, 3, p. 40) en (iii) de patiënt is overleden (*Kamerstukken II* 1989/90, 21 561, nr. 3, p. 40).
[148] Voor de vraag wanneer voldoende waarborgen zijn getroffen, kan worden aangesloten bij de Gedragscode Gezondheidsonderzoek. Deze gedragscode is in 2004 door de AP goedgekeurd. Inmiddels is in 2013 een nieuwe versie van de Gedragscode ingediend. Deze is echter nog niet goedgekeurd door de AP.
[149] Deze situatie ziet op onderzoeken waarbij zo grote aantallen patiënten betrokken zijn, dat niet redelijkerwijs kan worden gevergd dat iedereen moet worden bereikt of het vragen van toestemming mogelijk zou kunnen leiden tot selectieve respons (*Kamerstukken II* 1993/94, 21561, 20, p. 3). Herleiding moet redelijkerwijs worden voorkomen, hetgeen inhoudt dat de hulpverlener maatregelen moet treffen die: "ten minste tot gevolg te hebben dat de individuele onderzoeker of het onderzoeksinstituut, behalve over de geanonimiseerde of gecodeerde gegevens, niet tevens beschikt over de gegevens die dienen om rechtstreeks tot daadwerkelijke herleiding over te gaan. Uiteraard zal de onderzoeker of het onderzoeksinstituut ook niet door middel van het vergelijken van verschillende bestanden met geanonimiseerde of gecodeerde gegevens tot indirecte herleiding mogen overgaan. Voor zover dergelijke vergelijkingen voor het onderzoek noodzakelijk zijn, kan worden gedacht aan bijzondere procedures van besluitvorming door bij voorbeeld een commissie van toezicht verbonden aan het onderzoeksinstituut. Verder is het denkbaar dat de hulpverlener een intermediaire organisatie inschakelt die, anders dan de onderzoeker of het onderzoeksinstituut, vanwege het feit dat deze organisatie de sleutel van de gecodeerde gegevens beheert, beschikt over de mogelijkheid gegevens tot de individuele natuurlijke persoon te herleiden" Zie *Kamerstukken II* 1993-1994, 21 561, nr. 20 p. 4.
[150] Artikel 9, tweede lid, aanhef en onder g, AVG jo. artikel 28 Uitvoeringswet AVG.
[151] Deze bepaling is een uitwerking van artikel 9, tweede lid, aanhef en onder g, AVG.
[152] Overweging 34 van de AVG noemt in dit verband de volgende voorbeelden van analyses waaruit de genetische gegevens kunnen blijken: "(…) met name een chromosoomanalyse, een analyse van

betrokkene, maar ook op anderen in dezelfde genetische lijn (familieleden), bevat artikel 28 UAVG de volgende doorbrekingsgronden:

- artikel 28, eerste lid, UAVG bepaalt dat het verwerken van de genetische gegevens alleen is toegestaan met betrekking tot de persoon bij wie de genetische gegevens zijn verkregen;

- artikel 28, tweede lid, UAVG bepaalt vervolgen dat het verbod om genetische gegevens te verwerken in andere gevallen (dus bij 'bovenpersoonlijk gebruik') aleen is toegestaan als:

  (i) een zwaarwegend geneeskundig belang prevaleert (bijvoorbeeld indien uit een erfelijkheidsonderzoek blijkt dat de behandeling van familieleden noodzakelijk is), of;

  (ii) de verwerking noodzakelijk is ten behoeve van wetenschappelijk onderzoek dat een algemeen belang dient of ten behoeve van statistiek, waarbij geldt dat:

  (a) de betrokkene uitdrukkelijke toestemming heeft gegeven, en;
  (b) bij de uitvoering van het onderzoek is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

4.3.59 Het verkrijgen van uitdrukkelijke toestemming voor bovenpersoonlijk gebruik is niet vereist indien dit onmogelijk blijkt of een onevenredige inspanning vergt.[153]

Ad (i) Biometrische gegevens[154]

4.3.60 De nationale wetgever heeft ook voor de verwerking van biometrische gegevens een doorbrekingsgrond geformuleerd. Artikel 29 UAVG bepaalt dat het verbod om biometrische gegevens te verwerken ten behoeve van de unieke identificatie van een persoon niet geldt, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Er zal dus moeten kunnen worden onderbouwd dat biometrische beveiliging/authenticatie noodzakelijk en proportioneel is.

4.3.61 Het is goed denkbaar dat de toegang tot de blockchain wordt voorzien van een biometrisch authenticatiesysteem. Denkbaar is bijvoorbeeld dat de blockchain zo wordt vormgegeven dat gebruikers hun vingerafdruk moeten scannen om toegang te kunnen krijgen tot de blockchain. Artikel 29 UAVG zal een relevante doorbrekingsgrond kunnen vormen voor de biometrische gegevens die ten behoeve van dit identiteitsmanagement van de gebruikers van de blockchain worden verwerkt, mits

---

desoxyribonucleïnezuur (DNA) of van ribonucleïnezuur (RNA) of (…)een analyse van andere elementen waarmee soortgelijke informatie kan worden verkregen."
[153] Artikel 28, derde lid, UAVG.
[154] Artikel 9, tweede lid, aanhef en onder g, AVG jo. artikel 29 UAVG.

uiteraard kan worden onderbouwd dat de aard van de blockchain rechtvaardigt dat biometrie wordt ingezet ter beveiliging van de blockchain. Gezien het feit dat bij inzet van blockchains in de zorg veelal gevoelige gegevens zullen worden verwerkt, zal sneller betoogd kunnen worden dat een biometrische beveiliging van de blockchain noodzakelijk en proportioneel is.

III. De (aanvullende) verwerking van persoonsgegevens van strafrechtelijke aard

4.3.62 Het kan voorkomen dat zorgverleners, maar bijvoorbeeld ook overheidsinstanties met een rol in het sociaal domein, strafrechtelijke gegevens verwerken in aanvulling op medische gegevens. Strafrechtelijke persoonsgegevens zijn persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen. Gedacht kan worden aan veroordelingen en gegronde verdenkingen, maar ook aan gegevens over de toepassing van het formele strafrecht, bijvoorbeeld het gegeven dat iemand is gearresteerd of tegen hem een proces-verbaal is opgesteld wegens een bepaald vergrijp. Het aanvullend verwerken van dergelijke strafrechtelijke gegevens kan noodzakelijk zijn voor bijvoorbeeld het opstellen van een op de persoon toegesneden behandelplan.

4.3.63 Persoonsgegevens van strafrechtelijke aard vormen onder de AVG een aparte categorie persoonsgegevens en onderscheiden zich van de in artikel 9 AVG genoemde bijzondere persoonsgegevens. Deze gegevens mogen alleen worden verwerkt voor zover de verwerking plaatsvindt onder toezicht van de overheid[155] of indien de verwerking is toegestaan op grond van Europees of nationaal recht dat passende waarborgen voor de betrokkene biedt. De nationale uitzonderingen zijn nader uitgewerkt in de artikelen 31 tot en met 33 UAVG. Het gaat het bestek van dit rapport te buiten om deze gronden afzonderlijk te bespreken. Op het moment dat een verwerkingsverantwoordelijke constateert dat persoonsgegevens van strafrechtelijke aard zullen worden verwerkt in een blockchain, dient de verwerkingsverantwoordelijke er alert op te zijn dat hiervoor een afzonderlijke wettelijke grondslag in de artikelen 10 jo. artikelen 31 tot en met 33 UAVG moet bestaan.

4.3.64 Eén van de gronden die voor blockchains in de zorg relevant kan zijn is artikel 33, eerste lid, aanhef en onder c, AVG dat bepaalt dat gegevens van strafrechtelijke aard mogen worden verwerkt indien dit noodzakelijk is ten behoeve van de goede behandeling of verzorging van de betrokkene in aanvulling op de verwerking van gegevens over de gezondheid door hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening.

4.3.65 Tot slot bevatten ook de sectorale wetten bepalingen die het mogelijk maken dat gegevens van strafrechtelijke aard worden verwerkt. De verwerkingsverantwoordelijke

[155] Voor zorgaanbieders en private organisaties zal geen sprake zijn van het verwerken van strafrechtelijke gegevens onder toezicht van de overheid. Dit maakt dat een zorgaanbieder zich op één van de nationale uitzonderingsbepalingen van artikelen 31 tot en met 33 UAVG moet kunnen beroepen.

dient aldus ook altijd in de sectorale wetten te kijken of een grondslag voorhanden is voor de verwerking van de gegevens van strafrechtelijke aard. Hierbij kan bijvoorbeeld gewezen worden op:

- artikel 7.4.0, eerste lid, onderdeel a, Jw dat onder meer bepaalt dat het college of een door het college aangewezen persoon persoonsgegevens mag verwerken, waaronder persoonsgegevens van strafrechtelijke aard, voor zover dit noodzakelijk is voor de toeleiding naar, advisering over, bepaling van of inzetten van een voorziening op het gebied van jeugdhulp;
- artikel 4.1.8 Jw dat onder meer bepaalt dat de jeugdhulpaanbieder, de jeugdhulpverlener en de gecertificeerde instelling persoonsgegevens van strafrechtelijke aard kunnen verstrekken aan toezichthouders indien dit noodzakelijk is voor het onderzoeken van een melding van geweld bij de verlening van jeugdhulp.

IV. De wettelijke grondslagen voor het verwerken van (bijzondere) persoonsgegevens

4.3.66 In de voorgaande paragrafen is toegelicht dat een verwerkingsverantwoordelijke pas bevoegd is tot het verwerken van persoonsgegevens in een blockchain indien hij heeft vastgesteld dat: (i) het (medisch) beroepsgeheim niet van toepassing is of kan worden doorbroken, en (ii) voor zover er sprake is van het verwerken van bijzondere persoonsgegevens (bijv. medische gegevens, genetische gegevens, biometrische gegevens), een wettelijke doorbrekingsgrond voorhanden is die het verbod op het verwerken van bijzondere persoonsgegevens doorbreekt en (iii) een wettelijke grondslag bestaat voor het verwerken van eventuele strafrechtelijke gegevens.

4.3.67 Zodra deze stappen zijn doorlopen, dient de verwerkingsverantwoordelijke vervolgens ten aanzien van íeder persoonsgegeven (dus zowel normale als bijzondere persoonsgegevens) vast te stellen of de verwerking kan worden gebaseerd op een wettelijke grondslag.[156] De wettelijke grondslagen voor het verwerken van persoonsgegevens staan beschreven in bijzondere (zorgspecifieke) wetten of in artikel 6, eerste lid, AVG. De algemene wettelijke grondslagen van artikel 6 AVG luiden als volgt:

> a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
>
> b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;

[156] Als de verwerkingsverantwoordelijke heeft vastgesteld dat zich een doorbrekingsgrond voordoet voor het verwerken van een bijzonder persoonsgegeven, dan zal dit vaak betekenen dat de verwerkingsverantwoordelijke óók een wettelijke grondslag heeft in de zin van artikel 6, eerste lid, AVG om het bijzondere persoonsgegeven te verwerken.

c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;

e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;

f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

4.3.68 Hieronder gaan wij in op de (voor de zorg) meest relevante wettelijke grondslagen. Daarbij zullen wij steeds niet-uitputtende voorbeelden geven uit de relevante sectorale wetten.

Ad (a) De betrokkene verleent toestemming voor de verwerking van persoonsgegevens op de blockchain (artikel 6, eerste lid, aanhef en onder a, AVG)

4.3.69 Een veel gebruikte wettelijke grondslag in de zorg is de wettelijke grondslag 'toestemming'. Voor de voorwaarden voor rechtsgeldige toestemming en voorbeelden uit de sectorale wetten verwijzen wij naar de eerdere bespreking van de doorbrekingsgrond 'uitdrukkelijke toestemming' (randnrs. 4.3.17 e.v. van dit rapport).

Ad (b) Noodzakelijk voor de uitvoering van een overeenkomst of het treffen van precontractuele maatregelen (artikel 6, eerste lid, aanhef en onder b, AVG)

4.3.70 Persoonsgegevens mogen daarnaast door een gebruiker van een blockchain worden verwerkt indien de verwerking noodzakelijk is voor de uitvoering van een overeenkomst of het treffen van precontractuele maatregelen (artikel 6, eerste lid, aanhef en onder b, AVG). Een beroep op deze wettelijke grondslag is alleen mogelijk indien de betrokkene partij is bij de overeenkomst of als de betrokkene heeft verzocht om het treffen van precontractuele maatregelen.

Een voorbeeld van een zorgspecifieke overeenkomst is de overeenkomst inzake de geneeskundige behandeling (behandelingsovereenkomst) in de zin van artikel 7:446 BW.

Ad (c) Noodzakelijk voor de uitvoering van een wettelijke verplichting (artikel 6, eerste lid, aanhef en onder c, AVG)

4.3.71 De verwerking van persoonsgegevens is voorts toegestaan indien de verwerking noodzakelijk is om te kunnen voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust (artikel 6, eerste lid, aanhef en onder c, AVG). De wettelijke verplichting kan voortvloeien uit Europees of nationaal recht. De wettelijke verplichting hoeft geen expliciete opdracht tot gegevensverwerking te bevatten. Het gaat er om dat het, om aan de wettelijk verplichting te voldoen, noodzakelijk is dat persoonsgegevens worden verwerkt. In de praktijk zal de wettelijke verplichting echter veelal wel betrekking hebben op het (verplicht) vastleggen of bewaren van gegevens of het verstrekken daarvan aan derden.

Een voorbeeld van een zorgspecifieke wettelijke plicht tot het verwerken van persoonsgegevens is de dossierplicht die rust op een hulpverlener die op grond van een geneeskundige behandelingsovereenkomst zorg levert aan een patiënt (artikel 7:454 BW).[157] Voor de daarmee verband houdende verwerkingen kan dan een grondslag worden gevonden in de wettelijke verplichting van artikel 6, eerste lid, aanhef en onder c, AVG.

4.3.72 Andere (niet-uitputtende) voorbeelden uit de relevante sectorale wetgeving betreffen:

- artikel 9.1.2, eerste lid, Wlz dat bepaalt dat Wlz-uitvoerders, zorgaanbieders, het CAK en het CIZ elkaar kosteloos persoonsgegevens verstrekken van de verzekerde, waaronder gezondheidsgegevens, voor zover dat noodzakelijk is voor onder meer: (onderdeel a) het nemen van indicatiebesluiten, (onderdeel e) de zorglevering, en (onderdeel i) het verrichten van controle of fraudeonderzoek door de Wlz-uitvoerders;
- artikel 9.1.3, tweede lid, Wlz dat bepaalt dat onder meer zorgverzekeraars, het Zorginstituut en de SVB voor de in artikel 9.1.3, eerste lid, Wlz genoemde doeleinden verplicht zijn op verzoek (gezondheids)gegevens te verstrekken aan een Wlz-uitvoerder, het CAK of het CIZ;
- artikel 7.4.0, tweede lid, Jw dat bepaalt dat jeugdhulpaanbieders, aanbieders van preventie, gecertificeerde instellingen, de raad voor de kinderbescherming en gekwalificeerde gedragswetenschappers het college of een door het college aangewezen persoon kosteloos de persoonsgegevens van een jeugdige of zijn ouders moeten verstrekken, waaronder het burgerservicenummer van de jeugdige en bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard, die voor het college of die personen noodzakelijk zijn voor de uitvoering van de werkzaamheden, bedoeld in het eerste lid van artikel 7.4.0 Jw.

[157] Zie Art. 7:454 BW: "De hulpverlener richt een dossier in met betrekking tot de behandeling van de patiënt. Hij houdt in het dossier aantekening van de gegevens omtrent de gezondheid van de patiënt en de te diens aanzien uitgevoerde verrichtingen en neemt andere stukken, bevattende zodanige gegevens, daarin op, een en ander voor zover dit voor een goede hulpverlening aan hem noodzakelijk is."

Ad (d) Noodzakelijk voor de bescherming van de vitale belangen van de betrokkene (artikel 6, eerste lid, aanhef en onder d, AVG)

4.3.73 Voor deze wettelijke grondslag geldt grotendeels hetzelfde als voor de 'vitaal belang' doorbrekingsgrond van artikel 9, tweede lid, aanhef en onder c, AVG. Enig verschil is dat artikel 6, eerste lid, aanhef en onder d, AVG niet de voorwaarde stelt dat de betrokkene geen toestemming *kan* verlenen. Desalniettemin geldt hier dat als toestemming kan worden gevraagd aan de betrokkene, dit de voorkeur verdient.

> Voor een nadere bespreking van deze wettelijke grondslag verwijzen wij naar de bespreking van de doorbrekingsgrond 'vitaal belang' (zie randnr. 4.3.37 van dit rapport).

Ad (e) Noodzakelijk voor de vervulling van een taak van algemeen belang (artikel 6, eerste lid, aanhef en onder e, AVG)

4.3.74 Een belangrijke wettelijke grondslag voor bestuursorganen is artikel 6, eerste lid, aanhef en onder e, AVG: de verwerking van persoonsgegevens is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen (bijv. het uitvoeren van publiekrechtelijke taken in het sociaal domein). De publiekrechtelijke taak of taak van algemeen belang moet zijn vastgesteld in nationaal of Europees recht.

4.3.75 De sectorale wetten bevatten diverse wettelijke bepalingen op grond waarvan bestuursorganen in het kader van hun (zorg)taken persoonsgegevens mogen verwerken, mits dat noodzakelijk is voor de aan hen opgedragen taken. Zie onder meer:

- artikel 7.4.0, tweede lid, Jw dat bepaalt dat jeugdhulpaanbieders, aanbieders van preventie, gecertificeerde instellingen, de raad voor de kinderbescherming en gekwalificeerde gedragswetenschappers het college of een door het college aangewezen persoon kosteloos de persoonsgegevens van een jeugdige of zijn ouders moeten verstrekken, waaronder het burgerservicenummer van de jeugdige en bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard, die voor het college of die personen noodzakelijk zijn voor de uitvoering van de werkzaamheden, bedoeld in het eerste lid van artikel 7.4.0 Jw.
- artikel 8.4.2, eerste lid, Jw dat bepaalt dat de Sociale verzekeringsbank bevoegd is tot het verwerken van persoonsgegevens van de jeugdige en zijn ouders, waaronder persoonsgegevens over de gezondheid, die noodzakelijk zijn voor het verrichten van betalingen en het budgetbeheer van onder meer het persoonsgebonden budget;
- artikel 5.1.1, eerste lid, Wmo dat bepaalt dat het college bevoegd is tot het verwerken van persoonsgegevens van de cliënt, waaronder

gezondheidsgegevens, die noodzakelijk zijn voor de beoordeling van diens behoefte aan ondersteuning van zijn participatie of zelfredzaamheid dan wel opvang of beschermd wonen;

- artikel 5.1.2, eerste lid, Wmo dat bepaalt dat een aanbieder die een maatwerkvoorziening levert en een derde aan wie ten laste van een pgb betalingen worden gedaan, bevoegd is tot het verwerken van persoonsgegevens van de cliënt, waaronder gegevens over gezondheid en die noodzakelijk zijn voor de levering van de diensten of hulpmiddelen aan of woningaanpassingen voor de cliënt;
- artikel 70, dertiende lid, Zvw dat bepaalt dat het CAK bevoegd is tot het verwerken van persoonsgegevens van gemoedsbezwaarden, waaronder gegevens over de gezondheid die noodzakelijk zijn voor het openen van een rekening.

Ad (f) Noodzakelijk voor behartiging van gerechtvaardigd belang van de verwerkingsverantwoordelijke of een ander

4.3.76 Tot slot kunnen ook de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde een rechtsgrond vormen voor de verwerking van persoonsgegevens. Artikel 6, eerste lid, aanhef en onder f, AVG bepaalt dat de verwerking van persoonsgegevens mag plaatsvinden indien de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde en deze gerechtvaardigde belangen zwaarder wegen dan de (privacy)belangen of rechten van de betrokkene. Om dit te kunnen vaststellen is met name van belang welke impact de gegevensverwerking heeft op de betrokkene. Dit is voornamelijk afhankelijk van de aard van de persoonsgegevens, de wijze waarop de persoonsgegevens worden verwerkt, de redelijke verwachting van de betrokkene, de gevolgen van de verwerking voor de betrokkene en de onderlinge verhouding tussen de verwerkingsverantwoordelijke en de betrokkene.[158]

4.3.77 Overheidsorganen kunnen geen beroep doen op de grond ‘gerechtvaardigd belang’, voor zover het gaat om de verwerking van persoonsgegevens in het kader van de uitoefening van hun publieke taken. De ‘gerechtvaardigd belang-grond’ zal slechts door een overheidsorgaan kunnen worden ingeroepen als deze zich bij de handelingen in welk kader persoonsgegevens worden verwerkt niet wezenlijk onderscheidt van een private partij. Bijvoorbeeld als het gaat om verwerking van persoonsgegevens in het kader van typisch bedrijfsmatige handelingen (zoals de beveiliging van gebouwen). Deze situatie lijkt zich in de zorg niet snel voor te doen. Als uitgangspunt zal dan ook moeten gelden dat overheidsorganen - voor zover het gaat om blockchains in de zorg -

[158] Opinion 06/2014 Article 29 Data Protection Working Party on the notion of legitimate interests of the data controller under artikel 7 of Directive 95/46/EC, p. 36-40.

verwerkingen niet zullen kunnen baseren op artikel 6, eerste lid, aanhef en onder f, AVG.

V. De verwerking van het nationale identificatienummer, zoals het BSN

4.3.78 Tot slot dient bij de vaststelling of een verwerkingsverantwoordelijke gebruiker persoonsgegevens op de blockchain mag verwerken, extra zorgvuldigheid te worden betracht bij het verwerken van nationale identificatienummers zoals het BSN.

4.3.79 Op grond van artikel 87 AVG mag de Nederlandse wetgever specifieke voorwaarden stellen aan het gebruik van het nationale identificatienummer. De Nederlandse wetgever heeft hieraan uitvoering gegeven door in artikel 46, eerste lid, UAVG te bepalen dat het gebruik van wettelijke identificatienummers in beginsel bij (formele) wet moet zijn voorgeschreven en slechts mag worden gebruikt ter uitvoering van de in de wet genoemde doelstellingen (artikel 46, eerste lid, UAVG). Hierna wordt ingegaan op het BSN; een in de zorg belangrijk nationaal identificatienummer.

Algemene wettelijke grondslagen in de Wabb

4.3.80 De wetgever heeft met artikel 10 Wabb een algemene wettelijke grondslag gecreëerd voor overheidsorganen om het BSN te verwerken voor de uitvoering van hun (publiekrechtelijke) taak. Daarnaast zijn de gebruikers van het BSN bij het onderling uitwisselen van persoonsgegevens op grond van artikel 11, eerste lid, Wabb verplicht tot het gebruik van BSN. Een gebruikers is (i) een overheidsorganen en (ii) ieder ander dan een overheidsorgaan of degene aan wie het BSN is toegekend, voor zover deze werkzaamheden verricht waarbij het gebruik door hem of haar van het BSN bij of krachtens de wet is voorgeschreven.[159]

Het (verplichte) gebruik van het BSN bij de uitvoering van de sectorale wetgeving

4.3.81 In de sectorale wetgeving wordt het gebruik van het BSN in veel gevallen verplicht gesteld. Hieronder volgt een (niet-uitputtende) toelichting per sectorale wet.

Het gebruik van het BSN op grond van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg ('Wabvz')

4.3.82 De Wabvz verplicht zorgaanbieders onder meer tot:

- het gebruik van het BSN van een cliënt met het doel te waarborgen dat de in het kader van de verlening van zorg te verwerken persoonsgegevens op de cliënt betrekking hebben (artikel 4 Wabvz);
- het vaststellen van het BSN van een cliënt bij de eerste keer dat de cliënt zich tot de zorgaanbieder wendt ter verkrijging van zorg (of voor zover dat

[159] Vgl. Artikel 1, aanhef en onder d, Wabb.

(op een later moment) noodzakelijk is om zich ervan te vergewissen dat het BSN betrekking heeft op de persoon over wie hij gegevens verwerkt ('vergewisplicht')) (artikel 5 Wabvz);
- het opnemen van het BSN van de cliënt door de zorgaanbieder in zijn administratie bij het vastleggen van persoonsgegevens met betrekking tot de verlening van zorg (artikel 8 Wabvz);
- het vermelden van het BSN van de cliënt door de zorgaanbieder bij het verstrekken van persoonsgegevens met betrekking tot de verlening van, indicatiestelling voor of verzekering van zorg aan een zorgaanbieder, een indicatieorgaan of een zorgverzekeraar (artikel 9 Wabvz).

Het gebruik van het BSN op grond van de Wlz

4.3.83 De volgende partijen zijn op grond van (onder meer, maar niet uitsluitend) de volgende bepalingen van de Wlz verplicht tot het gebruik van het BSN:

- de Wlz-uitvoerder is verplicht tot het gebruik van het BSN van een cliënt met het doel te waarborgen dat de in het kader van de verlening van de zorg te verwerken persoonsgegevens op die cliënt betrekking hebben (artikel 9.1.1, eerste lid, Wlz jo. artikel 4 Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg);
- de Wlz-uitvoerders, zorgaanbieders, het CAK, het CIZ, het Zorginstituut en de zorgautoriteit zijn verplicht tot het gebruik van het BSN bij onderling contact ter uitvoering van de Wlz (artikel 9.1.1, derde lid, Wlz);
- het CIZ stelt bij de aanvraag van een indicatiebesluit de identiteit van de verzekerde vast, onder meer aan de hand van het BSN, daarna geldt een vergewisplicht (artikel 9.1.1, zesde lid, Wlz).

Het gebruik van het BSN op grond van de Jw

4.3.84 De gecertificeerde instelling, de jeugdhulpaanbieder, de raad voor de kinderbescherming en het college gebruiken het BSN van een jeugdige met het doel te waarborgen dat de in het kader van de uitvoering van de Jeugdwet en de daarop berustende bepalingen te verwerken persoonsgegevens op die jeugdige betrekking hebben (artikel 7.2.1 Jw).[160] Het BSN wordt bij het eerste contact vastgelegd, daarna geldt een vergewisplicht (artikel 7.2.2 Jw).

Het gebruik van het BSN op grond van de Wmo 2015

4.3.85 Het college, een aanbieder en een derde aan wie ten laste van een persoonsgebonden budget betalingen worden gedaan, het CAK, bij gemeentelijke verordening

[160] Voor de gecertifieerde instelling geldt de uitzondering dat het gebruik van het BSN niet geldt voor het uitwisselen van persoonsgegevens van verdachten en veroordeelden ten behoeve van jeugdreclassering. (artikel 7.2.1, tweede lid, Jw).

aangewezen instanties die de bijdrage van een maatwerkvoorziening of een pgb voor opvang vaststellen en innen, de Sociale verzekeringsbank, de toezichthoudende ambtenaren, het AMHK, en een zorgverzekeraar of een zorgaanbieder als bedoeld in de Zorgverzekeringswet gebruiken het BSN bij het verstrekken van persoonsgegevens als bedoeld in de artikelen 5.2.1 tot en met 5.2.5 Wmo (artikel 5.2.9 Wmo). Het doel van het gebruik van het BSN is te waarborgen dat de in het kader van de uitvoering van de Wmo te verwerken persoonsgegevens op de juiste persoon betrekking hebben.

Het gebruik van het BSN op grond van de Zvw

4.3.86 De Zvw schrijft ten aanzien van het gebruik van het BSN ter uitvoering van de Zvw (onder meer, maar niet uitsluitend) het volgende voor:

- de zorgverzekeraar is verplicht tot het opnemen van het BSN van de verzekerde in zijn administratie tot zeven jaar na het einde van de verzekering (artikel 86, eerste lid, Zvw);
- de zorgverzekeraar gebruikt het BSN van de verzekerde met het doel te waarborgen dat de in het kader van de verzekering van zorg te verwerken persoonsgegevens op die verzekerde betrekking hebben (artikel 86, derde lid, Zvw);
- de zorgverzekeraars, het Zorginstituut, de zorgautoriteit (NZa), de minister van VWS[161], de rijksbelastingdienst, het Uitvoeringsinstituut werknemersverzekeringen, de Sociale verzekeringsbank, het college van burgemeester en wethouders, het CAK, of aan een daartoe door of vanwege een van deze zorgverzekeraars of instanties aangewezen persoon zijn verplicht tot het gebruik van het BSN voor zover zij bevoegd zijn tot het gebruik daarvan en zij gegevens uitwisselen op grond van artikel 88 en 89 Zvw.

4.4 Conclusie deel IV

4.4.1 Zoals volgt uit voorgaande bespreking van (i) het (medisch) beroepsgeheim, (ii) de doorbrekingsgronden voor de verwerking van bijzondere persoonsgegevens, (iii) de wettelijke grondslagen voor het aanvullend verwerken van persoonsgegevens van strafrechtelijke aard, (iv) de wettelijke grondslagen en tot slot (v) het regime voor het verwerken van het BSN, dient iedere verwerkingsverantwoordelijke die (bijzondere) persoonsgegevens verwerkt in een blockchain per verwerking te controleren of hij daartoe bevoegd is. De verwerkingsverantwoordelijke zal altijd alert moeten zijn op het feit dat in ieder geval een deel van de verwerkingsverantwoordelijke gebruikers op de blockchain niet bevoegd zal zijn tot het verwerken (waaronder begrepen: lezen) van de persoonsgegevens.

[161] Artikel 1, aanhef en onder n, Zvw.

4.4.2 Hiermee ontstaat het risico dat dat deel van de verwerkingsverantwoordelijken – zonder de daartoe vereiste wettelijke grondslag – persoonsgegevens verwerken binnen de blockchain. Dit zal een onrechtmatige verwerking van persoonsgegevens betreffen, met onder meer als gevolg een risico op hoge boetes van de AP. Dit aan het gebruik van de blockchain inherente risico, lijkt slechts te kunnen worden opgelost in een private, permissioned blockchain, waarbij lees- en schrijfrechten kunnen worden toegekend aan specifieke gebruikers, zodat:

- in het smart contract kan worden geregeld welke gebruikers (gelet op o.a. de gronden voor doorbreking van het medisch beroepsgeheim en voor de verwerking van bijzondere persoonsgegevens en gelet op de wettelijke grondslagen) toegang hebben tot welke persoonsgegevens;
- in het smart contract kan worden geregeld dat de verzender van een transactie per transactie kan bepalen welke gebruikers binnen de blockchain de transactie kunnen lezen;
- de persoonsgegevens voor niet-geautoriseerde gebruikers kunnen worden gehasht (zodat de impact van de verwerking wordt beperkt)[162], en;
- de niet-geautoriseerde gebruikers kunnen optreden als verwerkers en zij aldus de wettelijke grondslagen en doorbrekingsgronden van de geautoriseerde verwerkingsverantwoordelijken waarvoor zij persoonsgegevens verwerken, kunnen overnemen (vgl. deel III van dit advies).

[162] Als gezegd zullen niet-geautoriseerde gebruikers moeten kwalificeren als verwerkers voor de transacties waarvoor zij niet geautoriseerde zijn.

5 MATERIËLE VEREISTEN VAN DE BLOCKCHAIN

5.1 Inleiding

5.1.1 Nadat de verwerkingsverantwoordelijke gebruikers van de blockchain overeenkomstig deel IV van dit rapport hebben vastgesteld dat:

- (voor zover van toepassing) het medisch beroepsgeheim kan worden doorbroken;
- (in geval van bijzondere persoonsgegevens) een doorbrekingsgrond voorhanden is;
- een wettelijke grondslag bestaat voor het verwerken van persoonsgegevens op de blockchain, en;
- de bijzondere regels voor het verwerken van strafrechtelijke gegevens en/of het BSN geen beletsel vormen voor de verwerking.

dient vervolgens te worden vastgesteld of de verwerking van de persoonsgegevens in overeenstemming is met de overige materiële vereisten van de AVG.

5.1.2 In dit deel zal worden besproken welke uit de AVG voortvloeiende materiële vereisten in blockchain-verband specifieke privacyrechtelijke vragen oproepen. Daarbij zullen bovendien suggesties worden gedaan voor de wijze waarop een verwerkingsverantwoordelijke bij het gebruik van blockchain technisch en organisatorisch invulling kan geven aan deze materiële vereisten. In dit deel van het rapport zal meer concreet worden ingegaan op:

- de regels voor geautomatiseerde besluitvorming, waaronder profilering;
- de regels voor internationale doorgifte van persoonsgegevens;
- de beginselen genoemd in artikel 5 van de AVG, te weten:
  - (a) het beginsel dat persoonsgegevens moeten worden verwerkt op een wijze die rechtmatig, behoorlijk en transparant is (artikel 5, eerste lid, aanhef en onder a, AVG);
  - (b) het doelbindingsbeginsel (artikel 5, eerste lid, aanhef en onder b, AVG);
  - (c) het beginsel van minimale gegevensverwerking (artikel 5, eerste lid, aanhef en onder c, AVG);
  - (d) het juistheidsbeginsel (artikel 5, eerste lid, aanhef en onder d, AVG);
  - (e) het beginsel van opslagbeperking (artikel 5, eerste lid, aanhef en onder e, AVG);
  - (f) het beveiligingsbeginsel (artikel 5, eerste lid, aanhef en onder f, AVG;
- de verantwoordingsplicht (artikel 5, tweede lid, AVG).

- de beginselen van privacy by design & default;
- de verplichting tot het verrichten van een Data Protection Impact Assessment;
- de meldplicht datalekken.

5.2 Geautomatiseerde besluitvorming

5.2.1 Bij het gebruik van een blockchain en een daaraan ten grondslag liggend smart contract zal al snel sprake kunnen zijn van geautomatiseerde besluitvorming, zonder dat daarbij noodzakelijkerwijs menselijke tussenkomst plaatsvindt. Voor geautomatiseerde besluitvorming gelden in de AVG strikte vereisten. Op grond van artikel 22, eerste lid, AVG mag niemand worden onderworpen aan een besluit dat uitsluitend is gebaseerd op geautomatiseerde verwerking van persoonsgegevens, waaronder profilering,[163]dat rechtsgevolgen voor hem heeft of hem in aanmerkelijke mate treft (hierna: geautomatiseerde besluitvorming).[164]

5.2.2 Van gevolgen die een betrokkene 'anderszins in aanmerkelijke mate treft' is volgens de Artikel-29 Werkgroep sprake indien het geautomatiseerde besluit (i) de omstandigheden, het gedrag of de keuze van de betrokken personen in aanmerkelijke mate treft, (ii) een langdurig of blijvend effect op de betrokkene heeft, of (iii) in het uiterste geval, tot uitsluiting of discriminatie van personen leidt. Het is moeilijk om in zijn algemeenheid te bepalen welk gevolg ernstig genoeg is om te kunnen spreken van een gevolg dat een betrokkene in aanmerkelijke mate treft. Voorbeelden van gevolgen die een betrokkene in aanmerkelijke mate kunnen treffen zijn onder meer besluiten die iemands toegang tot gezondheidszorgdiensten raken en besluiten die iemands financiële situatie treffen, zoals zijn mogelijkheid om in aanmerking te komen voor een lening.[165]

5.2.3 In artikel 22, tweede lid, AVG zijn drie uitzonderingen opgenomen op het verbod op geautomatiseerde besluitvorming. Het verbod geldt niet als het besluit (kort gezegd):

a. noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
b. is toegestaan bij een Unierechtelijke of nationale bepaling; of
c. berust op de nadrukkelijke toestemming van de betrokkene.

5.2.4 In artikel 40 UAVG is de afwijkingsmogelijkheid onder b) nader uitgewerkt. Daaruit volgt dat het verbod op geautomatiseerde besluitvorming niet van toepassing is als de

[163] Profilering is volgens artikel 4, aanhef en onder 4, van de AVG elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.
[164] De geautomatiseerde voorbereiding van besluiten, waarbij het uiteindelijke besluit wordt genomen door een natuurlijke persoon met behulp van die geautomatiseerde voorbereiding, valt buiten de reikwijdte van artikel 22 AVG.
[165] Vgl. Artikel 29 Werkgroep, 'Guidelines on automated decision-making and profiling', WP 251, p. 10-11.

geautomatiseerde besluitvorming, anders dan op basis van profilering, noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of noodzakelijk is voor de vervulling van een taak van algemeen belang. Bij dit laatste heeft de wetgever (primair) gedacht aan individuele (gebonden) besluitvorming op basis van strikt individuele kenmerken, bijvoorbeeld bij het toekennen van bepaalde toeslagen. "Er is geen reden om bij dergelijke besluitvorming menselijke tussenkomst te vergen, omdat dit geen toegevoegde waarde heeft"[166], aldus de wetgever. Uit de toelichting volgt verder dat onder "taak van algemeen belang" een publieke taak moet worden begrepen.[167] Ook is vermeld dat de bepaling ruimte biedt aan de private sector om bij de vervulling van wettelijke verplichtingen gebruik te maken van geautomatiseerde besluitvorming zonder menselijke tussenkomst.[168]

5.2.5 Als een geautomatiseerd besluit wordt genomen op grond van een van de uitzonderingsgronden moet de verwerkingsverantwoordelijke passende maatregelen treffen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene.[169] Voor verwerkingsverantwoordelijken die geen bestuursorgaan zijn, moet het treffen van passende waarborgen ieder geval bestaan uit het recht van de betrokkene om op diens verzoek alsnog menselijke tussenkomst te krijgen van de verwerkingsverantwoordelijke, het recht voor een betrokkene om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten (artikel 22, derde lid, AVG en artikel 40, derde lid, UAVG). Voor *alle* verwerkingsverantwoordelijken geldt bovendien dat zij aan de betrokkene specifieke informatie over de geautomatiseerde besluitvorming moeten verstrekken, waaronder in ieder geval (i) een mededeling aan de betrokkene dat geautomatiseerde besluitvorming wordt toegepast, (ii) nuttige informatie over de onderliggende logica en (iii) het belang en de verwachte gevolgen van de geautomatiseerde besluitvorming.[170]

5.2.6 Van belang is verder nog dat geautomatiseerde besluiten op grond van artikel 22, vierde lid, AVG niet mogen worden gebaseerd op bijzondere categorieën van persoonsgegevens (zie artikel 9, eerste lid, AVG), tenzij de doorbrekingsgrond genoemd in artikel 9, tweede lid, onder a, AVG of in artikel 9, tweede lid, onder g, AVG van toepassing is en er passende maatregelen zijn getroffen.

5.2.7 Artikel 9, tweede lid, onder a, AVG bevat een doorbrekingsgrond voor het verbod om bijzondere persoonsgegevens te verwerken als de verwerking (kort gezegd) geschiedt met uitdrukkelijke toestemming van de betrokkene.

5.2.8 Artikel 9, tweede lid, onder g, AVG bevat een doorbrekingsgrond voor het verbod om bijzondere persoonsgegevens te verwerken als de verwerking noodzakelijk is om

---

[166] *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 120.
[167] *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 120.
[168] *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 121.
[169] Artikel 40, tweede lid, UAVG
[170] Zie artikel 13, tweede lid, aanhef en onder f, AVG en artikel 14, tweede lid, aanhef en onder g, AVG. Vgl. Artikel 29-Werkgroep, 'Guidelines on automated decision-making and profiling', WP 251, p. 33 e.v.

redenen van zwaarwegend algemeen belang, op grond van Unierecht (Europese Unie) of nationaal recht, waarbij:

- de evenredigheid met het nagestreefde doel wordt gewaarborgd;
- de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd; en
- passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en fundamentele belangen van de betrokkene.

5.2.9 Voor blockchains in de zorg waarbij sprake is van geautomatiseerde besluitvorming zal de verwerkingsverantwoordelijke gebruiker steeds moeten controleren of zich een van bovengenoemde grondslagen voordoet die de geautomatiseerde besluitvorming rechtvaardigt. Voor zover een dergelijke wettelijke grondslag ontbreekt, zal menselijke tussenkomst moeten worden ingebouwd, zodat geen sprake meer is van geautomatiseerde besluitvorming.

5.2.10 De vraag is wanneer sprake is van (voldoende) menselijke tussenkomst. In de Tweede Kamer is die vraag aan de orde gekomen. Houdt dat in dat er betekenisvolle menselijke handelingen verricht moeten worden of is het simpelweg goedkeuren van een op geautomatiseerde verwerking gebaseerd besluit voldoende om niet tegen het verbod op geautomatiseerde besluitvorming aan te lopen? Het antwoord op die vraag luidt als volgt[171]:

> "De Artikel 29-Werkgroep heeft menselijke tussenkomst als volgt omschreven: «Om te kwalificeren als menselijke tussenkomst, moet de verwerkingsverantwoordelijke verzekeren dat het toezicht op het besluit betekenisvol is en niet symbolisch. Het toezicht moet worden uitgevoerd door iemand die bevoegd is om het besluit te veranderen. Als onderdeel van de analyse moet met alle beschikbare input- en output-gegevens rekening worden gehouden.» En: «De beoordelaar dient een grondige beoordeling te verrichten van alle relevante gegevens, inclusief aanvullende informatie die wordt verstrekt door betrokkene.»"

5.2.11 In de voetnoot bij bovengenoemde passage staat:

> "Article 29 data protection working party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 3 October 2017, WP 251, p. 10 & 16. «An automated process produces what is in effect a recommendation concerning a data subject. If a human being reviews and takes account of other factors in making the final decision, that decision would not be «based solely» on automated processing.»"

[171] *Kamerstukken II* 2017-2018, 34 851, nr. 7, p. 47.

5.2.12 De interpretatie van de Artikel 29-Werkgroep van wat onder menselijke tussenkomst moet worden verstaan, wordt dus door de wetgever omarmd: menselijke tussenkomst moet betekenisvol zijn.

5.3 Internationale doorgifte

5.3.1 Zoals reeds is vastgesteld in deel II van dit rapport, is het mogelijk dat er bij het gebruik van een blockchain sprake is van de verwerking van persoonsgegevens buiten de Europese Unie. Deze situatie doet zich bijvoorbeeld voor indien een van de gebruikers, dan wel zijn node, zich buiten de Europese Unie bevindt en daar persoonsgegevens verwerkt. In dat geval is er sprake van internationale doorgifte van persoonsgegevens. Er mogen op grond van de AVG pas persoonsgegevens naar zogenoemde derde landen (buiten de EU) worden doorgegeven (waaronder begrepen: opgeslagen) als aan de eisen wordt voldaan die daarvoor gelden. Die eisen zijn opgenomen in de artikelen 44 t/m 49 AVG. Daaruit volgt – samengevat – dat in de volgende gevallen persoonsgegevens mogen worden doorgegeven aan derde landen:

- Als de Europese Commissie een zogenoemd 'adequaatheidsbesluit' heeft genomen over het derde land, inhoudende dat dat land, een gebied of een of meerdere nader bepaalde sectoren in dat derde land een passend beschermingsniveau waarborgt (artikel 45 AVG)[172];
- Door passende waarborgen te bieden, bijvoorbeeld door gebruikmaking van door de Europese Commissie of de AP goedgekeurde standaardbepalingen (artikel 46-47 AVG); of
- Als een beroep kan worden gedaan op een van de gronden voor doorgifte voor specifieke situaties, bijvoorbeeld als de doorgifte noodzakelijk is voor de uitvoering van een in het belang van de betrokkene gesloten overeenkomst (artikel 49 AVG).

5.3.2 Verwerkingsverantwoordelijken zullen aan de hand van bovengenoemde regels – die in dit rapport niet nader worden uitgewerkt – moeten vaststellen of zich een grond voordoet die maakt dat de internationale doorgifte van persoonsgegevens via de blockchain is toegestaan.

5.3.3 Voor zover een niet in de EU gevestigde verwerkingsverantwoordelijke of (sub)verwerker persoonsgegevens op de blockchain verwerkt over betrokkenen in de EU voor:

a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist; of

[172] Ten tijde van het schrijven van dit rapport heeft de Europese Commissie adequaatheidsbesluiten (onder meer, maar niet uitsluitend) genomen over Andorra, Argentinië, Canada, Israël, Japen, Nieuw-Zeeland, Zwitserland en de Verenigde Staten (voor zover de betreffende organisatie is aangesloten bij het EU-VS Privacy Shield). Zie voor een volledige lijst van door de Europese Commissie uitgegeven adequaatheidsbesluiten de website van de Europese Commissie: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt,

moet schriftelijk een vertegenwoordiger in één van de lidstaten worden aangewezen waar de betrokkenen zich bevinden. De vertegenwoordiger moet zijn gevestigd in een van die lidstaten en moet door de verwerkingsverantwoordelijke of de (sub)verwerker worden gemachtigd om naast hem of in zijn plaats te worden benaderd, meer in het bijzonder door de toezichthoudende autoriteiten en betrokkenen, over alle met de verwerking verband houdende aangelegenheden (artikel 27 AVG).

5.3.4 De verplichting om overeenkomstig artikel 27 AVG een vertegenwoordiger aan te wijzen geldt niet voor:

- een incidentele verwerking waarbij zich geen grootschalige verwerking voordoet van bijzondere persoonsgegevens of strafrechtelijke gegevens en waarbij de kans gering is dat zich een risico voordoet voor de rechten en vrijheden van natuurlijke personen, of;
- een overheidstantie of overheidsorgaan.

5.4 De beginselen van de AVG

5.4.1 Zoals hiervoor toegelicht, bevat artikel 5 van de AVG zes beginselen waaraan de verwerking van persoonsgegevens dient te voldoen:

(a) het beginsel dat persoonsgegevens moeten worden verwerkt op een wijze die rechtmatig, behoorlijk en transparant is;
(b) het doelbindingsbeginsel;
(c) het beginsel van minimale gegevensverwerking;
(d) het juistheidsbeginsel;
(e) het beginsel van opslagbeperking;
(f) het beveiligingsbeginsel.

5.4.2 Deze beginselen gelden onverkort voor de verwerking van persoonsgegevens in een blockchain, maar kunnen in blockchain-verband echter specifieke privacyrechtelijke vragen oproepen. Hieronder volgt een bespreking van de afzonderlijke privacybeginselen. Voor zover een beginsel in blockchain-verband specifieke privacyrechtelijke vragen oproept, zullen suggesties worden gedaan voor de wijze waarop een verwerkingsverantwoordelijke bij het gebruik van blockchain technisch en organisatorisch (zoveel mogelijk) invulling kan geven aan het betreffende beginsel.

Ad (a) Rechtmatigheid, behoorlijkheid en transparantie

5.4.3 Artikel 5, eerste lid, aanhef en onder a, AVG schrijft voor dat persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Deze eis vindt in feite zijn uitwerking in een groot deel van de overige privacy-eisen, die hierna nog aan de orde komen.

5.4.4 De eis van rechtmatigheid, behoorlijkheid en transparantie brengt in blockchain-verband geen onoverkomelijke privacyrechtelijke problemen met zich mee. Niettemin verdient het aanbeveling dat de gebruikers met elkaar afspreken dat zij de privacyregels in acht zullen nemen bij het gebruik van de blockchain. Daarmee wordt ook een zekere waarborg ingebouwd ten aanzien van andere eisen die niet specifiek blockchain-gerelateerd zijn, maar waaraan de gebruikers wel moeten voldoen.

Ad (b) Doelbinding

5.4.5 Artikel 5, eerste lid, aanhef en onder b, AVG schrijft voor dat persoonsgegevens dienen te worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De persoonsgegevens mogen vervolgens niet verder worden verwerkt op een met die doeleinden onverenigbare wijze.

5.4.6 Ook deze eis roept in blockchain-verband geen specifieke privacyrechtelijke vragen op. De verwerkingsverantwoordelijke gebruikers dienen voorafgaand aan het ontwerp en het gebruik van de blockchain een heldere en duidelijke omschrijving te geven van de doelstelling(en) van de verwerkingen die via de blockchain plaats zullen vinden. Slechts aan de hand van een afgebakende en concreet omschreven doelstelling, kan worden beoordeeld welke persoonsgegevens noodzakelijk zijn om binnen de blockchain te verwerken.

Ad (c) Minimale gegevensverwerking

5.4.7 Op grond van artikel 5, eerste lid, aanhef en onder c, AVG moeten persoonsgegevens toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Dit beginsel wordt aangeduid als het beginsel van minimale gegevensverwerking, ook wel het beginsel van dataminimalisatie genoemd. Deze eis heeft onder meer tot gevolg dat de partij die informatie op de blockchain plaatst steeds zal moeten nagaan welke andere gebruikers de informatie mogen zien en of die persoonsgegevens ook (nog langer) nodig zijn. De verwerking dient steeds beperkt te zijn tot het strikt noodzakelijke.

5.4.8 Het waarborgen van het beginsel van dataminimalisatie in een blockchain wordt gezien als één van de grootste privacy-uitdagingen bij het gebruik van blockchain. Dit heeft verschillende redenen.

5.4.9 Allereerst geldt bij het gebruik van blockchain als uitgangspunt dat elke gebruiker van de blockchain een kopie heeft van de (gehashte) persoonsgegevens die op de blockchain worden verwerkt. Het plaatsen van persoonsgegevens op de blockchain leidt ertoe dat niet-geautoriseerde gebruikers bij het gebruik van de blockchain bepaalde gehashte persoonsgegevens ontvangen, die zij buiten de blockchain nimmer zouden ontvangen en die bovendien niet noodzakelijk zijn voor de uitvoering van hun taken. De verwerking van dergelijke gehashte persoonsgegevens staat in principe

haaks op het beginsel van dataminimalisatie, nu die persoonsgegevens voor de niet-geautoriseerde partij niet ter zake dienend zullen zijn.

5.4.10 Een andere reden is dat een blockchain in beginsel uitgaat van 'immutability'. Immutability houdt in dat eenmaal toegevoegde transacties in een blockchain niet gewijzigd of verwijderd kunnen worden. Dit kan botsen met het beginsel van dataminimalisatie, aangezien persoonsgegevens die op enig moment niet meer noodzakelijk zijn toch (blijvend) worden verwerkt op de blockchain. Verwerkingsverantwoordelijken zullen technische maatregelen moeten treffen om te bewerkstelligen dat deze niet-noodzakelijke persoonsgegevens uit de blockchain kunnen worden verwijderd (zie voor een nadere bespreking van enkele technische oplossingen om persoonsgegevens in een blockchain (zo veel mogelijk) te verwijderen, de bespreking van het beginsel van opslagbeperking en het verwijderingsrecht van de betrokkene, randnrs. 5.4.31 e.v. en 6.4.9 e.v. van dit rapport).

Suggesties voor het waarborgen van dataminimalisatie bij het gebruik van blockchain in de zorg

5.4.11 Hoewel het een uitdaging kan zijn om de verwerking van persoonsgegevens in een blockchain in lijn te brengen met het beginsel van dataminimalisatie, lijkt dit niet onmogelijk. De volgende stappen kunnen worden doorlopen om er (zoveel mogelijk) voor te zorgen dat de persoonsgegevens die op de blockchain worden verwerkt zijn beperkt tot het strikt noodzakelijke:

I. Voorkom de opslag van persoonsgegevens op de blockchain door het opnemen van links naar off-chain persoonsgegevens;
II. Pseudonimiseer de (aanvullende) persoonsgegevens met een hash;
III. Stel de standaardinstellingen van de blockchain af op een zo hoog mogelijk privacyniveau;
IV. Informeer de gebruikers van de blockchain over de wijze waarop zij zich bij het gebruik van de blockchain kunnen houden aan het beginsel van dataminimalisatie;
V. Beperk ook de verwerking van additionele persoonsgegevens op de blockchain tot het minimum.

5.4.12 Daarbij zij opgemerkt dat de hierboven beschreven stappen slechts een suggestie vormen en geenszins uitputtend zijn. Het is goed mogelijk dat ook andere technische oplossingen kunnen worden aangewend om de verwerking van persoonsgegevens in een blockchain zoveel mogelijk in lijn te brengen met het beginsel van dataminimalisatie.

5.4.13 De in het licht van het beginsel van dataminimalisatie meest wenselijke ontwerpkeuze is dat geen persoonsgegevens in de transacties op de blockchain worden opgenomen. Dit kan bijvoorbeeld worden bewerkstelligd door gebruik te maken van links (pointers) op de blockchain naar off-chain persoonsgegevens, mits de links zelf ook geen

persoonsgegevens bevatten. Deze optie verdient aldus sterk de voorkeur. In het geval er toch persoonsgegevens worden verwerkt in de transacties op de blockchain, dan wel de link persoonsgegevens bevat, dienen de persoonsgegevens in ieder geval eerst gesalt en gehasht te worden voordat de persoonsgegevens in een transactie worden opgenomen.

5.4.14 Hieronder volgt een nadere toelichting.

I - Voorkom opslag van persoonsgegevens op de blockchain door het opnemen van links naar off-chain persoonsgegevens

5.4.15 Als gezegd leidt het plaatsen van persoonsgegevens op de blockchain ertoe dat niet-geautoriseerde gebruikers bij het gebruik van de blockchain bepaalde gehashte persoonsgegevens ontvangen, die zij buiten de blockchain nimmer zouden ontvangen en die bovendien niet noodzakelijk zijn voor de uitvoering van hun taken. Dit leidt tot een botsing met het beginsel van dataminimalisatie. Om dit te kunnen ondervangen en op die manier invulling te geven aan het beginsel van dataminimalisatie, verdient het sterk de voorkeur om persoonsgegevens off-chain op te slaan en on-chain een link naar de betreffende informatie op te nemen. Met andere woorden: de blockchain wordt gebruikt als een 'access control' grootboek.

5.4.16 Een goed voorbeeld uit de praktijk is het Microbiome center Nederland, dat via blockchain een keten faciliteert voor het analyseren van menselijke feces ten behoeve van het ontwikkelen van persoonsgerichte medicatie. Via de blockchain worden de arts, het laboratorium, de apotheek en de patiënt binnen een bepaald proces aan elkaar verbonden, in binnen- en buitenland.

5.4.17 Op de blockchain worden alleen sleutels voor de verschillende gebruikers gebruikt en gehashte pointers naar:

- Gegevens van de patiënt;
- Analyses van de arts;
- Rapporten van het laboratorium;
- Recepten van en voor de apotheek;
- Betalingen voor de geleverde services.

5.4.18 Hier wordt dus alleen verwezen naar de locatie van de data die persoonsgegevens bevatten, maar de eigenlijke data staat niet op de blockchain.[173]

5.4.19 Bijkomend voordeel van deze benadering, is dat het hierdoor makkelijker wordt om persoonsgegevens te verwijderen dan wanneer die gegevens op de blockchain zijn opgeslagen. De persoonsgegevens kunnen bij off-chain opslag immers uit het bronsysteem worden verwijderd waar de URL-link naar verwijst. Ook kan de URL-link naar de onderliggende persoonsgegevens worden doorgeknipt, waardoor het voor de

[173] Voor autorisaties van gebruikers geldt dat de autorisaties ofwel in het smart contract kunnen zijn opgenomen, ofwel buiten de blockchain kunnen worden opgeslagen.

geautoriseerde gebruikers niet meer mogelijk zal zijn om toegang te krijgen tot de persoonsgegevens en andere gegevens, waar die URL-link naar verwijst (dit wordt aangeduid als 'logic erasure').

Terzijde: in deze optie worden er (in beginsel) weliswaar geen persoonsgegevens op de blockchain zelf gezet, maar worden er wel op andere wijze persoonsgegevens verwerkt (die zijn immers te raadplegen via de URL). Dit betekent dat ook ten aanzien van die persoonsgegevens de regels uit de AVG in acht moeten worden genomen (tenzij de AVG niet van toepassing zou zijn, zie daarvoor deel I). Doordat er binnen deze optie (in beginsel)[174] geen persoonsgegevens op de blockchain zelf worden gezet, worden ook de privacyrechtelijke issues die inherent zijn aan het gebruik van de blockchain – zoals de vraag naar de grondslag van niet-geautoriseerde gebruikers om (gehashte) persoonsgegevens te verwerken – maximaal ondervangen.

II – Pseudonimiseer de (aanvullende) persoonsgegevens met een hash

5.4.20 Voor zover de doelstelling van de blockchain niet toestaat dat op de blockchain gebruik wordt gemaakt van een link naar off-chain opgeslagen persoonsgegevens, waarbij de link zelf ook geen persoonsgegevens bevat, kan het noodzakelijk zijn om persoonsgegevens in de transactie op te nemen. In dat geval dienen de persoonsgegevens in de transacties in ieder geval te worden gepseudonimiseerd door middel van het hashen en (bij voorkeur) ook salten ervan. De persoonsgegevens dienen alleen ontsleuteld te kunnen worden door de door geautoriseerde gebruikers. Uitgangspunt daarbij zal steeds moeten zijn dat de (bijzondere) persoonsgegevens in de transactie beperkt worden tot het strikt noodzakelijke. Bovendien moet worden geborgd dat de persoonsgegevens slechts met die geautoriseerde gebruikers worden gedeeld die daarover mogen komen te beschikken (zie deel IV). Zoals besproken in deel III, zal ervan uit moeten worden gegaan dat alle gebruikers, ook de gebruikers die slechts een hash zien omdat zij voor een bepaalde transactie niet geautoriseerd zijn, toch persoonsgegevens verwerken.[175] Voor deze niet-geautoriseerde gebruikers zal moeten worden vastgesteld op grond van welke wettelijke grondslag de verwerking plaatsvindt (wat zou kunnen worden ondervangen als die niet-geautoriseerde gebruikers zouden kwalificeren als verwerker).

5.4.21 Een vraag is nog in hoeverre de public keys van gebruikers of andere identifiers van gebruikers die (zo is reeds in deel II toegelicht) ook persoonsgegevens kunnen vormen over de gebruiker, in het licht van het dataminimalisatie-beginsel zouden moeten worden verwijderd. Het lijkt verdedigbaar dat het (nog) verder beperken van de verwerking van deze gegevens niet nodig is. Zo heeft de Franse privacy toezichthouder onderkend dat, gelet op het feit dat deze public keys en identifiers essentieel zijn voor het functioneren van de blockchain, het niet mogelijk is om deze gegevens verder te

[174] Belangrijke voorwaarde voor de conclusie dat het opnemen van een verwijzing niet leidt tot de verwerking van persoonsgegevens is dat bij het ontwerp van de blockchain wordt geborgd dat de URL-beschrijvingen geen persoonsgegevens bevatten. Zo dient bijvoorbeeld voorkomen te worden dat de link de naam van de patiënt bevat.
[175] Dat zal zeker het geval zijn als het door toekomstige ontwikkeling van de techniek (zoals toegenomen rekenkracht) mogelijk zou worden om hashes te kraken.

minimaliseren. De Franse privacy toezichthouder acht het in dit licht acceptabel dat de public key van gebruikers blijvend (zichtbaar) worden verwerkt in de transacties van de blockchain.[176]

III – Stel de standaardinstellingen van de blockchain af op een zo hoog mogelijk privacyniveau

5.4.22 Het verdient aanbeveling om de standaardinstellingen van de blockchain zo in te stellen dat een zo hoog mogelijk privacyniveau wordt verwezenlijkt, zonder dat dit noodzakelijkerwijs ten koste gaat van de functionaliteit van de blockchain. Meer concreet:

- ontwerp de blockchain zo dat transacties in beginsel altijd automatisch gepseudonimiseerd worden door het hashen of encrypten van de persoonsgegevens en dat deze standaardinstelling slechts kan worden opgeheven, indien en de verzendende gebruiker door middel van een actieve handeling andere gebruikers aanwijst die de inhoud van de transactie mogen raadplegen. Een dergelijke standaardinstelling komt de privacybescherming ten goede, aangezien hierdoor wordt voorkomen dat zomaar (ongehashte) persoonsgegevens op de blockchain worden gezet;
- (voor zover in algemene zin mogelijk en wenselijk) ontwerp het uploadscherm in de wallet van de gebruikers op een dusdanige manier dat gebruik wordt gemaakt van vaste informatievelden. Het hanteren van vaste informatievelden voorkomt dat gebruikers onnodig veel persoonsgegevens in een transactie opnemen;
- (voor zover in algemene zin mogelijk) stel de blockchain (technisch) zo in dat gebruikers slechts persoonsgegevens met andere gebruikers op de blockchain kunnen delen die daartoe wettelijk bevoegd zijn. Indien op voorhand kan worden vastgesteld dat twee gebruikers nimmer persoonsgegevens met elkaar mogen delen, omdat daarvoor een wettelijke grondslag ontbreekt, zouden de standaardinstellingen van de blockchain zo moeten zijn ingesteld dat de betreffende gebruiker ook niet de optie heeft om de persoonsgegevens met die onbevoegde gebruiker te delen.

5.4.23 Bovengenoemde maatregelen kunnen deels worden gerealiseerd door middel van een smart contract dat aan de blockchain ten grondslag ligt.

5.4.24 Een andere optie om uitvoering te geven aan het beginsel van dataminimalisatie is de inzet van ZKP. Bij deze techniek wordt er kort gezegd via de blockchain een claim (of attribuut) getoond (bijv. dat de patient ouder is dan 18), maar niet de informatie die daaraan ten grondslag ligt (bijv. de precieze leeftijd van de patiënt). Het uitwisselen van de onderliggende gegevens vindt plaats buiten de blockchain om via een directe

[176] Vgl. CNIL. 'blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data', 6 november 2018, p. 7.

beveiligde verbinding tussen de wallets van de gebruikers (door middel van een wallet to wallet verbinding). Kortom, op de blockchain worden in de transacties slechts zeer beperkt persoonsgegevens opgenomen (bijv. de public key van de gebruiker).

IV – Informeer de gebruikers van de blockchain over de wijze waarop zij zich bij het gebruik van de blockchain kunnen houden aan het beginsel van dataminimalisatie

5.4.25 In aanvulling op bovengenoemde technische oplossingen, zouden gebruikers van de blockchain kunnen worden geïnformeerd over de maatregelen die binnen de blockchain zijn getroffen om het dataminimalisatie-beginsel te waarborgen. Het enkel treffen van de hiervoor beschreven technische oplossingen zullen niet het gewenste effect sorteren indien de gebruikers van de blockchain er alsnog voor (kunnen) kiezen om persoonsgegevens (zonder enige vorm van hashing) op de blockchain te zetten. Ter voorkoming van dit risico kan de volgende maatregel worden getroffen:

- informeer de gebruikers door middel van een informatiedocument over de wijze waarop zij verantwoord (en in lijn met het beginsel van dataminimalisatie) gebruik kunnen maken van de blockchain, bijvoorbeeld door hen erop te wijzen dat (i) zij de inhoud van de transactie moeten beperken tot pointers en (ii) zij slechts gebruikers moeten autoriseren voor het raadplegen van de door hen te verzenden transacties, voor zover die gebruikers tot die raadpleging bevoegd zijn.

5.4.26 Deze instructie zou beschikbaar kunnen worden gesteld aan de gebruiker voordat deze persoonsgegevens via de blockchain verzendt (bijvoorbeeld via een pop-up in het uploadscherm).

V– Beperk ook de verwerking van additionele persoonsgegevens op de blockchain tot het minimum

5.4.27 Binnen een blockchain worden (additionele) persoonsgegevens verwerkt die niet zichtbaar zijn in de transacties, maar wel noodzakelijk kunnen zijn voor het functioneren van de blockchain. Hierbij kan gedacht worden aan:

- de persoonsgegevens die binnen de applicatie-laag van de blockchain worden verwerkt (waaronder het IP-adres van de gebruiker en de accountgegevens van de gebruiker in zijn of haar wallet);
- de persoonsgegevens die in het smart contract worden verwerkt met als doel het toekennen van autorisaties aan gebruikers;
- de persoonsgegevens die door de nodes op de blockchain worden verwerkt (bijvoorbeeld de persoonsgegevens die door de nodes worden gebruikt consensus te bereiken over het toevoegen van een nieuwe transactie).

5.4.28 Het beginsel van dataminimalisatie strekt zich ook uit tot de verwerking van deze niet in de transacties zichtbare additionele persoonsgegevens. Het gevolg daarvan is dat de verwerkingsverantwoordelijke ook de verwerking van additionele persoonsgegevens zo

veel mogelijk moet beperken tot het strikt noodzakelijke. Het voorgaande kan worden bewerkstelligd door bij het ontwerp van de blockchain (zoveel mogelijk) rekening te houden met de bescherming van de privacy van betrokkenen.[177] Voorbeelden van privacyvriendelijke ontwerpkeuzes zijn:

- het op zodanige wijze technisch instellen van de wallet van de gebruikers dat het IP-adres van de gebruikers niet wordt opgeslagen;
- het gebruikmaken van een smart contract waarin geen persoonsgegevens zijn opgenomen;
- het in plaats van het proof of work consensus-model gebruikmaken van proof of stake, zodat niet per transactie alle nodes (persoons)gegevens hoeven te verwerken om een nieuwe transactie aan de blockchain toe te voegen.

Ad (d) Juist en actueel

5.4.29 Verwerkingsverantwoordelijke gebruikers dienen bij het gebruik van blockchain maatregelen te treffen die waarborgen dat de persoonsgegevens die zij verwerken op de blockchain juist en actueel zijn. Dit volgt uit artikel 5, eerste lid, aanhef en onder d, AVG dat kort gezegd bepaalt dat persoonsgegevens juist moeten zijn en zo nodig moeten worden geactualiseerd.

5.4.30 Verwerkingsverantwoordelijke gebruikers moeten op grond van artikel 5, eerste lid, aanhef en onder d, AVG alle redelijke maatregelen nemen om persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren. De geautoriseerde gebruiker die op de blockchain persoonsgegevens plaatst, moet ervoor zorgdragen dat deze persoonsgegevens juist en nauwkeurig zijn. Mochten gegevens toch onjuist zijn, dan dienen de gegevens te kunnen worden gerectificeerd of gewist. Daar wordt in paragraaf 6.4 van dit deel nader op ingegaan.

Ad (e) Het beginsel van opslagbeperking

5.4.31 Bij het verwerken van persoonsgegevens in een blockchain zal daarnaast moeten worden gewaarborgd dat de persoonsgegevens niet langer worden bewaard dan noodzakelijk (het zogenoemde 'beginsel van opslagbeperking').

5.4.32 Artikel 5, eerste lid, aanhef en onder e, AVG bepaalt dat persoonsgegevens in een vorm die het mogelijk maakt de betrokkenen te identificeren niet langer worden bewaard dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt (artikel 5, eerste lid, aanhef en onder e, AVG). In diverse sectorale wetten worden specifieke bewaartermijnen genoemd. Deze specifieke bewaartermijnen gaan voor op de algemene bewaartermijn van de AVG. Gelet hierop, dienen verwerkingsverantwoordelijke gebruikers

[177] Zie in dit verband ook de bespreking van het beginsel van privacy by design & default (paragraaf 5.6 van dit rapport).

voorafgaand aan het verwerken van persoonsgegevens in een blockchain altijd te controleren of er voor de verwerking van de betreffende persoonsgegevens een specifieke bewaartermijn is geformuleerd in een sectorale wet. Voor blockchains in de zorg zullen onder andere de volgende bewaartermijnen van belang zijn[178]:

- **Wmo** - Op grond van artikel 5.3.4, eerste lid, Wmo geldt voor persoonsgegevens die door daartoe bevoegd partijen[179] in het kader van de uitvoering van de Wmo en Jw over een betrokkene worden verwerkt een bewaartermijn van (i) vijftien jaar te rekenen vanaf de tijdstip van ontvangst of vervaardiging van de persoonsgegevens of (ii) zoveel langer als redelijkerwijs in verband met de zorgvuldige uitvoering van hun taken op grond van de Wmo c.q. Jw noodzakelijk is.

- **Jw** - Op grond van artikel 7.3.8, derde lid, JW geldt voor het dossier van een jeugdhulpverlener een bewaartermijn van (i) vijftien jaar te rekenen vanaf het tijdstip van ontvangst of vervaardiging van de persoonsgegevens of (ii) zoveel langer als redelijkerwijs uit de zorg van een goed jeugdhulpverlener voortvloeit.

- **Wgbo** –De Wgbo bevat een bewaartermijn van vijftien jaar na het beëindigen van de behandelingsovereenkomst voor persoonsgegevens die in een medisch dossier over de patiënt worden verwerkt, te rekenen vanaf het tijdstip van vervaardiging, dan wel zoveel langer als redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit (artikel 7:454, derde lid, BW).

- **Archiefwet** – Instanties die gebonden zijn aan de Archiefwet zullen in aanvulling op de uit de AVG en de sectorale wetten voortvloeiende bewaartermijnen, op grond van de Archiefwet bepaalde bescheiden moeten archiveren. De Archiefwet geldt voor overheidsorganen[180] en verplicht hen om ten aanzien van bescheiden selectielijsten op te stellen waarin wordt toegelicht welke archiefbescheiden na welke periode voor vernietiging in aanmerking komen en welke bescheiden moeten worden bewaard.[181] Verschillende partijen binnen de zorg zijn gebonden aan de Archiefwet. Zo vallen onder meer de academische ziekenhuizen, het Centrum Indicatiestelling Zorg, de Inspectie voor de Gezondheidszorg, de Nederlandse Zorg Autoriteit, de Sociale Verzekeringsbank en gemeenten onder de

[178] Dit betreft geen uitputtende lijst, maar slechts een indicatie van mogelijk relevante bewaartermijnen. Gebruikers doen er verstandig aan om ook andere wetten te controleren op bijzondere bewaartermijnen die relevant zijn voor de persoonsgegevens die worden verwerkt.
[179] Het gaat hierbij om het college, zorgaanbieders, derden aan wie ten laste van een pgb betalingen worden gedaan, het CAK, bij gemeentelijke verordening aangewezen instanties die bevoegd zijn om een maatwerkvoorziening, dan wel een persoonsgebonden budget voor opvang vast te stellen en te innen, de Sociale verzekeringsbank, toezichthoudende ambtenaren en het advies- en meldpunt huiselijk geweld en kindermishandeling ('AMHK').
[180] Een overheidsorgaan in de zin van de Archiefwet is (i) een orgaan van een rechtspersoon die krachtens publiekrecht is ingesteld, of (ii) een ander persoon of college met enig openbaar gezag bekleed. Zie artikel 1, aanhef en onder b, Archiefwet.
[181] Zie artikel 5 van de Archiefwet.

reikwijdte van de Archiefwet.[182] De door deze partijen vastgestelde bewaartermijnen lopen zeer uiteen. Zo geldt voor openbare academische ziekenhuizen een bewaartermijn van het patiëntendossier van twintig jaar na de laatste behandeling of het overlijden van de patiënt en voor andere bescheiden (waaronder de ontslagbrief, het operatieverslag en het eerste hulp-verslag) een bewaartermijn van 115 jaar na de geboortedatum van de patiënt.[183]

Het voorgaande maakt dat overheidsorganen die gebruikmaken van blockchain moeten controleren of en zo ja, voor welke (persoonsgegevens in) archiefbescheiden die op de blockchain staan een op grond van de Archiefwet vastgestelde bewaartermijn geldt.

Op het moment dat het niet meer noodzakelijk is om persoonsgegevens te verwerken – omdat bijvoorbeeld de door de sectorale wet voorgeschreven bewaartermijn is verlopen – zullen persoonsgegevens na het verlopen van de bewaartermijn verwijderd moeten worden.

5.4.33 Evenals het beginsel van dataminimalisatie brengt ook het beginsel van opslagbeperking blockchain-specifieke privacy-uitdagingen met zich mee. De uit de algemene en bijzondere bewaartermijnen voortvloeiende verwijderingsplicht kan botsen met het onveranderlijke karakter van een blockchain. De vraag rijst of en zo ja op welke wijze invulling kan worden gegeven aan de verplichting persoonsgegevens te verwijderen. Hieronder zullen enkele (technische) suggesties worden gedaan om (zoveel mogelijk) uitvoering te geven aan bovengenoemde verwijderingsplicht.[184]

Suggesties voor het waarborgen van het beginsel van opslagbeperking op de blockchain

5.4.34 De volgende organisatorische en technische maatregelen zouden getroffen kunnen worden om uitvoering te geven aan het beginsel van opslagbeperking:

I. maak met de verwerkingsverantwoordelijke gebruikers (in de onderlinge regeling) heldere afspraken over de wijze waarop 'verwijdering' op de blockchain plaatsvindt;

[182] Zie voor een indicatie van de overheidsorganen die vallen onder de reikwijdte van de Archiefwet het door het Nationaal Archief beheerde overzicht van vastgestelde Basisselectiedocumenten en selectielijsten: https://www.nationaalarchief.nl/sites/default/files/field file/website_VASTGESTELDE_selectielijsten_per_05042018.pdf
[183] Vgl. Besluit vaststelling selectielijst neerslag handelingen beleidsterrein Openbare en bijzondere academische ziekenhuizen vanaf 1985.
[184] Daarbij zij opgemerkt dat de Europese privacy toezichthouders (de Franse toezichthouder uitgezonderd) nog geen richting hebben gegeven ten aanzien van de wijze waarop de verwijdering van persoonsgegevens op de blockchain moet plaatvinden om te kunnen voldoen aan de AVG. Er bestaat bij de hieronder beschreven suggesties aldus geen zekerheid dat met implementatie daarvan wordt voldaan aan de uit het beginsel van opslagbeperking voortvloeiende verwijderingsplicht na afloop van de bewaartermijn.

II. tref technische maatregelen die het mogelijk maken om zoveel mogelijk invulling te geven aan de (verplichte) verwijdering van persoonsgegevens op de blockchain;
III. neem op de blockchain een bevestiging op van de 'verwijdering';
IV. creëer een exportmogelijkheid voor geautoriseerde verwerkingsverantwoordelijken die zijn gebonden aan een archiefplicht.

5.4.35 Hieronder volgt een nadere toelichting

I– Maak met de verwerkingsverantwoordelijke gebruikers heldere afspraken over de wijze waarop 'verwijdering' op de blockchain plaatsvindt.

5.4.36 Het verdient allereerst aanbeveling dat de verwerkingsverantwoordelijke gebruikers van de blockchain afspraken met elkaar maken over de wijze waarop de verwijdering van persoonsgegevens op de blockchain wordt vormgegeven. Aan deze afspraken kan (deels) gevolg worden gegeven door middel van een aan de blockchain ten grondslag liggend smart contract. In de afspraken zou onder meer kunnen worden vastgesteld:

(i) welke gebruikers bevoegd zijn om persoonsgegevens op de blockchain te verwijderen[185] en daarover te beslissen;
(ii) op welke wijze verwijdering plaatsvindt (zie de hierna te bespreken opties);
(iii) op welke wijze gebruikers binnen de blockchain worden geïnformeerd over de (beoogde) verwijdering; en
(iv) of en zo ja, op welke wijze op de blockchain wordt opgenomen dat een verwijdering heeft plaatsgevonden.

5.4.37 De hierboven beschreven afspraken moeten worden opgenomen in de onderliggende regeling die de gezamenlijke verwerkingsverantwoordelijke gebruikers op grond van artikel 26 AVG moeten opstellen (zie deel II van dit rapport)

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

5.4.38 Zoals eerder toegelicht, leidt de onveranderlijkheid van de blockchain ertoe dat eenmaal in transacties toegevoegde persoonsgegevens niet meer verwijderd kunnen worden. Doordat de Europese privacy toezichthouders zich hierover nog niet hebben uitgelaten, is het momenteel onduidelijk of de verwerkingsverantwoordelijke, na het eenmaal plaatsen van persoonsgegevens op de blockchain, nog wel kan voldoen aan het vereiste om persoonsgegevens na het verlopen van de bewaartermijn (of bijvoorbeeld, als daar aanleiding toe is, op verzoek van de betrokkene) te verwijderen.

5.4.39 Het aan blockchain inherente probleem dat eenmaal geplaatste persoonsgegevens niet *kunnen* worden verwijderd, wordt niet weggenomen door het versleutelen en hashen

[185] Het ligt het meest voor de hand dat iedere verwerkingsverantwoordelijke gebruiker van de blockchain zelf moet kunnen beslissen of tot verwijdering van de door hem op de blockchain verwerkte persoonsgegevens moet worden overgegaan.

van persoonsgegevens die op de blockchain worden geplaatst. Versleutelde en gehashte persoonsgegevens zijn, zo wordt in dit rapport zekerheidshalve tot uitgangspunt genomen, immers nog steeds persoonsgegevens.

5.4.40 Het voorgaande maakt dat de verwerkingsverantwoordelijke (ook) (technische) maatregelen zal moeten treffen om tóch (zoveel mogelijk) invulling te kunnen geven aan de verplichting om persoonsgegevens te verwijderen. Of en zo ja, welke technische maatregelen getroffen kunnen worden door de verwerkingsverantwoordelijke om verwijdering te verwezenlijken, is sterk afhankelijk van het ontwerp van de blockchain.

5.4.41 Zoals hierna zal blijken, kan de volledige verwijdering van persoonsgegevens slechts plaatsvinden indien de gegevens op de blockchain zijn beperkt tot pointers naar off-chain persoonsgegevens die zelf ook geen persoonsgegevens bevatten.[186] Deze optie verdient dan ook sterk de voorkeur. Worden er toch persoonsgegevens over een betrokkene op de blockchain geplaatst, dan zou volledige verwijdering van de persoonsgegevens over die betrokkene in de blockchain kunnen worden bewerkstelligd als ervoor wordt gekozen per betrokkene (bijv. per patiënt/verzekerde) een persoonlijke blockchain te hanteren en deze persoonlijke blockchain vervolgens in zijn geheel te vernietigen. Voor zover slechts enkele persoonsgegevens over een betrokkene zouden moeten worden verwijderd, zullen slechts technische maatregelen kunnen worden getroffen die maken dat de inhoud van de betreffende transactie voor henzelf wordt gehasht en versleuteld (bijv. door middel van het weggooien of vernietigen van de aan de transactie gekoppelde sleutel). Nadat de verwijderende gebruiker het 'verwijderingsproces' heeft voltooid, zal deze, net als alle andere niet-geautoriseerde gebruikers, de inhoud van de (ontoegankelijk gemaakte) transactie niet meer kunnen raadplegen, maar slechts een hash van de inhoud van de transactie zien. Het is momenteel niet duidelijk of het op deze wijze voor (verwijderende) gebruikers onleesbaar maken van persoonsgegevens voldoende is om te kunnen spreken van verwijdering van persoonsgegevens in de zin van de AVG.

5.4.42 Hieronder volgt een nadere bespreking van de (technische) oplossingen afgestemd op het ontwerp van de blockchain.[187]

Situatie I – Op de blockchain zijn slechts verwijzingen opgenomen naar persoonsgegevens die off-chain staan opgeslagen

5.4.43 De (in het licht van het beginsel van opslagbeperking) meest wenselijke situatie is dat de transacties van de blockchain geen persoonsgegevens bevatten, maar slechts links (URL-pointers) naar persoonsgegevens die off-chain staan opgeslagen op de

[186] Bij deze opties vindt de feitelijke verwijdering van persoonsgegevens off-chain plaats.
[187] De hierna beschreven oplossingsrichtingen zijn niet uitputtend. Het is goed mogelijk dat ook andere technische oplossingen kunnen worden ingezet om zoveel mogelijk uitvoering te geven aan de onder meer uit het beginsel van opslagbeperking voortvloeiende verwijderingsplicht.

blockchain. Belangrijk voordeel van deze ontwerpkeuze is dat de verwijdering van de persoonsgegevens relatief gemakkelijk kan plaatsvinden.

5.4.44 De verwijdering van de persoonsgegevens kan plaatsvinden door de link naar de off-chain persoonsgegevens onbruikbaar te maken door de link naar de off-chain locatie van de persoonsgegevens door te knippen.[188] Het doorknippen van de link vindt off-chain plaats. Het effect daarvan is dat de persoonsgegevens niet langer door de geautoriseerde gebruikers via de blockchain kunnen worden geraadpleegd. De gebruikers van de blockchain zullen na verwijdering de pointer nog steeds kunnen raadplegen, maar ontvangen een foutmelding als ze op de pointer klikken. Doordat de pointer niet kan worden verwijderd uit de transactie, is het van belang dat bij het ontwerp van de blockchain wordt geborgd dat de URL-beschrijvingen geen persoonsgegevens bevatten.[189]

5.4.45 De verwerkingsverantwoordelijke dient zich tot slot te realiseren dat het onbruikbaar maken van de link uiteraard nog niet maakt dat de off-chain persoonsgegevens zijn verwijderd. Om dit te bewerkstelligen, dient de verwerkingsverantwoordelijke, in aanvulling op het onbruikbaar maken van de link, ook de off-chain persoonsgegevens te verwijderen.

Situatie II – Op de blockchain worden toch persoonsgegevens geplaatst

5.4.46 In het geval er toch persoonsgegevens worden geplaatst op de blockchain, dan wel de pointer persoonsgegevens bevat, is het niet meer mogelijk om de persoonsgegevens uit de transacties te verwijderen, tenzij er – als gezegd – voor gekozen zou worden om per persoon een blockchain te gebruiken en de gehele op die persoon betrekking hebbende blockchain zou worden verwijderd. Veelal zal echter de wens bestaan om tot verwijdering van *bepaalde* (persoonsgegevens in) transacties over te gaan. De geautoriseerde gebruiker die tot verwijdering van persoonsgegevens in bepaalde transacties over wil gaan kan dan slechts technische maatregelen treffen die maken dat de inhoud van de betreffende transactie ook voor hemzelf wordt gehasht en versleuteld (bijv. door middel van het weggooien of vernietigen van de aan de transactie gekoppelde sleutel). Nadat de verwijderende gebruiker het 'verwijderingsproces' heeft voltooid, zal deze ten aanzien van de ontoegankelijk gemaakte transactie voortaan handelen als een niet-geautoriseerde gebruiker. De verwijderende gebruiker zal, net als alle andere niet-geautoriseerde gebruikers, de inhoud van de (ontoegankelijk gemaakte) transactie niet meer kunnen raadplegen, maar zal slechts een hash van de inhoud van de transactie kunnen zien.

5.4.47 Het ontoegankelijk maken van de gehashte en versleutelde persoonsgegevens op de blockchain kan op verschillende manieren plaatsvinden, bijvoorbeeld door de

[188] Een voordeel van het gebruikmaken van pointers is dat de link niet slechts blijvend, maar ook tijdelijk onbruikbaar kan worden gemaakt. Dit kan een noodzakelijke maatregel zijn om invulling te geven aan het recht op beperking van de verwerking.
[189] Zo dient bijvoorbeeld voorkomen te worden dat de link de naam bevat van de patiënt op wie de gegevens betrekking hebben.

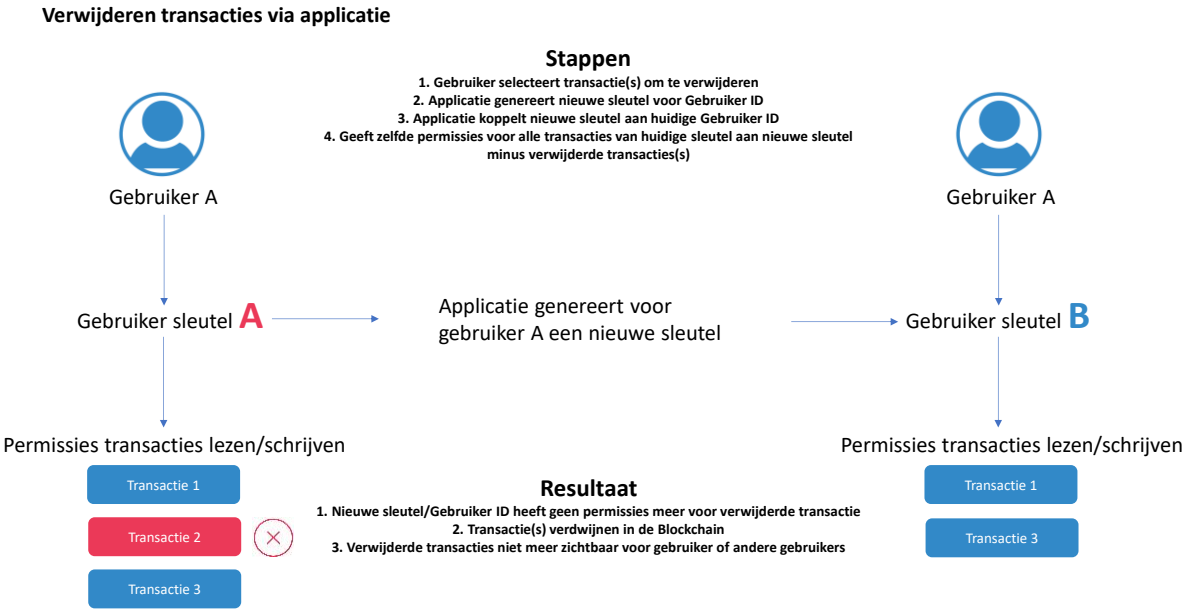
vernietiging van de private keys van de gebruikers (ook wel 'blacklisting' genoemd) via (i) de applicatie of (ii) het smart contract. Een variatie op de vernietiging van de private key via de applicatie of het smart contract is het door middel van het User Management ontkoppelen van de private keys van betrokkenen. Hieronder volgt een nadere toelichting.

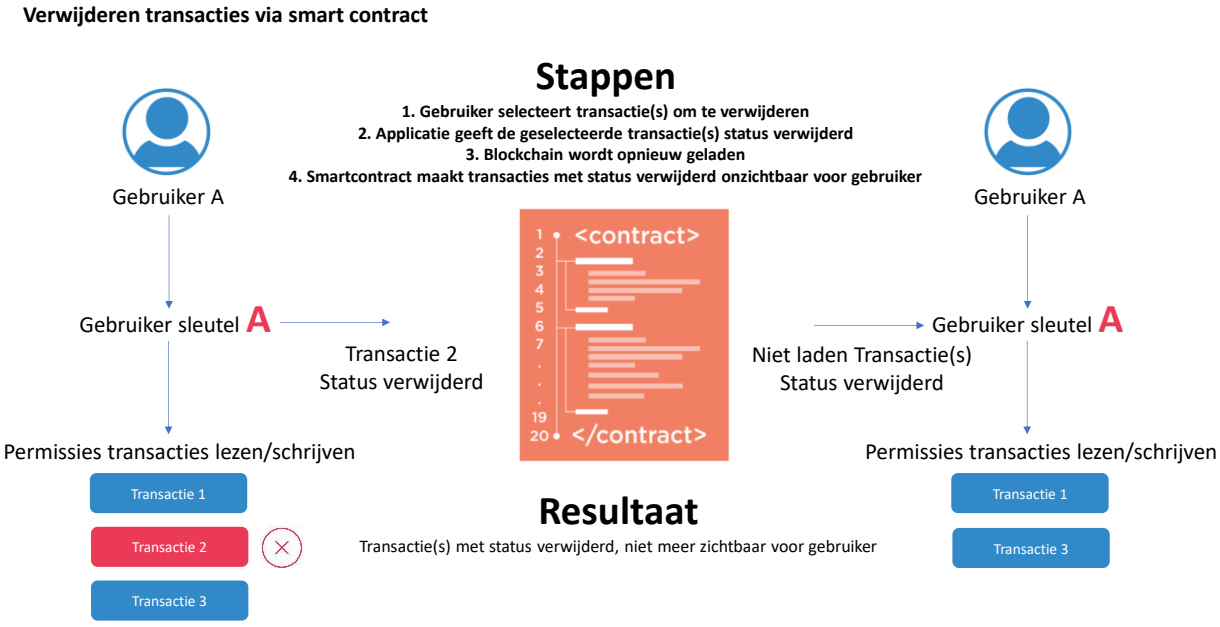
Ad (i) De vernietiging van de private keys door gebruikers

5.4.48 De persoonsgegevens die worden verwerkt in een transactie op de blockchain kunnen allereerst ontoegankelijk worden gemaakt door vernietiging van de private keys van de geautoriseerde gebruikers.

5.4.49 Zoals eerder toegelicht (deel II, randnr. 2.3.4) beschikt iedere gebruiker over een private key om de inhoud van een transactie te versleutelen en te ontsleutelen. De verstrekkende geautoriseerde gebruiker versleutelt de transactie door middel van een salt en een hash en autoriseert de ontvangende gebruiker(s) om de persoonsgegevens in de transactie te raadplegen. De ontvangende geautoriseerde gebruikers kunnen de gehashte persoonsgegevens in de transactie ontsleutelen met hun private key. Op het moment dat de private key van *iedere* geautoriseerde gebruiker wordt verwijderd en de gebruikers ook de off-chain persoonsgegevens verwijderen die corresponderen met de persoonsgegevens in de te verwijderen transactie(s), kan geen enkele gebruiker van de blockchain de betreffende transactie ontsleutelen. De geautoriseerde gebruikers veranderen in niet-geautoriseerde gebruikers en zien slechts een hash die in principe, uitgaande van een deugdelijke versleuteling, niet (meer) kan worden ontsleuteld.[190] Het verwijderingsproces kan plaatsvinden via de applicatie of via een smart contract. Hieronder volgt een schematische weergave van beide oplossingen.

[190] Behoudens eventuele toekomstige ontwikkelingen, zoals toegenomen rekenkracht.





5.4.50 De verwerkingsverantwoordelijken zullen (onder meer) de volgende maatregelen moeten treffen om tot een werkbaar 'verwijderingsproces' te komen:

(a) Bij het ontwerp van de blockchain – en meer specifiek de vormgeving van het sleutelbeheer en de versleuteling van transacties – zullen de verwerkingsverantwoordelijken moeten borgen dat iedere geautoriseerde gebruiker

per transactie een nieuwe private key krijgt toebedeeld waarmee hij de persoonsgegevens kan ontsleutelen.[191]

> De achtergrond van deze maatregel is als volgt. Bij het vormgeven van het sleutelbeheer hebben de verwerkingsverantwoordelijken de keuze om:
>
> (a) elke verwerkingsverantwoordelijke één private key te geven waarmee hij alle transacties binnen de blockchain kan ontsleutelen waarvoor hij is geautoriseerd, dan wel;
> (b) bij iedere transactie een nieuwe private key uit te geven aan de geautoriseerde gebruiker die door de verstrekkende gebruiker wordt geautoriseerd om de inhoud van die specifieke transactie te ontsleutelen.
>
> Het nadeel van optie (a) is dat een verwerkingsverantwoordelijke na het vernietigen van zijn sleutel geen enkele transactie meer kan raadplegen. Dit zou onwenselijk zijn. Het doel van het verwijderen van de sleutel is namelijk om de persoonsgegevens in één of meerdere transacties ontoegankelijk te maken ('gedifferentieerde verwijdering'). Het gedifferentieerd verwijderen van private keys zal slechts mogelijk zijn indien overeenkomstig optie (b) per transactie een nieuwe private key uit wordt gegeven aan de geautoriseerde gebruikers.
>
> Het voorgaande maakt dat, voor zover de verwerkingsverantwoordelijken gebruik willen maken van deze optie, de mogelijkheid van het gedifferentieerd verwijderen van private keys al tijdens de ontwerpfase moet worden ingebouwd in het sleutelbeheer en de versleuteling van de transacties.

(b) De verwerkingsverantwoordelijken gebruikers dienen daarnaast in de verwerkersovereenkomst de verplichting op te nemen dat de geautoriseerde verwerkers op verzoek van de verwerkingsverantwoordelijken hun private key voor de betreffende transacties(s) verwijderen.

Ad (ii) Het door middel van het User Management ontkoppelen van de gebruiker met zijn sleutel(s)

5.4.51 Een variatie op de vernietiging van de private key via de applicatie of het smart contract is dat de verwerkingsverantwoordelijke gebruikers ervoor kunnen kiezen om een super user aan te wijzen die het user management en het sleutelbeheer voert. De super user krijgt de bevoegdheid om – op verzoek van een 'verwijderende' geautoriseerde verwerkingsverantwoordelijke – alle aan de transactie gekoppelde private keys van zichzelf en van zijn eventuele geautoriseerde verwerkers te ontkoppelen. Door de ontkoppeling kunnen zij hun private key niet meer gebruiken.

5.4.52 Ook deze technische oplossing vereist dat de verwerkingsverantwoordelijken maatregelen treffen. Zo zullen de verwerkingsverantwoordelijken:

[191] Het per transactie uitgeven van een private key aan de geautoriseerde gebruikers heeft daarnaast een positief effect op de beveiliging van de blockchain.

(i) reeds tijdens de ontwerpfase de uitgifte van sleutels moeten koppelen aan een centrale user management;
(ii) een super user moeten aanwijzen die het beheer van het centrale user management en de verwijdering van private keys op zich neemt;
(iii) een protocol moeten opstellen over wanneer en onder welke voorwaarden de super user gehoor mag geven aan een verzoek om de private keys behorend bij een transactie te verwijderen, en tot slot;
(iv) moeten borgen dat de betreffende gebruikers ook de off-chain persoonsgegevens die corresponderen met de persoonsgegevens in de te verwijderen transactie(s) verwijderen.

5.4.53 Zoals gezegd, is het onzeker of de hierboven (achter randnrs. 5.4.46 e.v.) beschreven technische maatregelen voldoende zijn om te kunnen concluderen dat persoonsgegevens die op de blockchain zijn opgenomen, daadwerkelijk zijn verwijderd. Na het doorlopen van bovengenoemd proces zal op de blockchain uiteindelijk nog steeds een hash van de (salted en versleutelde) persoonsgegevens zijn opgenomen, echter zonder dat verwijderende gebruikers nog beschikken over een sleutel om die persoonsgegevens te raadplegen.

5.4.54 Uitgaande van de opinie van de artikel-29 Werkgroep over anonimiseringstechnieken, zullen de meeste Europese privacy toezichthouders vermoedelijk menen dat van de verwijdering van persoonsgegevens geen sprake is al zal daar in bepaalde gevallen discussie over mogelijk zijn. De opinie van de Franse privacy toezichthouder over blockchain biedt meer perspectief:

> "(…) another example is the deletion of the keyed hash function's secret key (…). Proving of verifying which information has been hashed would no longer be possible. In practice, the hash would no longer pose a confidentiality risk. Once again, the information would also need to be deleted in other systems where it has been stored for processing.
>
> (…) these solutions do not, stricly speaking, result in an erasure of the data, insofar as the data would exist in the blockchain. However, the CNIL observes that it does allow data subjects to get closer to an effective exercise of their right to erasure. Their equivalence for what concerns the requirements of the GDPR should be evaluated."[192]

5.4.55 Het is vooralsnog niet duidelijk of, en zo ja wanneer de Europese privacy toezichthouders nadere richting zullen geven over de vraag of het ontoegankelijk maken van de persoonsgegevens door het vernietigen van de sleutels en het ook off-chain verwijderen door de gebruikers van de persoonsgegevens die in de te verwijderen transactie(s) zijn opgenomen, een toelaatbaar alternatief vormt voor het verwijderen van persoonsgegevens op de blockchain.

[192] Vgl. CNIL, 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data', 6 november 2018, p. 7.

III –Neem op de blockchain een bevestiging op van de 'verwijdering'

5.4.56 Het verdient aanbeveling om op de blockchain een bevestiging op te nemen, zodat het voor de verwijderende gebruiker kenbaar is dat er gegevens uit de blockchain zijn 'verwijderd'. Het voorgaande geldt overigens eveneens voor zover de persoonsgegevens ontoegankelijk zijn gemaakt door het onbruikbaar maken van een link naar persoonsgegevens die off-chain staan opgeslagen.

5.4.57 De bevestiging van het ontoegankelijk maken van de persoonsgegevens of het onbruikbaar maken van de link naar de persoonsgegevens zou automatisch op de blockchain kunnen worden geplaatst. Zo zou in het smart contract kunnen worden ingeregeld dat na het weggooien van een sleutel of het ontoegankelijk maken van een link automatisch een transactie op de blockchain wordt opgenomen met daarin een verwijderingscode.[193] Voor de verwijderende gebruiker zal daarmee veelal direct duidelijk zijn dat hij in het verleden de inhoud van de transactie ontoegankelijk heeft gemaakt.[194]

IV – Creëer een exportmogelijkheid voor geautoriseerde verwerkingsverantwoordelijken die zijn gebonden aan een archiefplicht

5.4.58 Het verdient aanbeveling een exportmogelijkheid te creëren voor geautoriseerde verwerkingsverantwoordelijken die zijn gebonden aan een uit de Archiefwet voortvloeiende archiefplicht. Voor deze gebruikers is van belang dat zij de mogelijkheid hebben om voorafgaand aan de 'verwijdering' van de persoonsgegevens die gegevens naar hun eigen, interne archiefsysteem te exporteren. Daarmee wordt bewerkstelligd dat de geautoriseerde verwerkingsverantwoordelijken die gegevens nog wel overeenkomstig hun selectielijsten kunnen bewaren, maar niet meer actief via of op de blockchain hoeven te verwerken.

Ad (f) Beveiliging

5.4.59 Een belangrijke voorwaarde voor het gebruik van een blockchain in de zorg, is dat de blockchain voldoet aan de minimale beveiligingseisen die de AVG en de bijzondere, sectorale wetgeving stellen.

5.4.60 Artikel 5, eerste lid, aanhef en onder f, AVG bepaalt dat een verwerkingsverantwoordelijke door het nemen van passende technische en organisatorische maatregelen een passende beveiliging van persoonsgegevens dient te waarborgen, zodat de persoonsgegevens onder meer beschermd zijn tegen

[193] Hierbij kan gedacht worden aan een hash met daarin een bepaalde code waaruit voor de verwijderende gebruiker blijkt dat hij in het verleden deze transactie ontoegankelijk heeft gemaakt.
[194] De verwijderende gebruiker zal buiten de blockchain doorgaans een zelfstandige registratie bijhouden waaruit blijkt op grond van welk verwijderingsverzoek en met welke reden een transactie ontoegankelijk is gemaakt. In deze registratie kan de 'verwijderingscode' (zie de vorige voetnoot) van de ontoegankelijk gemaakte transactie worden gekoppeld aan het betreffende verwijderingsverzoek. Op die manier blijft voor de gebruiker inzichtelijk wat de achtergrond is geweest van het ontoegankelijk maken van een transactie op de blockchain.

ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

5.4.61 Daarnaast moet de verwerkingsverantwoordelijke, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te kunnen waarborgen.[195] Bij de beoordeling van het passende beveiligingsniveau dient met name rekening te worden gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens, hetzij per ongeluk hetzij onrechtmatig. Waar passend, omvatten de beveiligingsmaatregelen onder meer het volgende:

> a) de pseudonimisering en versleuteling van persoonsgegevens;
> b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
> c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
> d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.[196]

5.4.62 De hierboven beschreven algemene beveiligingsplicht maakt dat de verwerkingsverantwoordelijke gebruikers verplicht zijn om te waarborgen dat de blockchain voldoende is beveiligd. Bovendien moeten de verwerkingsverantwoordelijke gebruikers van de blockchain erop toezien dat de getroffen beveiligingsmaatregelen ook daadwerkelijk worden nageleefd. Het gaat het bestek van dit rapport te buiten om in detail te bespreken aan welke technische vereisten de beveiliging van een blockchain dient te voldoen. Bij het vaststellen van de beveiligingsmaatregelen zou aansluiting kunnen worden gezocht bij de Richtsnoeren Beveiliging van persoonsgegevens van de AP.[197]

5.4.63 Om bij het gebruik van een blockchain te komen tot een gepast beveiligingsniveau, zullen in ieder geval de volgende maatregelen moeten worden getroffen[198]:

I. Stel een beveiligingsplan voor de blockchain vast;

---

[195] Artikel 32 AVG.
[196] Artikel 32, eerste lid, AVG.
[197] https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_beveiliging_van_persoonsgegevens.pdf
[198] De hierna volgende opsomming van beveiligingsmaatregelen is niet uitputtend, maar vormt slechts een indicatie van de beveiligingsmaatregelen die bij het gebruik van de blockchain zouden moeten worden getroffen.

II. Waarborg dat degenen die als gebruiker inloggen op de blockchain ook daadwerkelijk bevoegd zijn om in te loggen;
III. Waarborg dat (medewerkers van) gebruikers die geen toegang meer nodig hebben tot de blockchain, daadwerkelijk geen toegang meer kunnen krijgen tot de blockchain;
IV. Stel een werkwijze vast om nieuwe gebruikers toegang te geven tot de blockchain en stel vast wie de toegang tot de blockchain verwezenlijkt;
V. Organiseer de encryptie, hashing en het sleutelbeheer van de blockchain;
VI. Maak met de verwerkingsverantwoordelijke gebruikers heldere afspraken over het verrichten van audits en het geven van uitvoering aan de resultaten van audits;
VII. Voer een evaluatie uit van het minimaal aantal nodes en miners dat nodig is om de beveiliging van de blockchain te waarborgen;
VIII. Stel technische en organisatorische maatregelen vast (waaronder een noodplan) om eventuele schade te beperken in het geval een gebrek wordt geconstateerd in de gehanteerde cryptografie;
IX. Implementeer de (aanvullende) specifieke beveiligingsverplichtingen die volgen uit de sectorale wetgeving;
X. Waarborg dat de (sub)verwerkers van de blockchain eveneens passende beveiligingsmaatregelen treffen.

5.4.64 Hieronder volgt een nadere toelichting.

I – Stel een beveiligingsplan van de blockchain vast

5.4.65 De gezamenlijke verwerkingsverantwoordelijken zullen allereest een beveiligingsplan moeten vaststellen waarin concrete beveiligingsmaatregelen zijn opgenomen over de beveiligde verbinding voor communicatie tussen nodes, de beveiliging van de node en de beveiliging van de gegevens op de node.

5.4.66 De gezamenlijke verwerkingsverantwoordelijken zullen de afspraken over hun respectievelijke verplichtingen ten aanzien van de uitvoering van de technische beveiliging van de blockchain moeten vastleggen in hun onderlinge regeling.

II – Waarborg dat degenen die als gebruiker inloggen op de blockchain ook daadwerkelijk bevoegd zijn om in te loggen

5.4.67 Een belangrijk aspect van de beveiliging van een blockchain, is dat er een controleproces bestaat voor de identiteit van gebruikers. Met dit controleproces kan worden geborgd dat degenen die toegang krijgen tot de blockchain ook daadwerkelijk bevoegd zijn om de persoonsgegevens op de blockchain te verwerken. Een dergelijk controleproces kan slechts plaatsvinden voor zover gebruik wordt gemaakt van een permissioned blockchain.

5.4.68 Een (nieuw) technisch middel dat voor de identificatie van gebruikers zou kunnen worden ingezet is het gebruik van Zero Knowledge Proof (‘ZKP’). Door middel van het

gebruik van ZKP kan een betrouwbare digitale identiteit worden ontwikkeld, bijvoorbeeld Self Sovereign Identity ('SSI').[199]

5.4.69 De identiteit van gebruikers zou tevens gewaarborgd kunnen worden door het gebruik van biometrie. Door gebruikers van de blockchain bijvoorbeeld te verplichten om door middel van een vingerscanner hun identiteit kenbaar te maken voordat zij toegang verkrijgen tot de blockchain kan met een zeer hoge mate van betrouwbaarheid de identiteit van een gebruiker worden vastgesteld. Dit zal uiteraard wel betekenen dat in het kader van de blockchain biometrische gegevens worden verwerkt waarvoor een doorbrekingsgrond in de zin van artikel 9 AVG moet bestaan. Zoals reeds toegelicht in deel III van dit rapport zal een dergelijke doorbrekingsgrond mogelijk gevonden kunnen worden in artikel 9, tweede lid, aanhef en onder g, AVG jo. artikel 29 UAVG.

III – Waarborg dat (medewerkers van) gebruikers die geen toegang meer nodig hebben tot de blockchain, daadwerkelijk geen toegang meer kunnen krijgen tot de blockchain

5.4.70 Een ander belangrijk aspect van de beveiliging van een blockchain is dat in het geval gebruikers geen toegang meer nodig hebben tot de blockchain, daadwerkelijk wordt geëffectueerd dat die betreffende gebruikers geen toegang meer tot de blockchain kunnen krijgen. Dit betekent dat de autorisaties moeten worden ingetrokken. Het lijkt raadzaam dat de verwerkingsverantwoordelijken in hun onderlinge regeling een partij aanwijzen die het intrekken van de autorisaties namens gebruikers op zich neemt.

IV – Stel een werkwijze vast om nieuwe gebruikers toegang te geven tot de blockchain en stel vast wie de toegang tot de blockchain verwezenlijkt

5.4.71 De verwerkingsverantwoordelijke gebruikers van de blockchain zullen gezamenlijk een werkwijze moeten vaststellen om nieuwe gebruikers toegang te geven tot de blockchain. Ook hier geldt dat het raadzaam is om een partij aan te wijzen die de vastgestelde toegangsprocedure namens aangesloten gebruikers uitvoert. De werkwijze zou als bijlage kunnen worden opgenomen in de onderlinge regeling die de verwerkingsverantwoordelijken op grond van 26 AVG met elkaar moeten aangaan (zie deel III van dit rapport).

V– Organiseer de encryptie, hashing en het sleutelbeheer van de blockchain

5.4.72 Een ander aspect waar de verwerkingsverantwoordelijken van de verwerkingen binnen de blockchain overeenstemming over zullen moeten bereiken is de encryptie- en/of hashingtechnieken die gebruikers van de blockchain hanteren voor de pseudonimisering van de persoonsgegevens op de blockchain. Gebruikers zouden daarbij bijvoorbeeld een keuze kunnen maken tussen de in deel II van dit rapport (randnr. 2.2.11) genoemde encryptietechnieken.

5.4.73 Een daarmee samenhangende verplichting is het maken van afspraken over het sleutelbeheer. De sleutels zullen in een goed beveiligde omgeving bewaard moeten

[199] Het gaat het bestek van dit rapport te buiten om uitgebreid stil te staan bij de werking van ZKP en SSI.

worden. Gebruikers kunnen concrete afspraken maken over de minimale beveiligingseisen waaraan de gegevensdrager waarop de sleutels worden opgeslagen moet voldoen.

5.4.74 Een belangrijk aspect van het sleutelbeheer is tot slot dat de verwerkingsverantwoordelijke gebruikers van de blockchain een werkwijze zullen moeten vaststellen voor het verlies van sleutels. De gebruikers zullen moeten waarborgen dat de beschikbaarheid en toegang van de persoonsgegevens na verlies van de sleutels tijdig wordt hersteld. Een oplossing daarvoor zou kunnen zijn dat gebruikers gebruikmaken van een super-user die de bevoegdheid heeft om vervangende sleutels uit te geven en de toegang tot de blockchain te herstellen. Uiteraard zal in dat geval de betreffende gebruiker opnieuw geautoriseerd moeten worden om de transacties ten aanzien waarvan hij geautoriseerd was, na terugkeer op de blockchain, wederom te kunnen inzien.

VI – Maak met de verwerkingsverantwoordelijke gebruikers heldere afspraken over het verrichten van audits en het geven van uitvoering aan de resultaten van audits

5.4.75 De AVG verplicht tot het periodiek controleren van het beveiligingsniveau van de blockchain. De geautoriseerde verwerkingsverantwoordelijken zullen met elkaar afspraken moeten maken over het verrichten van audits en het geven van uitvoering aan de uitkomsten van de audits. Ook deze afspraken dienen te worden opgenomen in de onderlinge regeling. Gelet op het mogelijk grote aantal geautoriseerde verwerkingsverantwoordelijken, zal het ook voor deze beveiligingsmaatregel raadzaam zijn om een partij aan te wijzen die het laten verrichten van audits en het gevolg geven aan de uitkomsten daarvan (in overleg) op zich neemt.

VII – Voer een evaluatie uit van het minimaal aantal nodes dat nodig is om de beveiliging van de blockchain te waarborgen

5.4.76 Het verdient aanbeveling om in het kader van de beveiliging van de blockchain een evaluatie te verrichten van het minimum aantal nodes dat nodig is om een passend beschermingsniveau te kunnen bieden voor de persoonsgegevens die op de blockchain worden verwerkt. In de praktijk wordt aangenomen dat een aantal van zes nodes voldoende is om een passend beschermingsniveau te bieden. Zorg ervoor dat het aantal nodes nimmer onder dit minimumniveau komt.

VIII – Stel technische en organisatorische maatregelen vast (waaronder een noodplan) om eventuele schade te beperken in het geval een gebrek wordt geconstateerd in de gehanteerde cryptografie

5.4.77 Het is mogelijk dat onverwachts een gebrek wordt geconstateerd in de door de blockchain gehanteerde algoritmes of de gehanteerde cryptografie. De Franse privacy toezichthouder heeft in zijn blockchain-rapport aanbevolen om in ieder geval een

noodplan te hebben opgesteld voor het geval een dergelijk incident zich voordoet.[200] Het doel van het noodplan is dat de gehanteerde algoritmes c.q. cryptografie voortvarend kunnen/kan worden gewijzigd om eventuele schade zo snel mogelijk te voorkomen of te beperken. De verwerkingsverantwoordelijke gebruikers van de blockchain zullen een dergelijk noodplan gezamenlijk moeten opstellen.

IX– Implementeer de (aanvullende) specifieke beveiligingsverplichtingen die volgen uit de sectorale wetgeving

5.4.78 Het is mogelijk dat de sectorale wetten – in aanvulling op de algemene beveiligingsplicht van de AVG – bijzondere (vaak strengere) beveiligingsverplichtingen stellen. Voor zover een dergelijke bijzondere beveiligingsplicht van toepassing is, zal de beveiliging van de blockchain ook aan deze voorwaarden moeten voldoen. Verwerkingsverantwoordelijke gebruikers van de blockchain doen er aldus verstandig aan om in het kader van de beveiliging van de blockchain te controleren of zij bij de verwerking van de persoonsgegevens zijn gebonden aan specifieke beveiligingsnormen en zo ja, deze ook te implementeren. Relevant voor onderhavig rapport is dat de Jw, de Wmo en de Wlz specifieke beveiligingsverplichtingen bevatten:

- op grond van de Jw en de Wmo moet de beveiliging van de verwerking van het BSN voldoen aan NEN-ISO-IEC 27001 en NEN-ISO-IEC 27002 of daaraan gelijkwaardige normen.[201]
- de Wlz schrijft een andere beveiligingsnorm voor. Op grond van de Wlz moet de beveiliging van de verwerking van het BSN voldoen aan de NEN 7510.[202]

Voor zover op de blockchain het BSN wordt verwerkt en de verwerking valt binnen de reikwijdte van de hierboven beschreven bepalingen, zal het beveiligingsniveau van de blockchain tevens moeten voldoen aan de hierboven beschreven beveiligingsnormen. Dit zal de implementatie van aanvullende organisatorische en technische maatregelen vereisen.

X– Waarborg dat de (sub)verwerkers van de blockchain eveneens passende beveiligingsmaatregelen treffen

Ook de (sub)verwerkers van de persoonsgegevens op de blockchain (waaronder de niet-geautoriseerde gebruikers van de blockchain) moeten passende beveiligingsmaatregelen treffen. De verwerkingsverantwoordelijke gebruikers moeten waarborgen dat de (sub)verwerkers aan de hiervoor beschreven beveiligingseisen voldoen. Die beveiligingseisen moeten worden opgenomen in een (sub)verwerkersovereenkomst die door gebruikers voorafgaand aan het eerste gebruik van de blockchain moet worden ondertekend. In aanvulling hierop zal regelmatig moeten worden gecontroleerd of de (sub)verwerkers aan de beveiligingseisen voldoen.

---

[200] Vgl. CNIL. 'blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data', 6 november 2018, p. 10.
[201] Zie artikel 7.2.1, eerste lid, Jw en artikel 7.2.4 jo. 7.2.5 Jw jo. artikel 6 Regeling Jw. Zie voor de Wmo in gelijke zin: artikel 5.2.9, zesde lid, Wmo jo. artikel 3 Uitvoeringsregeling Wmo.
[202] Artikel 9.1.1, vierde lid, Wlz jo. artikel 2 Regeling gebruik burgerservicenummer in de zorg.

5.5 De verantwoordingsplicht

5.5.1 Tot slot zullen de verwerkingsverantwoordelijke gebruikers van de blockchain moeten kunnen aantonen dat zij de hiervoor beschreven beginselen van de AVG bij het gebruik van de blockchain naleven. Dit volgt uit de in artikel 5, tweede lid, AVG opgenomen 'verantwoordingsplicht' die inhoudt dat een verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de in artikel 5, eerste lid, AVG genoemde beginselen voor de verwerking van persoonsgegevens (zie hiervoor) en moet kunnen aantonen dat hij deze beginselen naleeft. Artikel 24, eerste lid, AVG bepaalt in het verlengde daarvan dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen neemt om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Een van die maatregelen kan zijn dat de verwerkingsverantwoordelijke gegevensbeschermingsbeschermingsbeleid opstelt en uitvoert (artikel 24, tweede lid, AVG). Bij de vraag of en zo ja, welke maatregelen moeten worden genomen, houdt de verwerkingsverantwoordelijke rekening met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen. De maatregelen moeten worden geëvalueerd en indien nodig geactualiseerd. Een van de manieren om (deels) uitvoering te geven aan voorgaande eisen betreft het bijhouden van een verwerkingsregister (artikel 30 AVG).

5.5.2 De verantwoordingsplicht roept geen blockchain-specifieke privacyvragen op. Evenals bij verwerkingen die buiten de blockchain plaatsvinden, zal de verwerkingsverantwoordelijke moeten kunnen aantonen dat hij aan de AVG voldoet. De verwerkingsverantwoordelijke zal de verwerkingen die plaatsvinden binnen de blockchain moeten verantwoorden in zijn verwerkingsregister (voor zover hij op grond van artikel 30, eerste lid, AVG verplicht is tot het bijhouden daarvan). Ook de gebruiker van de blockchain die optreedt als verwerker zal overigens een register moeten bijhouden, zij het dat daarin minder informatie hoeft te worden opgenomen dan in het verwerkingsregister van de verwerkingsverantwoordelijke (artikel 30, tweede lid, AVG).

5.6 Privacy by design en privacy by default

5.6.1 Op grond van artikel 25 van de AVG dient een blockchain te voldoen aan de beginselen van *privacy by design* en *privacy by default*.

> **Privacy by design** houdt in dat reeds bij het ontwerpen van een nieuw of te wijzigen systeem waarmee gegevens worden verwerkt (zoals een blockchain) wordt nagedacht over de mogelijke privacyimplicaties die het systeem met zich mee kan brengen, zodat het systeem op een dusdanige wijze kan worden vormgegeven dat mogelijke privacyrisico's proactief voorkomen worden en dus al in een zo vroeg mogelijk stadium privacywaarborgende maatregelen worden getroffen. Door het beginsel van privacy by design na te leven wordt

privacybescherming geïntegreerd in het ontwerp van het nieuwe systeem of beleid. Doel daarvan is dat het risico op toekomstige privacy schendingen wordt verkleind.

5.6.2 Het naleven van de beginselen van privacy by design & default betreft een zeer algemene verplichting, waarbij de verwerkingsverantwoordelijken aan de hand van verschillende factoren een belangenafweging moeten maken ten aanzien van de technische en organisatorische aspecten van gegevensverwerkingen op de blockchain. Die factoren zijn (onder meer) de stand van de techniek, de uitvoeringskosten, de aard, de omvang, de context en het doel van de verwerking en de risico's (waarschijnlijkheid en ernst[203]) voor de rechten en vrijheden van de betrokkenen. Deze beoordeling vindt plaats voorafgaand aan het gebruik van de blockchain. Met inachtneming van die factoren zullen de verwerkingsverantwoordelijken bij het ontwerp van de blockchain passende technische en organisatorische maatregelen moeten hebben getroffen. Het doel daarvan is dat de in dit deel besproken gegevensbeschermingsbeginselen – zoals dataminimalisatie – op een doeltreffende manier worden toegepast en in het technische ontwerp van de blockchain de nodige waarborgen worden ingebouwd ter naleving van de voorschriften van de AVG en ter bescherming van de rechten van de betrokkenen (artikel 25, eerste lid, AVG).

5.6.3 Deze verplichting is het best te begrijpen als een zorgplicht van de verwerkingsverantwoordelijke om een zo beperkt mogelijke inbreuk op de persoonlijke levenssfeer te maken bij de verwerking van persoonsgegevens. Deze zorgplicht zal in verschillende contexten geconcretiseerd moeten worden, maar verschillende elementen worden al expliciet in de (toelichting bij[204]) de AVG genoemd: het minimaliseren van de verwerking van persoonsgegevens, het zo spoedig mogelijk pseudonimiseren van persoonsgegevens, het transparant maken van de functies en de verwerking van persoonsgegevens, het in staat stellen van de betrokkene om controle uit te oefenen op de informatieverwerking en het in staat stellen van de verwerkingsverantwoordelijke om beveiligingskenmerken te creëren en te verbeteren.

5.6.4 Ook dienen bij het ontwerp van de blockchain passende technische en organisatorische maatregelen te zijn getroffen om ervoor te zorgen dat slechts persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt ten aanzien van:

- de hoeveelheid verzamelde persoonsgegevens (zo min mogelijk);
- de mate waarin zij worden verwerkt (hoe minder vaak, hoe beter);
- de termijn waarvoor zij worden opgeslagen (hoe korter, hoe beter), en;
- de toegankelijkheid ervan (hoe minder mensen toegang hebben, hoe beter).

[203] Zie voor een concretisering hiervan de overwegingen 75 en 76 van de AVG.
[204] Zie ogebruikerverweging 78 van de AVG.

5.6.5 De vraag rijst hoe bij het ontwikkelen van een blockchain concreet uitvoering kan worden gegeven aan de beginselen van privacy by design en privacy by default. Hierna worden enkele suggesties gedaan[205]:

- omschrijf voorafgaand aan de bouw van de blockchain de gebruikers en het doel van de blockchain zodat duidelijk kan worden afgebakend welke persoonsgegevens strikt noodzakelijk zijn voor het bereiken van de gestelde doelstelling;

- breng voorafgaand aan het ontwerp van de blockchain de belangrijkste privacyrisico's in kaart door middel van het verrichten van een DPIA;

- waarborg dat het verzamelen, het gebruik en het bewaren van de (persoons)gegevens op de blockchain is afgestemd op het specifieke doel van de blockchain. Dit kan onder meer worden bereikt door de blockchain op een dusdanige wijze vorm te geven dat:

    - misbruik van de gegevens zoveel mogelijk wordt voorkomen, bijvoorbeeld door het automatisch hashen en versleutelen van persoonsgegevens en door het hanteren van een verfijnd autorisatieproces voor de toegang tot bepaalde links of persoonsgegevens op de blockchain;

    - er een 'verwijderingsproces' bestaat voor de gegevens op de blockchain.

- hanteer standaardinstellingen die borgen dat de gebruikers geen, dan wel zeer beperkt (persoons)gegevens op de blockchain kunnen verwerken. Hierbij kan gedacht worden aan:

    - het beperken van transacties op de blockchain tot links naar off-chain persoonsgegevens;
    - minimalisatie van eventuele persoonsgegevens die toch op de blockchain worden verwerkt (vgl. randnrs. 5.4.7 e.v. van dit rapport);
    - het standaard gebruik maken van hashing en pseudonimiseringstechnieken, zodat niet-geautoriseerde gebruikers geen inzage kunnen krijgen in persoonsgegevens die zij niet mogen verwerken;
    - het gebruik van vaste informatievelden;
    - het via het smart contract inregelen dat gebruikers slechts met specifieke gebruikers gegevens kunnen uitwisselen.

[205] De hierna beschreven maatregelen zijn deels gebaseerd op de door de CBP (thans AP) onderschreven Privacy Enhancing Technologies ('PET'). Zie Koorn et al, 'Privacy Enhancing Technologies', Ministerie voor Binnenlandse Zaken en Koninkrijksrelaties.

- hanteer instellingen waardoor bewaartermijnen worden bewaakt. Hierbij kan gedacht worden aan het hanteren van een bewaar- en vernietigingsprotocol dat wordt geëffectueerd door middel van een smart contract;[206]

- hanteer een sterke beveiliging met een verfijnde autorisatiestructuur waarbij gebruikers zelfstandig kunnen aangeven welke gebruikers geautoriseerd zijn om de inhoud van hun transactie(s) te raadplegen. Beveiling van de blockchain vormt een doorlopend aandachtspunt. De beveiliging moet actief worden gemonitord en (indien nodig) worden geactualiseerd gedurende de gehele levenscyclus van (de persoonsgegevens die in) de blockchain (worden verwerkt). Feitelijk houdt dit in dat uitvoering moet worden gegeven aan de maatregelen die reeds bij de bespreking van de beveiligingsvereisten zijn genoemd (zie paragraaf 5.4.60 e.v. van dit deel van het rapport);

- (eventueel) bescherm de toegang tot de blockchain door middel van het gebruik van een betrouwbare digitale identiteit of het gebruik van biometrie;

- geef de betrokkene zoveel mogelijk regie over zijn eigen persoonsgegevens, bijvoorbeeld door middel van het gebruik van SSI. De betrokkene krijgt daardoor beslissingsmacht over zijn persoonsgegevens en kan bepalen wanneer en aan wie hij zijn identiteit en andere persoonsgegevens bekend maakt. Daarbij zij benadrukt dat het voeren van het eigen beheer slechts zal leiden slechts tot hogere privacybescherming indien de betrokkene is geïnformeerd over hoe hij verantwoordelijk met zijn gegevens kan omgaan;

- geef de betrokkene inzicht in de wijze waarop persoonsgegevens op de blockchain worden verwerkt. Verwerkingsverantwoordelijke gebruikers van de blockchain dienen daar transparant over te zijn en proactief aan de betrokkenen informatie te verstrekken over de verwerking van hun persoonsgegevens op de blockchain. Meer concreet dienen de geautoriseerde verwerkingsverantwoordelijken:

    - een informatiedocument beschikbaar te stellen over de wijze waarop de blockchain werkt en welke privacybeschermende keuzes er zijn gemaakt bij het ontwerp van de blockchain;
    - de betrokkenen door middel van een privacyverklaring te informeren over de wijze waarop zij hun rechten kunnen uitoefenen;
    - een informatieprotocol op te stellen waarin is toegelicht op welke wijze gebruikers van de blockchain en betrokkenen tijdig worden

[206] Hierbij kan gedacht worden aan het hanteren van een tijdscode op de transacties, zodat zij na verloop van tijd overeenkomstig de geldende bewaartermijn automatisch ontoegankelijk worden gemaakt.

geïnformeerd over eventuele wijzigingen die in het ontwerp en de werking van de blockchain zullen worden doorgevoerd;
- op de blockchain te vermelden dat geautoriseerde gebruikers persoonsgegevens hebben 'verwijderd' of gerectificeerd.

- geef de blockchain zo vorm dat betrokkenen gemakkelijk hun rechten uit kunnen oefenen (recht op inzage, recht op rectificatie, recht op verwijdering, recht op beperking van de verwerking, recht op dataportabiliteit). Dit kan onder meer bewerkstelligd worden door:

  - een contactpunt of loket op te richten waar betrokkenen terecht kunnen met hun verzoeken;
  - de optie in te bouwen dat de betrokkenen zelf kunnen nagaan welke persoonsgegevens over hen worden verwerkt.

5.7 De meldplicht datalekken

5.7.1 De verwerkingsverantwoordelijken zullen bij eventuele datalekken[207] in specifieke gevallen verplicht zijn om deze te melden aan de AP en de betrokkenen.

5.7.2 Artikel 33 van de AVG ziet op de melding van een datalek aan de AP. Een datalek moet altijd gemeld worden, tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De melding moet zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat duidelijk is geworden dat sprake is van datalek, worden gedaan. Als dat niet lukt, moet in de melding worden gemotiveerd waarom dat zo is. Als het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan dat ook in stappen (zonder onredelijke vertraging). Het derde lid van artikel 33 AVG bevat informatie over wat moet worden gemeld:

a) de aard het datalek, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
b) de naam en de contactgegevens van de Functionaris Gegevensbescherming (FG) of een ander contactpunt waar meer informatie kan worden verkregen;
c) de waarschijnlijke gevolgen van het datalek;
d) de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om het datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

5.7.3 Op grond van het vijfde lid van artikel 33 AVG moeten alle inbreuken worden gedocumenteerd (inclusief feiten, gevolgen en getroffen rectificerende maatregelen).

[207] In de AVG wordt gesproken over een inbreuk in verband met persoonsgegevens. Dat is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (artikel 4 aanhef en onder 12 AVG). Er wordt gemakshalve gesproken van datalek.

De documentatie moet de AP in staat stellen de naleving van artikel 33 van de AVG te controleren.

5.7.4 Artikel 34 van de AVG bevat de verplichting om een inbreuk te melden aan de betrokkene als deze "waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen". De melding moet onverwijld worden gedaan. De inhoudelijke eisen aan de mededeling staan in het tweede lid van artikel 34 van de AVG: een omschrijving, in duidelijke en eenvoudige taal, van de aard van het datalek en daarnaast, tenminste, de informatie genoemd achter b, c en d hiervoor, zoals die ook aan de AP moet worden gemeld.

5.7.5 In het derde lid van artikel 34 van de AVG is opgesomd in welke gevallen geen mededeling aan de betrokkene hoeft te worden gedaan, namelijk als:

i) de gegevens zijn versleuteld of op een andere wijze onbegrijpelijk zijn gemaakt voor onbevoegden;
ii) achteraf maatregelen zijn genomen om ervoor te zorgen dat het (hoge) risico zich waarschijnlijk niet meer zal voordoen; of
iii) de mededeling een onevenredige inspanning zou vergen (maar dan moet een openbare mededeling worden gedaan of een soortgelijke maatregel worden getroffen).

5.7.6 Daarnaast hoeft geen melding aan de betrokkene te worden gedaan als zich een uitzonderingssituatie voordoet als bedoeld in artikel 23 AVG jo. artikel 41 UAVG. Evenmin hoeft een melding aan betrokkenen te worden gedaan door gebruikers die een financiële onderneming in de zin van de Wet op het financieel toezicht zijn (artikel 42 Uitvoeringswet AVG). In dat laatste geval moeten de gegevens over het datalek wel een jaar worden bewaard met als doel om:

- lering te trekken uit het datalek en uit de wijze waarop dit is afgehandeld;
- antwoord te kunnen geven op vragen van betrokkenen en anderen;
- het datalek alsnog aan de betrokkenen te melden als dat in eerste instantie achterwege is gelaten, maar de omstandigheden vereisen dat dit alsnog gebeurt.[208]

5.7.7 De hierboven beschreven meldplicht datalekken kan bij het gebruik van een blockchain specifieke vragen oproepen. Afhankelijk van de aard van het datalek zal moeten worden bezien welke partij de meest geschikte partij is om het datalek te melden. Zou een derde onbevoegd toegang krijgen tot alle persoonsgegevens op de blockchain, dan ligt het in de rede dat de verwerkingsverantwoordelijke gebruikers gezamenlijk een melding bij de AP doen of dat één van hen dat ook mede namens de overige verwerkingsverantwoordelijken doet waarvan persoonsgegevens zijn gelekt. Hierover moeten afspraken worden gemaakt. Dat geldt ook voor de vraag:

[208] Wij leiden dit af uit p. 46 van de al eerder genoemde Beleidsregels meldplicht datalekken van de AP.

i) hoe wordt omgegaan bij een verschil van mening over de vraag of sprake is van een datalek, of een datalek moet worden gemeld en zo ja, aan wie (AP en/of de betrokkene); en
ii) hoe en door wie wordt beslist welke maatregelen worden getroffen om schadelijke gevolgen en kans op herhaling te voorkomen, althans te beperken.

5.8 Data Protection Impact Assessment (DPIA)

5.8.1 Tot slot dient te worden vastgesteld of een DPIA moet worden uitgevoerd voordat de blockchain in gebruik kan worden genomen. Bij het gebruik van blockchain in de zorg zal deze verplichting vrijwel altijd gelden, omdat sprake is van de toepassing van een nieuwe technologie en mogelijk op grote schaal (bijzondere) persoonsgegevens en andere gevoelige gegevens worden verwerkt. Hieronder een nadere toelichting.

5.8.2 Op grond van 35, eerste lid, AVG moeten verwerkingsverantwoordelijken voorafgaand aan een verwerking een gegevensbeschermingseffectbeoordeling (DPIA) uitvoeren voor verwerkingen die een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen, in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt. Bij de beantwoording van de vraag of sprake is van een verwerking met een hoog risico spelen de aard, omvang, context en doeleinden van de verwerking een rol. Een DPIA houdt in dat het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens wordt beoordeeld.

5.8.3 Een DPIA is op grond van artikel 35, eerste lid, AVG (in ieder geval) verplicht bij:

- Grootschalige verwerking van bijzondere persoonsgegevens;
- Een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die gebaseerd is op geautomatiseerde verwerking, waaronder *profiling*, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen; of
- Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

5.8.4 Buiten deze drie situaties geeft de AVG geen overzicht van verwerkingen met een hoog risico. De Europese privacy toezichthouders hebben criteria opgesteld om het risico te bepalen.[209] Daarnaast heeft de AP (conform artikel 35, vierde en vijfde lid, AVG) een lijst op haar website gepubliceerd van verwerkingen waarvoor een DPIA verplicht is. Daarbij is aangesloten bij de door de Europese privacy toezichthouders geformuleerde criteria. Uitgangspunt is dat een DPIA verplicht is indien aan twee van de in de lijst genoemde criteria wordt voldaan.

[209] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dDPIA#in-welke-gevallen-moet-ik-een-dDPIA-uitvoeren-5879

5.8.5 De DPIA moet tenminste het volgende bevatten (artikel 35, zevende lid, AVG):

> a) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;
> b) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
> c) een beoordeling van de in het eerste lid bedoelde risico's voor de rechten en vrijheden van betrokkenen; en
> d) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

5.8.6 Daarnaast zal de verwerkingsverantwoordelijke de betrokkenen of hun vertegenwoordigers in voorkomend geval naar hun mening moeten vragen over de voorgenomen verwerking (artikel 35, negende lid, AVG).

5.8.7 Wanneer uit de DPIA komt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken en de verwerkingsverantwoordelijke van mening is dat het niet mogelijk is dat risico te beperken door middel van maatregelen die met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn, moet de verwerkingsverantwoordelijke voorafgaand aan de verwerking op grond van artikel 36, eerste lid, AVG de AP raadplegen (zie ook overweging 94 bij de AVG).

5.8.8 Van belang is tot slot dat de verwerkingsverantwoordelijke indien nodig een toetsing dient te verrichten om te beoordelen of de verwerking overeenkomstig de DPIA wordt uitgevoerd. Dat moet in ieder geval als sprake is van een verandering van het risico dat de verwerkingen inhouden (artikel 35, elfde lid, AVG).

6 TRANSPARANTIE & DE RECHTEN VAN DE BETROKKENE

6.1 Inleiding

6.1.1 De verwerkingsverantwoordelijke gebruikers van de blockchain zullen ook (aanvullende) technische en organisatorische maatregelen moeten treffen om de uitoefening van de rechten van de betrokkene mogelijk te maken. Het gaat daarbij om:

- het recht op informatie (artikelen 13 en 14 AVG);
- het recht op inzage (artikel 15 AVG);
- het recht op rectificatie (artikel 16 AVG);
- het recht op wissing (artikel 17 AVG)[210];
- het recht op beperking van de verwerking (artikel 18 AVG);
- het recht op dataportabiliteit (artikel 20 AVG) en tot slot;
- het recht op bezwaar (artikel 21 AVG).

6.1.2 In dit deel zal worden besproken of bovengenoemde rechten blockchain-specifieke privacy issues met zich meebrengen en zo ja, welke concrete maatregelen getroffen zouden kunnen worden om de uitoefening van deze rechten ten aanzien van verwerkingen van persoonsgegevens in een blockchain zo goed mogelijk te faciliteren. Evenals bij de bespreking van de voorgaande delen zal steeds per afzonderlijk recht worden belicht in hoeverre een sectorale wet specifieke (van de AVG afwijkende) rechten aan de betrokkene toekent.

6.1.3 Op alle hierboven genoemde rechten kan een uitzondering worden gemaakt. Soms gaat het daarbij om specifieke bij het recht behorende uitzonderingen. Voor zover dat het geval is, komen die bij de bespreking van het betreffende recht aan bod. Er zijn echter ook enkele uitzonderingen die voor alle genoemde rechten gelden. Die uitzonderingen worden aan het einde van dit deel besproken.

6.1.4 Tot slot zij hier nog opgemerkt dat de verwerkingsverantwoordelijke gebruiker onverwijld en in ieder geval binnen een maand na ontvangst van daarvan, gevolg moet geven aan verzoeken van betrokkenen die zijn gebaseerd op de artikelen 15 t/m 21 AVG. Bij complexe verzoeken of een groot aantal verzoeken kan deze termijn met twee maanden worden verlengd (artikel 12, derde lid, AVG). Als de verwerkingsverantwoordelijke gebruiker het verzoek afwijst, moet hij onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek aan de betrokkene meedelen waarom het verzoek zonder gevolg is gebleven (artikel 12, vierde lid, AVG). De verwerkingsverantwoordelijke gebruiker moet, alvorens een beslissing op het

[210] Het recht op wissing wordt ook wel aangeduid als het recht op vergetelheid.

verzoek te nemen, zorgen voor een deugdelijke vaststelling van de identiteit van de verzoeker als over die identiteit twijfels zouden bestaan (artikel 12, zesde lid, AVG).

6.2 Het recht op informatie

6.2.1 Op de verwerkingsverantwoordelijke gebruiker van de blockchain rust, enkele uitzonderingen daargelaten (zie daarover randnr. 6.2.4 e.v.), de verplichting om de betrokkene te informeren over de verwerkingen van persoonsgegevens die binnen de blockchain plaatsvinden (artikel 13 en 14 AVG). Meer concreet dient iedere verwerkingsverantwoordelijke gebruiker op grond van artikel 13 AVG de betrokkene te informeren over:

- diens identiteit en contactgegevens en, indien aan de orde, die van zijn vertegenwoordiger;
- in voorkomend geval, de contactgegevens van de functionaris gegevensbescherming;
- de doelen waarvoor de persoonsgegevens op de blockchain worden verwerkt en de rechtsgrond van de verwerking;
- (indien aan de orde) het gerechtvaardigd belang waarop de verwerking is gebaseerd;
- de (categorieën van) ontvangers[211];
- eventuele doorgiften van persoonsgegevens aan een derde land of een internationale organisatie[212];
- de bewaartermijn van de persoonsgegevens op de blockchain of, als dat niet mogelijk is, de criteria ter bepaling van die termijn;
- de rechten van de betrokkene;
- of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is, dan wel een noodzakelijke voorwaarde is om een overeenkomst te sluiten, en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;
- als de verwerking op toestemming is gebaseerd: dat de betrokkene het recht heeft de verleende toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan; en

[211] De term 'ontvanger' is gedefinieerd in artikel 4, aanhef en onder 9, van de AVG: "een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt". Daaronder vallen volgens de Artikel 29-Werkgroep onder meer: andere verwerkingsverantwoordelijken, gezamenlijke verwerkingsverantwoordelijken en verwerkers aan wie/waaraan gegevens worden doorgegeven of verstrekt. Hoewel dit volgens de Artikel 29-Werkgroep wel de voorkeur verdient, is het niet noodzakelijk om de ontvangers bij naam te noemen. Een verwerkingsverantwoordelijke kan volstaan met het noemen van de categorieën van ontvangers. De informatie over de ontvangers dient zo specifiek mogelijk te zijn door aanduiding van het type ontvangers (oftewel door vermelding van de activiteiten die die ontvangers verrichten) en de industrie, de sector, de subsector en de locatie van de ontvangers. Vgl. Artikel-29 Werkgroep, 'Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679', WP260 rev.01, p. 43.

[212] En ook aanvullende informatie hierover, zie de artikelen 13 en 14 AVG.

- (voor zover aan de orde) het bestaan van geautomatiseerde besluitvorming op de blockchain en nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

6.2.2 Als de persoonsgegevens niet van de betrokkene zelf zijn verkregen, moet de verwerkingsverantwoordelijke de betrokkene ook informeren over:

- de betrokken categorieën van persoonsgegevens; en
- de bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen.

6.2.3 Op grond van artikel 12 AVG moet de verwerkingsverantwoordelijke passende maatregelen nemen opdat de betrokkene bovenstaande informatie in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm verkrijgt en in duidelijke en eenvoudige taal. In de praktijk wordt de informatie vaak gegeven door middel van een schriftelijke privacyverklaring die fysiek of elektronisch aan de betrokkene wordt verstrekt.

6.2.4 Er zijn verschillende situaties waarin de betrokkene niet hoeft te worden geïnformeerd, namelijk als:

- de betrokkene al op de hoogte is van de informatie die anders verstrekt zou worden[213];
- het verstrekken van de informatie onmogelijk blijkt[214] of onevenredig veel inspanning[215] zou vergen, in het bijzonder bij verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden (deze uitzondering geldt alleen als de gegevens *niet* bij de betrokkene zijn verkregen)[216];
- het voldoen aan de informatieverplichting de doelen van de verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen (deze

[213] Zie artikel 13, vierde lid, AVG en artikel 14, vijfde lid, aanhef en onder a, AVG.
[214] Het verstrekken van informatie is volgens de Artikel-29 Werkgroep pas onmogelijk indien de verwerkingsverantwoordelijke kan aantonen "welke factoren hem of haar feitelijk verhinderen om de informatie in kwestie aan de betrokkene te verstrekken. (...) In de praktijk zullen er zeer weinig situaties zijn waarin een verwerkingsverantwoordelijke kan aantonen dat het feitelijk onmogelijk is om de informatie aan betrokkenen te verstrekken." Vgl. Artikel-29 Werkgroep, 'Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679', WP260 rev.01, p. 34.
[215] Uit Overweging 62 van de AVG volgt dat bij de beoordeling van de 'onevenredige inspanning' in aanmerking mag worden genomen om hoeveel betrokkenen het gaat, hoe oud de gegevens zijn en welke passende waarborgen worden ingebouwd. Een voorbeeld van een zorgspecifieke situatie waarin zich volgens de Artikel-29 Werkgroep een situatie van 'onevenredig veel inspanning' voordoet is de volgende. "Een groot hoofdstedelijk ziekenhuis vereist van alle patiënten, in verband met poliklinische behandelingen, ziekenhuisopname en afspraken, dat ze een patiëntinformatieformulier invullen, waarin wordt gevraagd om de gegevens van twee familieleden (betrokkenen). Gegeven het zeer hoge aantal patiënten dat dagelijks het ziekenhuis bezoekt, zou het van het ziekenhuis onevenredig veel inspanning vergen om alle personen die door patiënten als familielid op een patiëntinformatieformulier worden vermeld de door artikel 14 vereiste informatie te verstrekken." Vgl. Artikel-29 Werkgroep, 'Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679', WP260 rev.01, p. 35-36.
[216] Zie artikel 14, vijfde lid, aanhef en onder b, AVG. In dat geval moeten passende maatregelen worden genomen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie.

uitzondering geldt alleen als de gegevens *niet* bij de betrokkene zijn verkregen)[217];
- de vastlegging/verkrijging/verstrekking van de persoonsgegevens in nationaal of Europees recht is voorgeschreven en dat recht voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen (deze uitzondering geldt alleen alleen als de gegevens *niet* bij de betrokkene zijn verkregen));
- de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim (deze uitzondering geldt alleen alleen als de gegevens *niet* bij de betrokkene zijn verkregen)[218];
- zich een situatie voordoet als bedoeld in artikel 23 AVG jo. artikel 41 Uitvoeringswet AVG (zie paragraaf 6.7 van dit rapport).

6.2.5 Bovengenoemde informatieverplichting leidt in beginsel niet tot blockchain-specifieke privacyrechtelijke issues. Net als iedere andere verwerking die buiten de blockchain plaatsvindt, zullen de betrokkenen overeenkomstig artikelen 13 en 14 AVG moeten worden geïnformeerd over de verwerking van persoonsgegevens op de blockchain. Het verdient aanbeveling om maatregelen te treffen die borgen dat de privacyverklaring (en eventuele wijzigingen in de inhoud daarvan) tijdig - en bij voorkeur geautomatiseerd - aan de betrokkene wordt verstrekt. Meer concreet zouden verwerkingsverantwoordelijke gebruikers van een blockchain in de zorg de volgende maatregelen moeten / kunnen treffen:

- *(*verplicht) maak heldere afspraken met de verwerkingsverantwoordelijke gebruikers van de blockchain over de inhoud van de privacyverklaring, de wijze van het beschikbaar stellen daarvan en de procedure voor het wijzigen en actualiseren van de privacyverklaring. Neem deze afspraken vervolgens op in de onderlinge regeling die de verwerkingsverantwoordelijke gebruikers op grond van artikel 26, eerste lid, AVG moeten opstellen;
- (aanbeveling) hoewel dit niet volgt uit artikel 13 en 14 AVG, dient de wezenlijke inhoud van de onderlinge regeling aan de betrokkene beschikbaar te worden gesteld (artikel 26, tweede lid, AVG).[219] Het ligt voor de hand om de wezenlijke inhoud van de onderlinge regeling gelijktijdig met en op

[217] Vgl. Artikel-29 Werkgroep, 'Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679', WP260 rev.01, p. 37: "Om gebruik te kunnen maken van deze uitzondering moeten verwerkingsverantwoordelijken aantonen dat de verstrekking van de informatie van artikel 14, eerste lid, op zichzelf al de verwezenlijking van de doeleinden van die verwerking zou frustreren.".
[218] Het gaat bij deze uitzondering onder meer om het in deel III besproken medisch beroepsgeheim. Vgl. Artikel-29 Werkgroep, 'Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679', WP260 rev.01, p. 39: "Een beroepsbeoefenaar in de gezondheidszorg (verwerkingsverantwoordelijke) heeft een beroepsgeheim in verband met de medische gegevens van zijn patiënten. Een patiënt (ten aanzien van wie het beroepsgeheim van toepassing is) verstrekt de beroepsbeoefenaar in de gezondheidszorg informatie over haar gezondheid die verband houdt met een erfelijke aandoening waaraan ook enkele familieleden van haar lijden. Ook verstrekt de patiënt de beroepsbeoefenaar in de gezondheidszorg bepaalde persoonsgegevens van haar familieleden (betrokkenen) met diezelfde erfelijke aandoening. De beroepsbeoefenaar in de gezondheidszorg is niet verplicht om die familieleden de informatie van artikel 14 te verstrekken, omdat de uitzondering van artikel 14, vijfde lid, onder d), van toepassing is. Als de beroepsbeoefenaar in de gezondheidszorg de informatie van artikel 14 zou moeten verstrekken aan de familieleden, zou het beroepsgeheim ten aanzien van zijn patiënt worden geschonden."
[219] Zie voor een uitgebreide bespreking van het vereiste van het opstellen van een onderlinge regeling deel III, randnrs. 3.3.11 van dit rapport.

dezelfde wijze als de privacyverklaring aan de betrokkene beschikbaar te stellen;

- (verplicht) zorg dat de privacyverklaring tijdig en in ieder geval voorafgaand aan de verwerking van de persoonsgegevens op de blockchain aan de betrokkene beschikbaar wordt gesteld, bijvoorbeeld door opname van de privacyverklaring in de wallet van de betrokkene of door het opnemen van een downloadlink bij de inlogpagina van de betrokkene;
- (verplicht) zorg dat bij een eventuele wijziging in de privacyverklaring de betrokkene daarover wordt geinformeerd, bijvoorbeeld door middel van een alert of pop-up bij het eerstvolgende gebruik van de blockchain, zodat de betrokkene (automatisch) wordt geïnformeerd over de wijziging;
- (aanbeveling) informeer de betrokkene via de privacyverklaring – dan wel door middel van een apart informatiedocument – over het ontwerp en de werking van de blockchain, zodat de betrokkene zich een beeld kan vormen van de werking van de blockchain;
- (aanbeveling) informeer de betrokkene via het hiervoor bedoelde informatiedocument in het bijzonder over de rol van de (nodes van de) niet-geautoriseerde gebruikers op de blockchain;
- (aanbeveling) (voor zover een contactpunt voor de betrokkene is ingesteld) vermeld in de privacyverklaring hoe de betrokkene in contact kan treden met het contactpunt en welke procedures door het contactpunt worden gehanteerd.

6.3 Het recht op inzage

6.3.1 De verwerkingsverantwoordelijke gebruikers van de blockchain zullen maatregelen moeten treffen om de uitoefening van het recht op inzage van de betrokkene mogelijk te maken. De betrokkene heeft op grond van artikel 15 AVG het recht om van een verwerkingsverantwoordelijke gebruiker kosteloos uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens op de blockchain en, wanneer zijn gegevens worden verwerkt, het recht op inzage in die persoonsgegevens. De verwerkingsverantwoordelijke gebruiker moet in dat geval een kopie van de persoonsgegevens aan de betrokkene verstrekken en de volgende informatie verschaffen:

- de verwerkingsdoeleinden;
- de betrokken categorieën van persoonsgegevens;
- de (categorieën van) ontvangers;
- de bewaartermijn die wordt gehanteerd of, als dat niet mogelijk is, de criteria om die termijn te bepalen;
- de rechten van de betrokkenen;
- alle beschikbare informatie over de bron van de persoonsgegevens als deze niet bij de betrokkene zijn verkegen;

- het bestaan van geautomatiseerde besluitvorming en nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Specifieke inzagerechten in de sectorale wetgeving van de zorg

6.3.2 Bij blockchains in de zorg is het mogelijk dat een specifiek inzagerecht van toepassing is op de persoonsgegevens die op de blockchain worden verwerkt. Diverse sectorale wetten bevatten namelijk specifieke inzagerechten voor betrokkenen. Het verdient aldus aanbeveling om als verwerkingsverantwoordelijke gebruiker te controleren of een betrokkene een beroep kan doen op een specifiek inzagerecht. De reikwijdte van het specifieke inzagerecht kan afwijken van het algemene inzagerecht dat is opgenomen in de AVG (bijvoorbeeld het recht op bescheiden versus het recht op inzage in persoonsgegevens). Hieronder enkele (niet-uitputtende) voorbeelden:

- **Wmo** - artikel 5.3.2, eerste lid, van de Wmo bepaalt dat (onder meer) het college, een aanbieder, het CAK en de SVB desgevraagd zo spoedig mogelijk inzage in en afschrift van de bescheiden verstrekken waarover zij met betrekking tot de betrokkene beschikken, tenzij zich een van de in artikel 5.2.3 genoemde uitzonderingen voordoet;
- **Jw -** artikel 8.4.4, aanhef en onder a, Jw verklaart het uit artikel 5.3.2 Wmo voortvloeiende inzagerecht van overeenkomstige toepassing op de SVB voor zover de SVB taken verricht op grond van de Jw;
- **Jw** - artikel 7.3.10 Jw bepaalt dat de jeugdhulpverlener aan de betrokkene desgevraagd inzage in en afschrift van het dossier, of delen daarvan verstrekt. De verstrekking blijft achterwege voor zover dit noodzakelijk is in het belang van de bescherming van de persoonlijke levenssfeer van een ander;
- **Wgbo** - artikel 7:456 BW bepaalt dat een hulpverlener aan de patiënt desgevraagd inzage in en afschrift van de in artikel 7:454 BW genoemde bescheiden verstrekt. De verstrekking blijft achterwege voor zover dit noodzakelijk is in het belang van de bescherming van de persoonlijke levenssfeer van een ander.

6.3.3 Het inzagerecht brengt geen blockchain-specifieke issues met zich mee. De verwerkingsverantwoordelijke gebruikers moeten kunnen voldoen aan inzageverzoeken. Hoewel het gebruik van blockchain daarbij geen belemmering lijkt te vormen, kunnen wel verschillende vragen rijzen bij het verlenen van inzage in persoonsgegevens op de blockchain.

6.3.4 Een eerste vraag is op welke wijze een verwerkingsverantwoordelijke gebruiker moet omgaan met een inzageverzoek dat (deels) betrekking heeft op persoonsgegevens in transacties waartoe hij niet is geautoriseerd en die hij aldus niet kan zien (oftewel de

versleutelde en gehashte persoonsgegevens). De verwerkingsverantwoordelijke gebruiker zal hierin geen inzage hoeven te geven, omdat hij ten aanzien van die voor hem niet toegankelijke persoonsgegevens geen verwerkingsverantwoordelijke is (zie deel II).

6.3.5 Een ander vraag is op welke wijze aan een inzageverzoek moet worden voldaan als met pointers wordt gewerkt. In dat geval zal het allereerst raadzaam zijn om van de betrokkene een nadere specificatie te vragen van de reikwijdte van het verzoek:

- indien het verzoek van de betrokkene daadwerkelijk is beperkt tot zijn persoonsgegevens op de blockchain, dan zal het inzageverzoek kunnen worden afgewezen (mits uiteraard geen andere persoonsgegevens over hem op de blockchain worden verwerkt);
- indien het verzoek van de betrokkene (ook) betrekking heeft op de persoonsgegevens die buiten de blockchain om zijn uitgewisseld of raadpleegbaar zijn via de in de transacties opgenomen pointers, dan zal de verwerkingsverantwoordelijke gebruiker (ook) inzage moeten geven in die persoonsgegevens.

6.3.6 Tot slot zij nog opgemerkt dat het inzagerecht van de betrokkene met het gebruik van blockchain zou kunnen worden versterkt, in die zin dat deze aldus vormgegeven zou kunnen worden dat de betrokkene toegang heeft tot de blockchain en doorlopend alle hem betreffende persoonsgegevens die in of via de blockchain worden verwerkt kan raadplegen, of in ieder geval een deel daarvan.[220] Bijkomend voordeel hiervan is dat bij een eventueel inzageverzoek een verwerkingsverantwoordelijke gebruiker niet (nogmaals) een overzicht van de persoonsgegevens op de blockchain hoeft te verstrekken, maar kan volstaan met een verwijzing naar de transacties op de blockchain. Het gebruik van blockchain kan in dat geval leiden tot een lastenverlichting voor verwerkingsverantwoordelijken.

6.4 Het recht op rectificatie, het recht op wissing & het recht op beperking van de verwerking

6.4.1 In dit onderdeel wordt ingegaan op het recht op rectificatie, het recht op wissing en het recht op beperking van de verwerking. Alvorens die rechten te bespreken, volgen eerst enkele opmerkingen die voor ieder van de drie rechten gelden.

6.4.2 Het is raadzaam om in de onderlinge regeling afspraken te maken over:

i) welke verwerkingsverantwoordelijke een verzoek beoordeelt[221];
ii) hoe aan een verzoek uitvoering wordt gegeven[222]; en

[220] Voorstelbaar is dat er redenen zijn op grond waarvan inzage in bepaalde persoonsgegevens moet worden geweigerd.
[221] Het ligt het meest voor de hand dat de gebruiker bij wie een verzoek wordt gedaan dat verzoek ook beoordeelt, tenzij die gebruiker geen verwerkingsverantwoordelijke is.

iii) het bestaan van een doorzendplicht, die zou kunnen inhouden dat een gebruiker die een verzoek heeft ontvangen, maar onbevoegd is om daaraan uitvoering te geven, het verzoek doorstuurt naar de bevoegde verwerkingsverantwoordelijke gebruiker en de betrokkene daarvan in kennis stelt.

6.4.3 Daarnaast is van belang dat de verwerkingsverantwoordelijke iedere ontvanger in kennis moet stellen van elke rectificatie of wissing van persoonsgegevens of beperking van de verwerking, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt (artikel 19 AVG).[223]

> Voor zover het hierbij gaat om gebruikers binnen de blockchain zou deze kennisgeving, indien technisch mogelijk, ook via de blockchain gerealiseerd kunnen worden door een informatieve transactie over de rectificatie/wissing/beperking van de gegevens aan de blockchain toe te voegen, die zichtbaar is voor de gebruikers die eerder ook toegang hadden tot de onjuiste/gewiste/beperkte gegevens.

Ook moet de verwerkingsverantwoordelijke informatie aan de betrokkene verstrekken over de ontvangers als deze daar om verzoekt.

6.4.4 Hierna worden het rectificatie, wissings- en beperkingsrecht ieder afzonderlijk besproken. Daarbij zij opgemerkt dat zekerheid over de vraag of ten aanzien van persoonsgegevens op de blockchain inderdaad op deugdelijke wijze aan die rechten kan worden voldaan niet kan worden gegeven, nu de privacy toezichthouder zich hier (nog) niet eerder over heeft uitgesproken en daar ook (nog) geen rechtspraak over is.

Ad (a) Het recht op rectificatie (art. 16 AVG)

6.4.5 De betrokkene heeft op grond van artikel 16 AVG recht op rectificatie van onjuiste persoonsgegevens die een verwerkingsverantwoordelijke over hem verwerkt. Daarnaast heeft hij het recht op vervollediging van onvolledige persoonsgegevens. Een en ander voor zover zicht geen weigeringsgrond voordoet.

6.4.6 Ook de sectorale wetten kunnen een eigen rectificatierecht bevatten. Zo kennen de Jw en de Wmo de volgende bepalingen:

- **Wmo** - personen van wie de gegevens zijn opgeslagen hebben het recht om op grond van artikel 5.3.2, vijfde lid, Wmo onder meer het college, een aanbieder, een derde aan wie ten laste van een persoonsgebonden budget betalingen worden gedaan en de SVB te verzoeken de gegevens te laten rectificeren;

---

[222] Zie voor enkele technische mogelijkheden hiertoe de specifieke bespreking van de drie rechten hierna.
[223] Zie voetnoot 235 en 236 voor een nadere toelichting op de vraag wanneer het voldoen aan een verzoek 'onmogelijk' is of 'onevenredige inspanning' vergt.

- **Jw** - artikel 8.4.4, aanhef en onder a, Jw verklaart het uit artikel 5.2.3 Wmo voortvloeiende rectificatierecht van overeenkomstige toepassing op de SVB voor zover de SVB taken verricht op grond van de Jw.

6.4.7 Zoals toegelicht in deel IV van dit rapport, zal het daadwerkelijke wijzigen van persoonsgegevens in een transactie op de blockchain, gelet op het onveranderlijke karakter daarvan, onmogelijk zijn. De Europese privacy toezichthouders hebben nog geen richting gegeven over of en zo ja op welke wijze persoonsgegevens in een blockchain gerectificeerd kunnen worden. Verdedigbaar lijkt echter dat onjuiste persoonsgegevens in een eerdere transactie kunnen worden 'gerectificeerd' door een nieuw blok toe te voegen aan de blockchain (een zogenoemd 'rectificatieblok') met daarin:

(i) de mededeling dat een eerdere transactie onjuiste persoonsgegevens bevat en
(ii) een vermelding van de juiste persoonsgegevens.

6.4.8 Het toevoegen van een rectificatieblok zou, voor zover het ontwerp van de blockchain dit toelaat, gecombineerd kunnen worden met het ontoegankelijk maken van de transactie waarin de onjuiste persoonsgegevens zijn opgenomen, via de in deel IV, randnrs. 5.4.34 e.v. genoemde technische oplossingen. Op deze wijze kan (beter) worden geborgd dat bij toekomstige transacties de juiste persoonsgegevens van de betrokkene worden gebruikt.

Ad (b) Het recht op gegevenswissing (art. 17 AVG)

6.4.9 Op grond van artikel 17, eerste lid, AVG heeft de betrokkene recht op wissing van hem betreffende persoonsgegevens op de blockchain. De verwerkingsverantwoordelijke gebruiker is bij ontvangst van een dergelijk verzoek verplicht persoonsgegevens te wissen, onder meer indien zich één van de volgende situaties voordoet:

- de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- (als de verwerking op toestemming is gebaseerd en er is geen andere rechtsgrond voor de verwerking): de betrokkene trekt zijn toestemming in;
- de persoonsgegevens zijn onrechtmatig (bijvoorbeeld in strijd met artikel 5 AVG) verwerkt;
- de betrokkene maakt conform artikel 21 AVG bezwaar tegen een verwerking gebaseerd op artikel 6, eerste lid, aanhef en onder e of onder f, AVG en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking[224];

[224] Zie voor een bespreking van het recht op bezwaar paragraaf 6.6 van dit deel van het rapport.

- de persoonsgegevens moeten worden gewist om te voldoen aan een in het Unierecht of het lidstatelijk recht neergelegde verplichting die op de verwerkingsverantwoordelijke rust;
- de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij.

6.4.10 Als de verwerkingsverantwoordelijke gebruiker van de blockchain de persoonsgegevens die moeten worden gewist (eerder) openbaar heeft gemaakt, moet hij op grond van artikel 17, tweede lid, AVG redelijke maatregelen (waaronder technische maatregelen) treffen om andere verwerkingsverantwoordelijken die de persoonsgegevens (ook) verwerken ervan op de hoogte te stellen dat de betrokkene heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen. Bij het nemen van die maatregelen mag de verwerkingsverantwoordelijke rekening houden met de beschikbare technologie en de uitvoeringskosten.

6.4.11 Artikel 17, derde lid, AVG bevat uitzonderingsgronden op de in het eerste lid opgenomen verplichting om persoonsgegevens te wissen. Een verwerkingsverantwoordelijke is onder meer niet verplicht persoonsgegevens te wissen voor zover de verwerking van die persoonsgegevens nodig is:

i) voor het nakomen van een in het Unierecht of het lidstatelijke recht neergelegde wettelijke verwerkingsverplichting die op de verwerkingsverantwoordelijke rust;
ii) voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend;
iii) om redenen van algemeen belang op het gebied van volksgezondheid overeenkomstig artikel 9, tweede lid, aanhef en onder h en i, AVG en artikel 9, derde lid, AVG (zie deel III van dit rapport);
iv) met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, voor zover wissing de verwezenlijking van de doelen van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen.

6.4.12 Het wissen van persoonsgegevens in een blockchain vormt, zoals gezegd, een van de grootste (technische) uitdagingen van het gebruik van blockchain. Bij de bespreking van het beginsel van opslagbeperking is uitvoerig stilgestaan bij de (technische) maatregelen die verwerkingsverantwoordelijke gebruikers zouden kunnen treffen om persoonsgegevens in een blockchain (zoveel mogelijk) ontoegankelijk te maken. Voor een overzicht van de te treffen maatregelen wordt verwezen naar deel IV, randnrs. 5.4.38 e.v. van dit rapport).

Ad (c) Het recht op beperking van de verwerking (art. 18 AVG)

6.4.13 Tot slot heeft de betrokkene op grond van artikel 18, eerste lid, AVG het recht op beperking van de verwerking van zijn persoonsgegevens (op de blockchain). Beperking van de verwerking houdt in dat persoonsgegevens slechts mogen worden verwerkt, met uitzondering van de opslag ervan, met toestemming van de betrokkene of voor de instelling, uitoefening of onderbouwing van een rechtsvordering door de betrokkene of ter bescherming van de rechten van een ander natuurlijke persoon of rechtspersoon of om gewichtige redenen van algemeen belang voor de Unie of voor een lidstaat.
De verwerkingsverantwoordelijke moet overgaan tot het beperken van de verwerking indien een van de volgende situaties van toepassing is:

> a) de juistheid van de persoonsgegevens wordt betwist door de betrokkene, gedurende een periode die de verwerkingsverantwoordelijke in staat stelt de juistheid van de persoonsgegevens te controleren;
> b) de verwerking is onrechtmatig en de betrokkene verzet zich tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan;
> c) de verwerkingsverantwoordelijke heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
> d) de betrokkene heeft overeenkomstig artikel 21, eerste lid, bezwaar gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van de betrokkene.

6.4.14 Van een toereikende (technische) beperking van de verwerking slechts sprake indien de persoonsgegevens in de transacties zijn afgeschermd voor de gebruikers en persoonsgegevens nog slechts kunnen worden gebruikt voor de artikel 21 AVG genoemde doeleinden[225] Het voorgaande zou kunnen worden bewerkstelligd dooruit de blockchain te verwijderen overeenkomstig de in deel IV, randnummer 5.4.38 e.v. van dit rapport genoemde oplossingen. Mocht er op enig moment geen reden tot beperking van de verwerking meer zijn, dan zouden de persoonsgegevens opnieuw op de blockchain opgenomen kunnen worden.

6.4.15 Aangezien het geven van uitvoering aan een verzoek om beperkte kennisneming veel kan vragen van de betreffende verwerkingsverantwoordelijke gebruiker, lijkt het raadzaam om te bezien of bij het kiezen van een maatregel kan worden gedifferentieerd naar de te verwachten duur van de beperking van de verwerking. Hieronder volgt een nadere toelichting.

[225] Maatregelen die ertoe strekken dat (tijdelijk) geen nieuwe verwerkingen met de persoonsgegevens kunnen plaatsvinden zullen dus niet volstaan, omdat de persoonsgegevens in een dergelijk geval vaak nog steeds kunnen worden geraadpleegd.

6.4.16 De hierboven beschreven (technische) invulling van de beperking van de verwerking lijkt in ieder geval aangewezen in de situatie dat de plicht om de verwerking te beperken een langdurig karakter heeft. Het gaat daarbij om de volgende twee situaties:

- de verwerking is onrechtmatig en de betrokkene verzet zich tegen wissing van de persoonsgegevens en vraagt in plaats daarvan om beperking van het gebruik ervan.
- de verwerkingsverantwoordelijke gebruiker heeft de persoonsgegevens niet meer nodig, maar de betrokkene wel (namelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering).

6.4.17 Er zijn ook twee gevallen waarin het om een tijdelijke, kortere beperking zou kunnen gaan, namelijk zo lang als nodig is om:

(i) de juistheid van persoonsgegevens te controleren; of
(ii) een bezwaar te beoordelen.

In deze twee gevallen is het denkbaar dat eerst bij de betrokkene wordt nagegaan of deze ermee kan instemmen dat niet direct wordt overgegaan tot het extern opslaan en afschermen en daarna uit de blockchain verwijderen van de betreffende persoonsgegevens, maar dat prioriteit zal worden gegeven aan de afhandeling van het beperkingsverzoek.

6.5 Het recht op dataportabiliteit

6.5.1 Verwerkingsverantwoordelijke gebruikers van een blockchain zullen maatregelen moeten nemen zodat betrokkenen hun recht op overdraagbaarheid (ook wel het recht op dataportabliteit) uit kunnen oefenen ten aanzien van hun persoonsgegevens op de blockchain.

6.5.2 Artikel 20 AVG bepaalt dat de betrokkene het recht heeft om de hem betreffende persoonsgegevens die hij aan een verwerkingsverantwoordelijke heeft verstrekt in een gestructureerd, algemeen gebruikt en machinaal leesbaar formaat[226] te verkrijgen en

[226] De Artikel-29 Werkgroep (thans Europees Data Protection Board ('EOBD') heeft in de Richtlijn inzake het recht op gegevensoverdraagbaarheid nader toegelicht wat wordt verstaan onder 'een machinaal leesbaar formaat'. Vgl. Artikel-29 Werkgroep, Richtlijnen inzake het recht op gegevensoverdraagbaarheid van 5 april 2017, WP 242 (16/NL), p. 21: "Wanneer in een bepaalde bedrijfstak of gegeven context geen specifieke formaten gangbaar zijn, dienen verwerkingsverantwoordelijken de persoonsgegevens te leveren in gangbare open formaten (bv. XML, JSON, CSV) samen met nuttige metagegevens met een zo hoog mogelijke mate van gedetailleerdheid, en tegelijkertijd een hoge mate van abstractie te behouden. Bijgevolg moeten geschikte metagegevens worden gebruikt om de betekenis van uitgewisselde informatie zo accuraat mogelijk te beschrijven. Hierdoor zouden metagegevens moeten volstaan om de functie en het hergebruik van de gegevens mogelijk te maken, maar uiteraard zonder dat daarbij bedrijfsgeheimen worden onthuld. Het is dan ook onwaarschijnlijk dat een persoon zijn postbus met inkomende e-mails in pdf-versie leveren voldoende gestructureerd of beschrijvend zal zijn om de gegevens van het Postvak IN makkelijk opnieuw te kunnen

i) deze aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de eerstgenoemde verwerkingsverantwoordelijke en ii) om, indien dat technisch mogelijk is, die gegevens door die eerstgenoemde verwerkingsverantwoordelijke over te láten dragen. De betrokkene heeft dit recht alleen als:

- de verwerking berust op toestemming (artikel 6, eerste lid, aanhef en onder a, AVG / artikel 9, eerste lid, aanhef en onder a AVG) of op een overeenkomst (artikel 6, eerste lid, aanhef en onder b, AVG); en

- de verwerking via geautomatiseerde procedés wordt verricht (daarvan is in het geval van een blockchain sprake).

6.5.3 Het recht op overdraagbaarheid van de verwerking verplicht geautoriseerde gebruikers om een technische mogelijkheid te creëren om de persoonsgegevens uit de blockchain te exporteren in een gestructureerd, algemeen gebruikt en machinaal leesbaar formaat (zoals PDF).

6.6 Het recht op bezwaar

6.6.1 Als de persoonsgegevens op de blockchain worden verwerkt op grond van artikel 6, eerste lid, aanhef onder e en f AVG, kan de betrokkene daartegen op grond van artikel 21, eerste lid, AVG bij de verwerkingsverantwoordelijke gebruiker te allen tijde bezwaar maken vanwege met zijn specifieke situatie verband houdende redenen. De voor de verwerking verantwoordelijke gebruiker van de blockchain staakt de verwerking van de persoonsgegevens, tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.

6.6.2 Een voor de zorg relevante bepaling is bovendien artikel 21, zesde lid, AVG dat bepaalt dat wanneer persoonsgegevens met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt, de betrokkene het recht heeft om met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens, tenzij de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang.

6.6.3 Deze eis leidt niet tot blockchain-specifieke issues.

---

gebruiken. In de plaats daarvan moeten de e-mailgegevens worden geleverd in een formaat waarin alle metagegevens behouden blijven, zodat de gegevens efficiënt opnieuw kunnen worden gebruikt.”.

6.7 Uitzonderingen op de rechten van de betrokkene

6.7.1 Op grond van artikel 23 AVG kunnen uitzonderingen worden gemaakt op de rechten van betrokkenen (waaronder begrepen de informatieplicht). Deze uitzonderingen zijn uitgewerkt in artikel 41, eerste lid, Uitvoeringswet AVG:

> 1. De verwerkingsverantwoordelijke kan de verplichtingen en rechten, bedoeld in de artikelen 12 tot en met 21 en artikel 34[227] van de verordening, buiten toepassing laten voor zover zulks noodzakelijk en evenredig is ter waarborging van:
> a. de nationale veiligheid;
> b. landsverdediging;
> c. de openbare veiligheid;
> d. de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
> e. andere belangrijke doelstellingen van algemeen belang van de Europese Unie of van Nederland, met name een belangrijk economisch of financieel belang van de Europese Unie of van Nederland, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;
> f. de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
> g. de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
> h. een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de gevallen, bedoeld in de onderdelen a, b, c, d, e en g;
> i. de bescherming van de betrokkene of van de rechten en vrijheden van anderen[228]; of
> j. de inning van civielrechtelijke vorderingen.

6.7.2 De verwerkingsverantwoordelijke gebruiker van de blockchain zal zelf moeten afwegen of zich een of meer uitzonderingsgronden voordoen. Daarbij moet hij op grond van artikel 41, tweede lid, Uitvoeringswet AVG in ieder geval, voor zover van toepassing, rekening houden met:

> a. de doeleinden van de verwerking of van de categorieën van verwerking;

[227] Dit artikel ziet op de plicht om bepaalde datalekken aan de betrokkene te melden.
[228] Hieronder kan ook de verwerkingsverantwoordelijke worden begrepen. Mogelijk zou in bepaalde gevallen betoogd kunnen worden dat deze situatie zich voordoet ten aanzien van bepaalde de rechten van betrokkenen. De redenering zou dan moeten zijn dat als de hiervoor beschreven wijze van bijvoorbeeld rectificatie of verwijdering niet zou volstaan, dat tot gevolg zou hebben dat geen gebruik van blockchain zou kunnen worden gemaakt en het belang om dat wel te kunnen doen zwaarder weegt dan het belang van de betrokkene om zijn gegevens gerectificeerd resp. gewist te krijgen (op de wijze zoals deze dat kennelijk wenst).

b. de categorieën van persoonsgegevens;
c. het toepassingsgebied van de ingevoerde beperkingen;
d. de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte;
e. de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken;
f. de opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking; f
g. de risico's voor de rechten en vrijheden van de betrokkenen; en
h. het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking.

6.7.3 Tot slot dient te worden benadrukt dat ook de sectorale wetgeving specifieke uitzonderingsgronden kan bevatten. Verwerkingsverantwoordelijke gebruikers doen er aldus verstandig aan om bij verwerkingen die zijn gebaseerd op een wettelijke grondslag die is gelegen in een bijzondere wet te controleren of in de toepasselijke sectorale wet relevante uitzonderingsgronden zijn opgenomen, zodat vooraf bij het ontwerp van de blockchain en het toekennen van autorisaties kan worden vastgesteld hoe met deze uitzonderingen om zou moeten worden gegaan.

7 AFSLUITING

Blockchain kent veel juridische en technische uitdagingen. In dit rapport is toegelicht op welke wijze het gebruik van blockchain in de zorg in overeenstemming kan worden gebracht met de AVG. Het rapport kan als leidraad dienen voor juristen en informatiemanagers in de zorg die voornemens zijn gegevens via blockchain te verwerken. De conclusies en aanbevelingen in de dit rapport zullen ook relevant kunnen zijn voor blockchains buiten de zorg.

8 DISCLAIMER

Dit onderzoeksrapport is opgesteld voor en in opdracht van het Zorginstituut Nederland. Anderen dan het Zorginstituut Nederland kunnen aan dit onderzoeksrapport geen rechten ontlenen. Op dit rapport zijn de algemene voorwaarden van Pels Rijcken & Droogleever Fortuijn N.V. van toepassing, te raadplegen via https://www.pelsrijcken.nl/algemene-voorwaarden.