PELS RIJCKEN

CoE DSC

Whitepaper

Juridische aspecten van de inzet van Secure Multi-Party Computation (MPC)

Pels Rijcken & Droogleever Fortuijn N.V. | Postbus 11756 | 2502 AT Den Haag | +31 70 515 3000 | pelsrijcken.nl

Inhoud

1 INLEIDING

Secure Multi-Party Computation (MPC) is een technologie die het mogelijk maakt om data-analyse toepassingen op een privacy-vriendelijke manier uit te voeren. MPC stelt partijen in staat om berekeningen te doen met data van de partij, zonder dat de data van de ene partij bekend wordt bij de andere partij. Als gevolg daarvan kunnen partijen hun data beschikbaar stellen voor gezamenlijke analyses zonder dat zij de grip over hun data verliezen.

Binnen het publieke domein bestaat de wens om gebruik te maken van MPC. Bij veel publieke organisaties bestaat echter onzekerheid over de juridische toelaatbaarheid van het gebruik van MPC. Publieke organisaties vragen zich bijvoorbeeld af hoe de inzet van MPC zich verhoudt tot de vereisten uit het privacyrecht. In het bijzonder rijst vaak de vraag in hoeverre de inzet van MPC bij kan dragen aan de rechtmatigheid van het verder (voor andere doeleinden) verwerken van persoonsgegevens oorspronkelijk voor een ander doel zijn verzameld (zogenaamd 'meervoudig gebruik'). Wetgeving met betrekking tot gegevensbescherming, zoals de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) en diverse sectorspecifieke wetten, bevatten regels over dergelijk meervoudig gebruik van gegevens. Zo kent de Algemene wet inzake rijksbelastingen (AWR) een geheimhoudingsplicht en bevat de Participatiewet (Pw) een strikte doelbinding.

Dit *whitepaper* heeft tot doel de bij publieke organisaties bestaande juridische onzekerheid waar mogelijk weg te nemen. In dit *whitepaper* verkennen de juridische experts van het Innovation, Privacy & Technology (IP&T)-team van Pels Rijcken en technische experts van Linksight en de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO), in opdracht van de Nederlandse Gaia-X hub, inmiddels onderdeel van het zogenaamde Centre of Excellence for Data Sharing & Cloud, de juridische aspecten (in relatie tot de technische aspecten) van de inzet van MPC, gebaseerd op twee op de specifieke toepassingsvormen. Daarbij wordt ook ingegaan op de vraag of en, zo ja, welke juridische vereisten van invloed kunnen zijn op de inzet van fundamenten van MPC.

2 AANLEIDING

Linksight heeft in 2022 de Digicampus / Gaia-X Hackathon gewonnen met haar idee voor de inzet van MPC in data-analyses tussen het overheids- en gezondheidsdomein. Tijdens deze Hackathon zijn vragen gerezen over de toepasbaarheid van MPC in het publieke domein. Als prijs voor de winst bij het Hackathon heeft Linksight de mogelijkheid gekregen om input te leveren voor dit *whitepaper* over de inzet van MPC in het publieke domein. Uiteindelijk is dit *whitepaper* opgesteld door Pels Rijcken in opdracht van de Nederlandse Gaia-X hub, inmiddels onderdeel van het zogenaamde Centre of Excellence for Data Sharing & Cloud (www.coe-dsc.nl).

3 REIKWIJDTE

Voor een gedegen juridische analyse is het noodzakelijk om een concrete toepassing van MPC tot uitgangspunt te nemen. De uitkomst van deze juridische analyse is in sterke mate afhankelijk van de keuze voor een specifieke MPC-toepassing en de technische keuzes binnen het systeemontwerp. Gezien de grote hoeveelheid aan verschijningsvormen die MPC kent, heeft Linksight ervoor gekozen om twee specifieke decentrale[1] MPC-toepassingen tot uitgangspunt te nemen in dit *whitepaper*, namelijk een specifieke vorm van 'homomorfe encryptie' (in dit *whitepaper* ook wel "decentrale homomorfe encryptie" ('DHE')) en een specifieke vorm van 'secret sharing', namelijk een die is gebaseerd op een 'full threshold secret sharing scheme' (in dit *whitepaper* ook wel aangeduid als "secret sharing" ('SS')).[2] Bij de beschrijving van beide technieken hebben wij de technische instellingen en ontwerpkeuzes die normaliter door Linksight tot uitgangspunt genomen. Deze instellingen en ontwerpkeuzes worden in hoofdstuk 4 verder toegelicht.

Dit *whitepaper* is slechts bedoeld om inzicht te bieden in de algemene juridische vraagstukken die kunnen spelen bij de toepassing van de hiervoor beschreven vormen van MPC. Dit *whitepaper* bevat geen technische vergelijking van alle vormen van MPC die momenteel op de markt zijn. Dit *whitepaper* is aldus niet bedoeld als hulpmiddel voor een keuze in welke specifieke vorm van MPC het meest effectief, veilig en passend is voor uw project. Het valt in zoverre dus ook niet uit te sluiten dat andere vormen van MPC dan DHE of SS geschikter zijn voor uw beoogde project. Het is in dat licht van belang om bij ieder MPC-project kritisch te bezien welke MPC-toepassing in dat uw concrete geval het meest passend is.

De doelgroep van dit *whitepaper* zijn met name beleidsbepalers en beslissers bij publieke organisaties. In het taalgebruik is zoveel mogelijk geprobeerd om de complexe technische en cryptografische materie voor die doelgroep toegankelijk te maken, zodat daarmee voldoende basis ontstaat om de juridische analyse goed te doorgronden. Wij gaan in op de technische nuances van beide technieken voor zover die evident relevant zijn voor de juridische analyse.

Hoewel de juridische vraagstukken en conclusies in dit *whitepaper* in algemene zin zullen gelden voor *iedere* MPC-toepassing, valt niet uit te sluiten dat de keuze voor een andere MPC-toepassing of ontwerpkeuze leidt tot andere juridische uitkomsten. Het is in dat licht altijd van belang om kritisch te bezien of en zo ja, op welke aspecten uw MPC-toepassing verschilt met de MPC-toepassingen die centraal zijn gesteld in dit *whitepaper.*

---

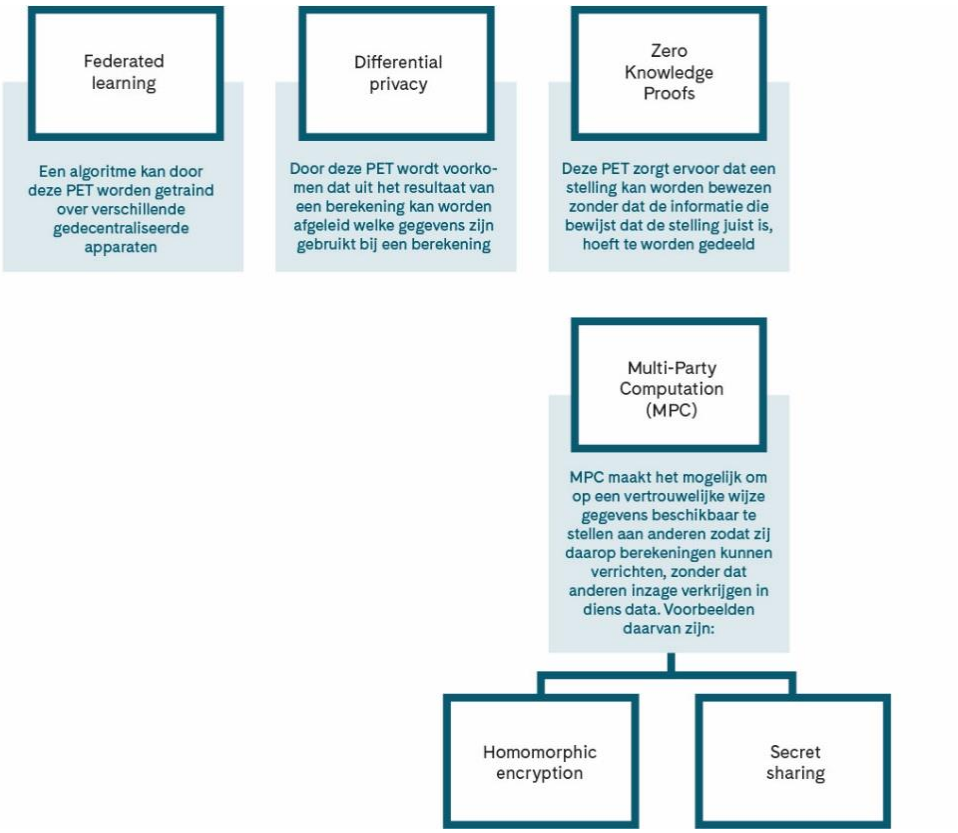
[1] Zie voor een nadere toelichting op het onderscheid tussen centraal en decentraal hoofdstuk 4 hierna.

[2] Daarbij geldt dat alle shares nodig zijn om tot een reconstructie te komen van de verschillende *shares*. Zie par. 4.2 van dit *whitepaper*.

Het concept van dit *whitepaper* is ter consultatie voorgelegd aan diverse marktpartijen die zich bezighouden met MPC. De input van deze marktpartijen is, waar nuttig en relevant, verwerkt in dit *whitepaper*. Na publicatie van dit *whitepaper* zal, onder meer met (een deel van) deze marktpartijen, worden bezien welke geschetste juridische vraagstukken een nadere analyse vereisen. Binnen dit vervolgtraject zullen ook andere toepassingsvormen van MPC en/of sub-technologieën in ogenschouw worden genomen.

4 MPC

MPC is een verzamelnaam van cryptografische technieken, die onderdeel zijn van het bredere palet *Privacy Enhancing Technologies* (PETs), waarmee organisaties op een privacyvriendelijke manier kunnen samenwerken op het gebied van data.

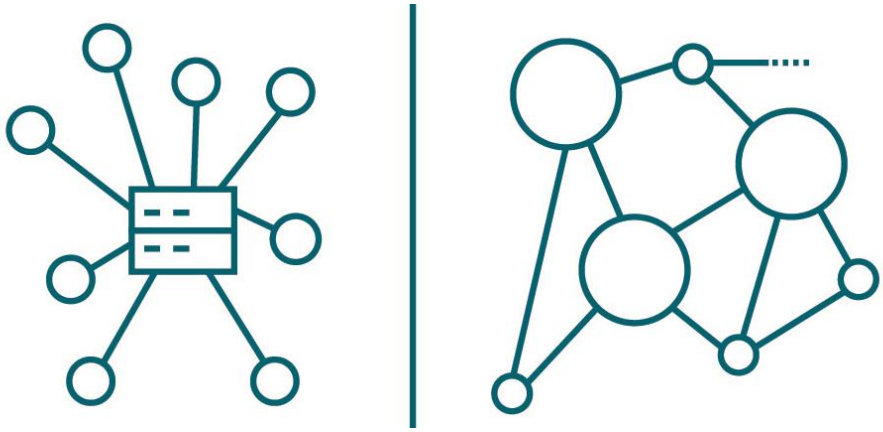


MPC maakt het daardoor mogelijk voor partijen om op een vertrouwelijke wijze aan elkaar gegevens beschikbaar te stellen zodat zij daarop berekeningen kunnen verrichten, zonder dat partijen inzage verkrijgen in elkaars data. In dit *whitepaper* gaan wij uit van de volgende definitie van MPC:

> "MPC is een 'gereedschapskist' met cryptografische technieken die het mogelijk maakt dat meerdere partijen gezamenlijk aan data kunnen rekenen, alsof ze een

gedeelde database hebben. Doordat de data op een cryptografische manier beschermd is, kan deze geanalyseerd worden zonder dat de partijen andermans data ooit kunnen inzien. De deelnemende partijen bepalen wie de uitkomst van de analyse mag inzien."

Voor de toepassing van MPC is het dus niet altijd nodig dat de data bij één partij worden ondergebracht (en dus centraal worden beheerd). Onder omstandigheden kan het mogelijk zijn dat bepaalde berekeningen op de data decentraal worden uitgevoerd. Data-eigenaren houden daardoor niet alleen controle over hun data maar ook over de berekeningen op hun data.



Centraal
Eén autoriteit is verantwoordelijk voor controle en verwerking van gegevens en transacties

Decentraal
Controle en validatie gebeurd door de 'nodes' knooppunten. Er is niet één controlerende autoriteit.

Welke techniek wordt toegepast, en of dat centraal of decentraal gebeurt, is afhankelijk van het specifieke geval en de gezochte oplossing; er is (nog) geen 'one-size-fits-all-oplossing'. Zoals gezegd, beperkt het *whitepaper* zich tot twee specifieke MPC varianten die decentraal worden toegepast, namelijk MPC die is gebaseerd op 'decentrale homomorfe encryptie' en MPC die is gebaseerd op 'secret sharing'. In het volgende hoofdstuk lichten wij de (technische) verschillen tussen deze twee specifieke decentrale vormen van MPC toe. Vervolgens zullen wij in hoofdstuk 5 bezien of en zo ja, welke specifieke juridische gevolgen een dergelijke keuze heeft.

4.1 *Decentrale homomorfe encryptie*

De decentrale homomorfe encryptie (DHE) maakt het mogelijk om analyses te maken op gegevens zonder de inhoud van die gegevens kenbaar te maken. Een homomorf

encryptieprotocol maakt gebruik van een publieke en een geheime sleutel. De publieke sleutel is bij iedereen bekend en kan door de partijen gebruikt worden om data te versleutelen. De versleuteling beschermt de onderliggende data en kan alleen met behulp van de geheime sleutel worden opgeheven. Deze geheime sleutel is niet of niet bij iedereen bekend. Een veel gebruikte aanpak is dat de geheime sleutel met behulp van *threshold* decryptie techniek wordt gesplitst over meerdere betrokken partijen, zodat niet één partij de gehele sleutel in handen heeft.

Alle partijen kunnen daarom hun eigen data versleutelen en de versleutelde data met een of meer andere partijen delen. De homomorfe eigenschap zorgt ervoor dat berekeningen op de versleutelde data kunnen worden uitgevoerd, zonder dat de data hoeven te worden ontsleuteld. De (tussen)resultaten van deze berekeningen kunnen de betrokken partijen wederom versleuteld met elkaar delen.

Voor de uitvoering van DHE is het niet altijd nodig om alle versleutelde data te delen. Slechts versleutelde (tussen)resultaten van de berekeningen die nodig zijn om de berekening af te maken hoeven gedeeld te worden. In sommige gevallen bestaan die (tussen)resultaten alleen uit bepaalde geaggregeerde informatie (zoals een som), in andere gevallen bestaan ze uit (een deel van) de versleutelde data zelf. Zoals gezegd, zijn de (tussen)resultaten zelf ook versleuteld. Pas als alle berekeningen zijn uitgevoerd wordt het antwoord, met behulp van de geheime sleutel(s), ontsleuteld. Stapsgewijs komt een analyse met behulp van de DHE – kort weergegeven – als volgt tot stand:

i. *Maken van afspraken*
De betrokken partijen maken afspraken over de versleuteling, de governance en de berekeningen, bijvoorbeeld welke methode voor koppeling wordt gehanteerd en over welke doelgroep data wordt gedeeld (ook wel 'overkoepelde populatie' genoemd).

ii. *Inladen van dataset naar een eigen data station*
Iedere betrokken partij beschikt over een lokale server die namens hen deelneemt in het netwerk dat wordt gebruikt voor de toepassing van DHE, ook wel het data station. De betrokken partijen laden ieder hun dataset in hun eigen data station.

iii. *Analyseverzoek wordt gedaan en geverifieerd*
Een betrokken partij kan vervolgens een analyseverzoek bij het eigen data station doen. Nadat door het data station is geverifieerd of de analyse is toegestaan (en dus in overeenstemming is met de in stap i. gemaakte afspraken), wordt deze doorgestuurd naar de andere data stations en ook door deze stations geverifieerd. Nadat alle data stations het analyseverzoek hebben

goedgekeurd, wordt de DHE door de data stations gestart.

iv. *Berekeningen worden een voor een door de data stations uitgevoerd*
De berekeningen door de DHE worden een voor een door de verschillende data stations doorlopen. In welke volgorde de data stations de berekeningen uitvoeren, is afhankelijk van de inhoud van het analyseverzoek. In ieder geval zorgt de DHE in deze toepassing ervoor dat de inputdata en de resultaten van de berekeningen van alle betrokken partijen homomorf worden versleuteld, waardoor deze geen direct leesbare informatie bevatten.

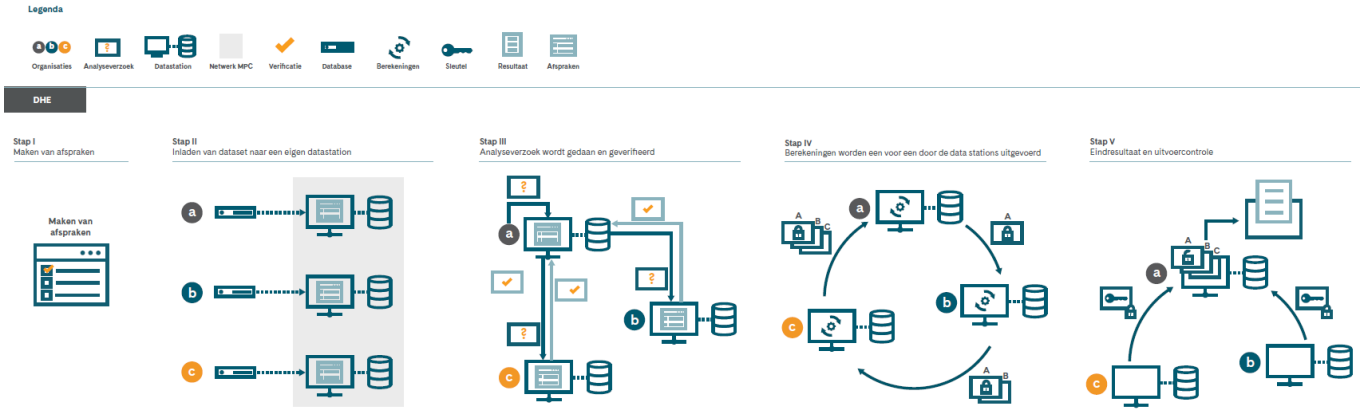
Kort en goed vindt het uitvoeren van de berekeningen door de data stations als volgt plaats. Het startende data station voert de op de DHE gebaseerde berekening uit op diens ingeladen dataset en deelt het tussenresultaat in homomorf versleutelde vorm met het opvolgende data station. Het opvolgende data station betrekt het ontvangen (homomorf versleutelde) tussenresultaat bij de (vervolg)berekening op diens ingeladen dataset. Het tussenresultaat van die vervolgberekening wordt door dit tweede data station vervolgens weer in homomorf versleutelde vorm met het daaropvolgende data station gedeeld.

De op de DHE gebaseerde berekeningen worden door ieder resterend data station doorlopen (en de tussenresultaten daarvan gedeeld) totdat het laatste data station wordt bereikt. Het laatste data station voert eveneens de op de DHE gebaseerde berekening uit op diens ingeladen dataset maar deelt het tussenresultaat niet – zoals de rest van de data stations heeft gedaan – met de andere data stations. Het laatste data station zal diens tussenresultaat (samen met de rest van de ontvangen tussenresultaten) gebruiken om te komen tot een eindresultaat.

v. *Het eindresultaat en de uitvoercontrole*
Pas aan het einde van het doorlopen van de DHE door het laatste data station, is het mogelijk om (door middel van een berekening) te komen tot een definitief resultaat. Dat definitieve resultaat is bovendien versleuteld en kan alleen gezamenlijk worden ontsleuteld. Met behulp van de *threshold* decryptie techniek is de geheime sleutel immers gesplitst over alle betrokken partijen, zodat niet één partij de gehele sleutel in handen heeft.

Op het ontsleutelde eindresultaat wordt vervolgens nog een uitvoercontrole toegepast. Als deze controle succesvol is, wordt het resultaat gedeeld met de partijen die dit volgens de gemaakte afspraken mogen ontvangen.[3]

[3] Zie **bijlage 1** voor een vergrote weergave van onderstaande afbeelding van de werking van SS.



4.2 *Secret sharing*

MPC op basis van secret sharing (SS) maakt het mogelijk data te delen en te analyseren zonder de inhoud van deze data kenbaar te maken. SS zorgt ervoor dat de inputdata van alle betrokken partijen wordt opgedeeld in meerdere stukjes, zgn. *shares*, die ieder afzonderlijk geen totaalbeeld van de oorspronkelijke data geven. Zonder de rest van de stukjes kan een betrokken partij één *share* ook niet terugbrengen tot de oorspronkelijke data.[4]

Iedere betrokken partij krijgt één *share* van een andere partij, waardoor alle betrokken partijen uiteindelijk beschikken over een set van *shares* waarop een berekening kan worden uitgevoerd. Deze *share*-set of de afzonderlijke tussenresultaten van de berekening op de *share*-set bevat – ieder afzonderlijk - ook geen oorspronkelijke data en kan ook niet teruggebracht worden naar de oorspronkelijke data. Pas als alle betrokken partijen de tussenresultaten samenbrengen kan daaruit iets worden afgeleid.

Stapsgewijs vindt een analyse met behulp van SS – kort weergegeven – als volgt plaats:

i. *Maken van afspraken*
De betrokken partijen maken afspraken over de versleuteling, de governance en de berekeningen, bijvoorbeeld welke methode voor koppeling wordt gehanteerd en over welke doelgroep data wordt gedeeld (ook wel de 'overkoepelde populatie' genoemd).

ii. *Datastations worden ingericht en analyseverzoek wordt gedaan en geverifieerd*
Er worden ten behoeve van SS minimaal drie servers ingericht die deelnemen in

[4] Zoals gezegd, kent secret sharing verschillende verschijningsvormen. Zo valt er een onderscheid te maken tussen lineair secret sharing en replicated secret sharing. Dit *whitepaper* ziet op een specifieke vorm van lineair secret sharing, namelijk op een lineair (arithmetische) secret sharing die is gebaseerd op een 'full threshold' secret sharing scheme, waarbij geldt dat alle shares nodig zijn om tot een reconstructie te komen van de verschillende shares.

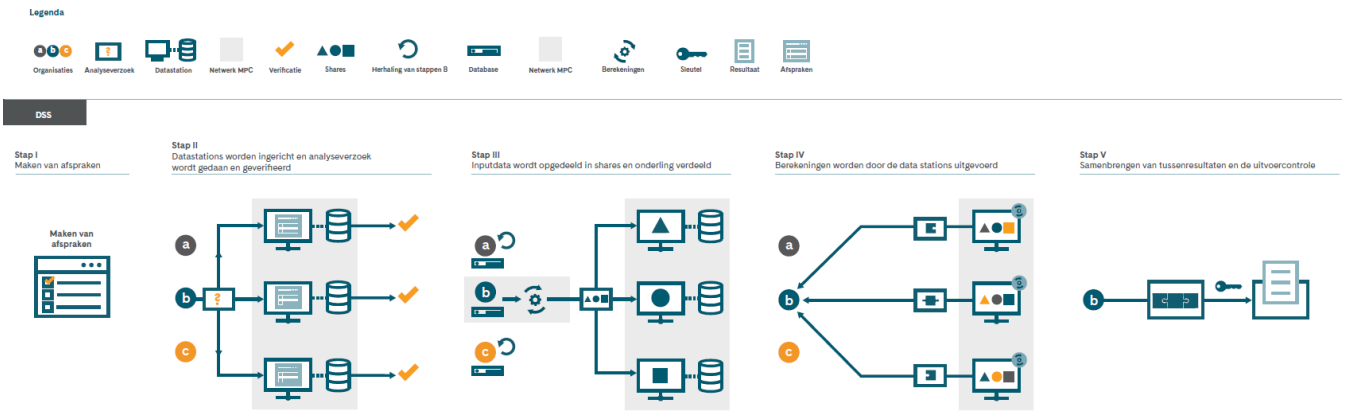
het netwerk dat wordt gebruikt voor de toepassing van SS, ook wel het data station. Een betrokken partij kan vervolgens een analyseverzoek bij een data station doen. Nadat door het data station is geverifieerd of de analyse is toegestaan (en dus in overeenstemming is met de in stap i. gemaakte afspraken), wordt deze doorgestuurd naar de andere data stations en ook door deze stations geverifieerd.

iii. *Inputdata wordt opgedeeld in shares en onderling verdeeld*
Nadat alle data stations het analyseverzoek hebben goedgekeurd, wordt SS door het data station gestart. De (benodigde) inputdata van de betrokken partijen wordt in deze toepassing door SS bij de betrokken partijen opgedeeld in afzonderlijke *shares* die geen informatie over de oorspronkelijke data bevatten (zie hierboven). Deze *shares* worden verdeeld tussen de drie (of meer) data stations en daarna door de betreffende deelnemers verwijderd, waardoor deze data stations (slechts) over een set van *shares* beschikken.

iv. *Berekeningen worden door de data stations uitgevoerd*
Op deze set van *shares* voert iedere betrokken partij vervolgens dezelfde berekeningen uit. Het tussenresultaat wordt vervolgens ook opgedeeld in afzonderlijke *shares.* Deze *shares* worden gedeeld met de daartoe aangewezen betrokken partij.

v. *Samenbrengen van tussenresultaten en de uitvoercontrole*
De *shares* van de tussenresultaten worden door die aangewezen partij samengebracht om te komen tot een leesbaar eindresultaat.

Op het eindresultaat wordt vervolgens nog een uitvoercontrole toegepast. Als deze controle succesvol is, wordt het resultaat gedeeld met de partijen die dit volgens de gemaakte afspraken mogen ontvangen.[5]



[5] Zie **bijlage 2** voor een vergrote weergave van bovenstaande afbeelding van de werking van SS.

4.3 *Verschillen tussen DHE en SS*

De wijze waarop gegevens worden gedeeld en gebruikt ten behoeve van berekeningen verschilt aldus bij DHE en SS. Bij DHE is het mogelijk om te kiezen voor een protocol waarbij de betrokken partijen steeds één voor één berekeningen uitvoeren en de tussenresultaten daarvan homomorf versleuteld gedeeld worden met de navolgende betrokken partijen, waardoor sprake is van een soort treintje. Bij SS delen alle betrokken partijen hun inputdata op in *shares* die worden verdeeld en gebruikt voor berekeningen. Doordat één set van *shares* en het tussenresultaat van de berekening daarop niks zegt zonder de rest van de *shares* of tussenresultaten, blijft de inhoud geheim. Uit het hoofdstuk hierna zal blijken dat de voornoemde verschillen relevant kunnen zijn voor de te volgen route voor de toets aan relevante juridische vereisten.

5 Privacyrechtelijke vraagstukken bij de toepassing van MPC

In dit hoofdstuk worden een aantal relevante juridische vereisten uit de (U)AVG, de Algemene wet bestuursrecht (Awb) en sectorspecifieke wetten beschreven die van invloed kunnen zijn op de inzet van beide vormen van MPC. Voor zover mogelijk wordt daarbij ook ingegaan op de vraag of en, zo ja, in hoeverre het vanuit juridisch oogpunt verschil maakt of gebruik wordt gemaakt van DHE of SS.

5.1 *Is de (U)AVG van toepassing?*

Vanuit juridisch perspectief dient allereerst te worden vastgesteld of de AVG van toepassing is op de MPC-toepassing.

De AVG is van toepassing indien bij de toepassing van MPC persoonsgegevens worden verwerkt. De definitie van 'persoonsgegeven' is ruim. Het betreft alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, de zogenaamde betrokkene (art. 4 aanhef en onder 1 AVG). Zo zijn NAW-gegevens persoonsgegevens, maar geldt dat ook voor bijvoorbeeld locatiegegevens of IP-adressen.

> 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 persoonsgegeven over de andere natuurlijke persoon.[6] De omstandigheid dat de persoonsgegevens van overleden personen niet worden beschermd door de AVG, sluit overigens niet uit dat de verwerking van dergelijke gegevens via andere wettelijke regelingen wordt gereguleerd.
>
> Let op: het is mogelijk dat niet de AVG, maar een andere wet van toepassing is op de verwerking van de gegevens. Hierbij kan onder meer gedacht worden aan

[6] Zie overweging 27 van de considerans van de AVG.

de Wet politiegegevens (Wpg) die van toepassing is op de verwerking van persoonsgegevens die in het kader van de politietaak worden verwerkt.[7] Zie in gelijke zin de Wet justitiële en strafvorderlijke gegevens (Wjsg) die van toepassing is op de verwerking van (onder meer) justitiële en strafvorderlijke gegevens. Dit onderstreept het belang om aan de start van het MPC-project vast te stellen welke wetgeving daadwerkelijk van toepassing is. Gemakshalve gaan wij in het verdere vervolg van dit *whitepaper* uit van een SS- of DHE-project waarop de AVG van toepassing is.

Voor de vraag of sprake is van identificeerbaarheid moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij kunnen worden gebruikt door de partij of door derden om de persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken. Om uit te maken of van middelen redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren, 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.[8] Niet relevant is of die middelen daadwerkelijk worden ingezet. Van 'anonieme' gegevens is pas sprake indien de identificatie van de betrokkene bij de wet verboden of in de praktijk ondoenlijk is, bijvoorbeeld omdat zij – gelet op de vereiste tijd, kosten en mankracht – een excessieve inspanning vergt.

Alleen gegevens die daadwerkelijk niet meer tot individuele personen terug te herleiden zijn (re-identificatie), zullen kwalificeren als *anonieme gegevens* waarop de AVG niet (langer) van toepassing is. In dat geval is er, met andere woorden, geen sprake meer van een persoonsgegeven. Herleidbaarheid dient aldus onomkeerbaar te zijn uitgesloten. Wij benadrukken dat deze toets dient te worden verricht voor zowel de verstrekker als de ontvanger van de data. Het is niet uitgesloten dat voor de verstrekker van een dataset sprake is van 'gepseudonimiseerde gegevens', terwijl voor de ontvanger sprake is van anonieme gegevens.

Wij wijzen in dit verband op HvJ EU 26 april 3023, T-557/20, ECLI:EU:T:2023:219, waarin het Europese Hof van Justitie ('HvJ') oordeelt dat het enkele feit dat een verstrekker van een gepseudonimiseerde dataset beschikt over een pseudonimiseringsleutel onvoldoende is om te concluderen dat (ook) de ontvanger (Deloitte) van deze gepseudonimiseerde dataset 'persoonsgegevens' verwerkt. Een dergelijke dataset kan voor de ontvanger anoniem zijn. Om een en ander vast te stellen is volgens het HvJ een juridische en technische analyse vereist vanuit de positie van de ontvanger. Om te bepalen of de doorgezonden informatie voor specifiek de ontvanger persoonsgegevens betreffen, is het aldus noodzakelijk om je te verplaatsen in de positie van de ontvanger teneinde te bepalen of de aan de ontvanger toegezonden informatie voor hem betrekking op

[7] Zie artikel 1, aanhef en onder a, Wpg.
[8] Zie overweging 26 van de considerans van de AVG. Zie ook Hof van Justitie van de Europese Unie 19 oktober 2016, ECLI:EU:C:2016:779, C-582/14, par. 24 e.v.

> 'identificeerbare personen'. Er dient te worden onderzocht of de ontvanger over wettelijke (en in de praktijk uitvoerbare) middelen beschikt om toegang te krijgen tot de aanvullende gegevens die nodig zijn voor de heridentificatie.
>
> Eenzelfde analyse zal ook moeten worden verricht om vast te stellen of deelnemers aan de MPC-toepassing persoonsgegevens verwerken als zij data verstrekken of ontvangen door middel van MPC.

Er bestaat veel discussie over de vraag wanneer sprake is van anonieme gegevens. In de Europese rechtspraak en de opinies van de Europese Toezichthouders (de European Data Protection Board (EDPB)[9]) en de nationale toezichthouder (de Autoriteit Persoonsgegevens ('AP')) wordt aangenomen dat vrijwel nooit sprake is van anonieme gegevens. Vooralsnog hanteren de EDPB en de AP[10] tot uitgangspunt dat het vrij lastig is – lees: vrijwel onmogelijk - om tot volledige anonimiteit te komen. Zo kan geen van de in de opinie van de EDPB in 2014 geanalyseerde technieken leiden tot volledige anonimiteit, aldus de EDPB:[11]

> "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."[12]

Van het verwerken van persoonsgegevens is op grond van art. 4 aanhef en onder 2 AVG onder meer sprake bij het verzamelen, vastleggen, ordenen, structureren en opslaan van persoonsgegevens.

---

9 Voorheen was de EDPB de Artikel 29-Werkgroep.

10 In meerdere adviezen en boetebesluiten wordt bij de bespreking van 'geanonimiseerde gegevens' verwezen naar het advies over anonimiseringstechnieken van de Artikel 29-Werkgroep en de daarin gehanteerde definitie van anonimiseren. Zie onder meer het boetebesluit van 11 maart 2021 van de Autoriteit Persoonsgegevens gericht aan de gemeente Enschede over wifitracking Raadpleegbaar via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_ap_gemeente_enschede.pdf. Autoriteit Persoonsgegevens, 'Microsoft Windows 10. De verwerking van persoonsgegevens via telemetrie', Rapport definitieve bevindingen 29 augustus 2017met correcties 6 oktober 2017. Raadpleegbaar via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/01_onderzoek_microsoft_windows_10_okt_2017.pdf. Autoriteit Persoonsgegevens, 'Normenkader digitale billboards', 25 juni 2018. Raadpleegbaar via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_branche_normkader_digitale_billboards.pdf.

11 Artikel 29-Werkgroep, 'Advies 5/2014 over anonimiseringstechnieken', WP 216

12 Idem, p. 27.

Bij vormen van MPC waarbij niet zeker is of de data door koppeling tot een persoon te herleiden kan zijn, zal zekerheidshalve als uitgangspunt moeten worden genomen dat de data (mogelijk) persoonsgegevens bevat. Meer concreet geldt daarbij het volgende.

1) Verwerken van persoonsgegevens bij de inzet van DHE

Indien de dataset die wordt ingeladen in het data station persoonsgegevens bevat zal bij **stap ii** in de regel sprake zijn van het verwerken van persoonsgegevens. Afhankelijk van de inhoud van het analyseverzoek, en de daarvoor benodigde gegevens, zal bij de verwerkingen ten behoeve van de berekeningen door de data stations in **stappen iv** en **v** (het komen tot een eindresultaat en de uitvoercontrole) ook sprake zijn van het verwerken van persoonsgegevens. Dat deze gegevens in **stap iv** homomorf zijn versleuteld doet daaraan niks af. Een dergelijke versleuteling is, zo zijn ook de Europese privacytoezichthouders van oordeel,[13] in beginsel omkeerbaar waardoor de gegevens niet kwalificeren als anonieme gegevens, maar als pseudonieme persoonsgegevens.

> NB: De verwerkingshandeling in **stap iv** (het doen van berekeningen door de data stations) zou theoretisch kunnen leiden tot anonieme gegevens als 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 te voegen tot een hoog aggregatieniveau.[14] Daarbij dient echter tot uitgangspunt te worden genomen dat het treffen van dergelijke maatregelen in **stap iv** herleidbaarheid niet onomkeerbaar uitsluit en dus ook niet snel leidt tot anonieme gegevens.

De homomorf versleutelde gegevens zijn voor de verstrekkende deelnemer in ieder geval persoonsgegevens.

De voor de verstrekkende deelnemer pseudonieme persoonsgegevens kunnen onder omstandigheden anoniem zijn voor de ontvangende deelnemers. Relevant in dat verband is in hoeverre de ontvangende deelnemers (eventueel door elkaars data te koppelen) redelijkerwijs over middelen beschikken om de versleutelde persoonsgegevens te ontsleutelen en daarmee (indirect) te herleiden tot een natuurlijk persoon. Aangezien e.e.a. niet geheel valt uit te sluiten, nemen wij bij de inzet van DHE zekerheidshalve tot uitgangspunt dat de ontvangende deelnemer persoonsgegevens verwekt.

De verwerkingen ten behoeve van de berekeningen door de data door de verstrekker in **stap iv**, waaronder de verstrekking aan een andere deelnemer, behelzen dus nog altijd een verwerking van persoonsgegevens.

---

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

[14] Zie Artikel 29-Werkgroep, 'Advies 5/2014 over anonimiseringstechnieken', WP 216, p. 24-25 en p. 34.

2) Verwerken van persoonsgegevens bij de inzet van SS

Net als bij DHE, zal in **stap iii** bij het opdelen van de dataset in afzonderlijke *shares* sprake zijn van het verwerken van persoonsgegevens indien die dataset persoonsgegevens bevat. Dat geldt overigens ook als deze opdeling leidt tot anonieme gegevens. Het anonimiseren zelf is immers ook een verwerking van persoonsgegevens.[15]

De vraag is of door middel van de inzet van SS tussentijds - als gevolg van **stap iii**: het opdelen van inputdata in *shares* - gesproken kan worden van anonieme gegevens (waarop de AVG niet van toepassing meer is). Daarvoor moet worden bezien in hoeverre de *shares* informatie bevatten die iets zeggen over een identificeerbaar persoon en in hoeverre deelnemers redelijkerwijs over middelen beschikken om, bijvoorbeeld door bestandskoppeling, de inputdata in de share alsnog (indirect) te herleiden tot een natuurlijk persoon. Daarbij is bepalend of het voor een deelnemer excessieve inspanning vergt om de informatie in de *share* te herleiden tot een natuurlijk persoon. Bij de inzet van SS geldt daarbij concreet het volgende.

Deelnemers beschikken niet over de relevante *shares* waarmee de informatie uit één *share* (door samenvoeging of vergelijking) kunnen worden herleid tot een individu. De deelnemer zal op zichzelf uit deze enkele eigen *share* geen (directe) informatie over een identificeerbare persoon kunnen afleiden. In veel gevallen leidt de inzet van SS namelijk tot een zodanige splitsing van de gegevens dat geen enkel deel dat een afzonderlijke betrokken partij ontvangt, toereikend is om alle of een deel van de persoonsgegevens te reconstrueren.[16]

Dat de 'eigen' *share* op zichzelf geen persoonsgegeven bevat, sluit echter niet uit dat de deelnemer, eventueel in strijd met de governance-afspraken, de ingeschakelde partij die het netwerk beheert of de andere deelnemers aan de MPC-toepassing ertoe beweegt om hun eigen *share* kenbaar te maken. Indien daarmee alsnog (indirecte) herleidbaarheid kan optreden, is er sprake van het verwerken van persoonsgegevens. Doordat het indirect herleiden van informatie in een *share* tot een individu door het samenvoegen of vergelijken van de *shares* nooit onomkeerbaar kan worden uitgesloten, nemen wij ook hier tot uitgangspunt dat bij de inzet van SS zekerheidshalve moet worden uitgegaan van het verwerken van persoonsgegevens.

Het vervolgens doen van berekeningen op deze *share* in **stap iv** behelst in zoverre dan ook de verwerking van persoonsgegevens. Ook het samenbrengen van de *shares* van de

---

15 Brief van de Autoriteit Persoonsgegevens van 25 juni 2018 over digitale billboards. Raadpleegbaar via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_branche_normkader_digitale_billboards.pdf.

16 Zie in dat verband wederom de uitspraak van 26 april 2023 van het Hof van Justitie van de Europese Unie (met kenmerk ECLI:EU:T:2023:219).

tussenresultaten in **stap v** zal dan een verwerking van persoonsgegevens opleveren. Dit is slechts anders, indien de tussenresultaten en/of het eindresultaat tezamen op geen enkele wijze iets zeggen over een identificeerbare persoon.

Toekomstperspectief

Hoewel het op dit moment aanbeveling verdient om bij de inzet van DHE en SS ervanuit te gaan dat persoonsgegevens verwerkt worden, raden wij om op dit punt de ontwikkelingen in de rechtspraak en de opinies van de toezichthouders ten aanzien van het begrip 'persoonsgegevens' en 'anonimiseringstechnieken' nauwgezet te volgen. Het valt niet uit te sluiten dat in toekomstige rechtspraak of opinies meer juridische ruimte wordt gezien om met de inzet van DHE of SS herleidbaarheid tot personen onomkeerbaar uit te sluiten. De inzet van SS wordt bijvoorbeeld al in andere contexten door de EPDB aangehaald. Zo heeft de EDPB recentelijk geoordeeld dat de inzet van SS kan voorzien in een doeltreffende aanvullende maatregel voor doorgifte, als bedoeld in art. 46 AVG.17 De inzet van SS waarborgt in grote lijnen een overeenkomend beschermingsniveau voor de naar het derde land doorgegeven gegevens. Daarmee onderkent de EDOB in ieder geval dat SS een nuttige privacy enhancing technologie kan vormen die ongerechtvaardigde toegang tot de data door buitenlandse autoriteiten genoegzaam kan uitsluiten. Opvallend is verder dat de EDPB het advies over anonimiseringstechnieken in hun agenda voor 2022/2023 heeft genoemd.18 De EDPB willen gemeenschappelijke standpunten en richtsnoeren, met name in de context van nieuwe technologieën, (opnieuw) vaststellen. Mogelijk bieden deze toekomstige standpunten meer juridische ruimte om met de toepassing van secret sharing, in specifieke contexten, de verwerking van persoonsgegevens uit te sluiten. In deze whitepaper kan daar echter niet op worden vooruitgelopen.

Voor zover met de MPC-toepassing (indirect) persoonsgegevens worden verwerkt, dient de met de MPC gepaarde verwerking van persoonsgegevens, voor zover de verwerking valt binnen de materiële reikwijdte van de AVG (zie art. 2 lid 2 AVG) te voldoen aan de (U)AVG. Ook zal de MPC aan de algemene beginselen van bestuur (abbb's) moeten voldoen en, eventueel, aan de aanvullende randvoorwaarden die zijn opgenomen in de

[17] Zie EDPB. 'Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen', versie 2.0, vastgesteld op 18 juni 2021 (raadpleegbaar via: https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf)

[18] Raadpleegbaar via: https://edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-work-programme-2023-2024_nl.

bijzondere wettelijke regeling die de verwerking van deze persoonsgegevens regelt (zie **par. 5.2 e.v**.)

Worden anonieme gegevens verwerkt, dan hoeft deze verwerking niet te voldoen aan de (U)AVG. Het (hergebruik) van deze anonieme gegevens bij de inzet van MPC hoeft daarmee alleen nog te worden getoetst aan de abbb's (zie daarover **par 5.7**) en, eventueel, de bijzondere wettelijke regeling die de verwerking van deze anonieme gegevens regelt (zie daarover **par. 5.3**).

5.2 *Hoe kan in zijn algemeenheid worden vastgesteld wie verwerkingsverantwoordelijke resp. verwerker is?*

In de AVG wordt een onderscheid gemaakt tussen de verwerkingsverantwoordelijke en de verwerker (zie art. 4, 24 en 28 AVG).

De verwerkingsverantwoordelijke is de centrale figuur binnen de AVG op wie in beginsel alle AVG-verplichtingen rusten. De verwerkingsverantwoordelijke stelt het doel en de middelen van de verwerking van persoonsgegevens vast. Dat betekent dat de verantwoordelijke bepaalt wat er met de persoonsgegevens gebeurt. In sommige gevallen volgt verwerkingsverantwoordelijkheid uit de wet.

De verwerkingsverantwoordelijke kan een verwerker inschakelen die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt. De verwerker staat altijd in een ondergeschikte relatie ten opzichte van de verantwoordelijke en dient diens instructies op te volgen.

De kwalificatie van de betrokken partijen bij de inzet van MPC

Indien persoonsgegevens bij de inzet van MPC verwerkt worden, zullen deze persoonsgegevens door de verschillende partijen worden aangeleverd en (een deel daarvan wordt) in homomorf versleutelde vorm (bij de inzet van DHE) of via *shares* (bij de inzet van secret sharing), uitgewisseld met andere betrokken partijen. De toepassing van MPC betreft een privacy-vriendelijke manier van het uitwisselen van persoonsgegevens tussen de verschillende betrokkenen.

Voor zover bij de aanlevering van de data en bij de uitwisseling daarvan geen sprake is van een hiërarchische relatie (en in dat kader ook geen afspraken zijn gemaakt) is iedere partij gelijk. Iedere partij is vrij en daarmee verantwoordelijk voor het verwerken en uitwisselen van de door hen ingeladen informatie.

Voorstelbaar is dat partijen ten aanzien van enkele gedeelten van de verwerking, bijvoorbeeld ten aanzien van de berekeningen bij de inzet van DHE (**stap iv**) of de

inrichting van de datastations bij SS (**stap ii**), in **stap i** gezamenlijk afspraken maken over het doel en de wijze waarop een verwerking gebeurt. Als gevolg daarvan zullen de betrokken partijen ten aanzien van die gedeelten van de verwerking kunnen kwalificeren als gezamenlijke verwerkingsverantwoordelijken. Op grond van art. 26 AVG dienen zij hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit de AVG in een onderlinge regeling vast te leggen.

Betrokken partijen die één data station draaien namens één van de verwerkingsverantwoordelijken binnen een MPC zullen veelal kwalificeren als verwerkers. De primaire taak van deze partijen is immers het laten functioneren van de MPC ten behoeve van alle verantwoordelijke partijen. Als de partijen die de data stations draaien daadwerkelijk verwerkers zijn, dan zijn de verantwoordelijken verplicht om met deze verwerkers verwerkersovereenkomsten te sluiten (art. 28 AVG).

5.3 *Biedt de inzet van DHE resp. de inzet van SS meer juridische ruimte voor het doorbreken van een sectorale geheimhoudingsplichten en/of een (strikte) doelbinding van (persoons)gegevens?*

De gegevens die de betrokken partijen willen verwerken bij de inzet van DHE of bij de inzet van SS zijn eerder voor bepaalde doeleinden verzameld en verwerkt. Voor de vraag of de verwerking van deze gegevens bij de inzet van MPC is toegestaan, moet onderscheid worden gemaakt tussen de verwerking van anonieme gegevens en de verwerking van persoonsgegevens.

Persoonsgegevens

Het primaire doeleinde waarvoor de persoonsgegevens zijn verzameld is veelal een ander doeleinde dan waarvoor de persoonsgegevens worden verwerkt bij de inzet van MPC (een zgn. verdere verwerking), bijv. – bij de inzet van DHE – ingeladen in een datastation (**stap ii**); en versleuteld en (vanwege het uitgangspunt dat versleuteling niet leidt tot anonieme gegevens (zie hierover par. 5.1)) uitgewisseld (**stap iv**); of – bij de inzet van SS – opgedeeld in *shares* (**stap iii**); en (vanwege het uitgangspunt dat de opdeling niet leidt tot anonieme gegevens (zie hierover par. 5.1)) uitgewisseld (**stappen iii** en **iv**).

Een verdere verwerking van persoonsgegevens is alleen toegestaan indien deze berust op toestemming van de betrokkene, op een Unierechtelijke bepaling of Unierecht of nationaal recht daarin voorziet, of verenigbaar is met het primaire doel waarvoor de gegevens werden verzameld (zie art. 6 lid 4 AVG en art. 5 lid 1 aanhef en onder b AVG).

> Let op: Het proces van anonimiseren is ook een verdere verwerking. Dat proces is volgens de voormalige EDPB als verenigbaar met de oorspronkelijke

doeleinden te beschouwen mits het anonimiseringsproces ertoe strekt op betrouwbare wijze anoniem gemaakte informatie te produceren en mits er een grondslag is voor het primaire gebruik.[19]

Vaak zal de verdere verwerking niet kunnen worden gebaseerd op een Unierechtelijke of nationaalrechtelijke bepaling en kan ook geen toestemming van de betrokkene worden verkregen. In dat geval zal moeten worden bezien of de verdere verwerking verenigbaar is. Een verdere verwerking is als verenigbaar met het oorspronkelijke verwerkingsdoel waarvoor de betrokken partij de gegevens heeft verzameld te beschouwen als de wettelijke basis waarop het primaire gebruik is gebaseerd de verdere verwerking toestaat.

Ter illustratie worden hieronder een aantal geheimhoudingsplichten of andere regels uit sectorspecifieke wetgeving besproken die van invloed kunnen zijn voor de vraag of de primaire wettelijke basis de verdere verwerking toestaat:

Art. 7:458 BW
Een hulpverlener kan in afwijking van het bepaalde in art. 7:457 BW gegevens over een patiënt, zonder toestemming van de patiënt, aan andere partij verstrekken als deze gegevens gepseudonimiseerd zijn en de verdere verwerking voldoet aan de randvoorwaarden art. 7:458 BW.

Art. 65 Pw
Het college van burgemeesters en wethouders (college) kan, blijkens het eerste lid van art. 65 Participatiewet (Pw), informatie die het college bij de uitvoering van de Pw heeft verkregen over (onder meer) een persoon of zaken van een ander, slechts verder bekend maken voor zover dat voor de uitvoering van de Pw noodzakelijk is dan wel op grond van de Pw is voorgeschreven of toegestaan. Ten behoeve van wetenschappelijk onderzoek of statistiek kunnen desgevraagd gegevens aan derden worden verstrekt voor zover de persoonlijke levenssfeer van de betrokkenen daardoor niet onevenredig wordt geschaad (zie art. 65 lid 3 Pw).

Wmo
De Wet maatschappelijke ondersteuning (Wmo) bevat een gesloten verstrekkingsregime en kenmerkt zich door een strikte doelbinding[20] en een strikte geheimhoudingsplicht. Uit dit strikte stelsel volgt dat de in het kader van deze wet verkregen gegevens uitsluitend kunnen worden verstrekt aan anderen, voor zover de Wmo daarvoor een expliciete wettelijke grondslag geeft. Zo is er een afwijkende regeling getroffen voor wetenschappelijk onderzoek of statistisch onderzoek op het gebied van de volksgezondheid, opgroei- en opvoedingsproblemen, psychische problemen en stoornissen, kinderbescherming of jeugdreclassering (zie art. 5.3.6 lid 1 Wmo).

---

19 Zie Artikel 29-Werkgroep, 'Advies 5/2014 over anonimiseringstechnieken', WP 216, p. 8.
20 Vgl. *Kamerstukken* II 2013/14, 33 841, nr. 3, p. 66: Uit de memorie van toelichting bij de wet blijkt dat de wetgever bijzondere aandacht heeft gehad voor het doelbindingsvereiste en om deze reden per actor zo concreet en nauwkeurig mogelijk heeft omschreven voor welke specifieke taken het is toegestaan dat de in het kader van deze wet verkregen gegevens mogen worden verwerkt en verstrekt aan anderen.

Staat de wettelijke basis waarop het primaire gebruik is gebaseerd de verdere verwerking niet expliciet toe, dan moet bezien worden of de verdere verwerking verenigbaar is (art. 6 lid 4 AVG). Bij deze toets zouden de volgende regels tot uitgangspunt genomen kunnen worden. De verdere verwerking kan (sneller) verenigbaar worden geacht indien:[21]

> a) de verwerking van persoonsgegeven bij de inzet van DHE of de inzet van SS niet in strijd is met een geheimhoudingsplicht[22] of andere regels uit sectorspecifieke wetgeving (zie de hiervoor besproken voorbeelden);
> b) het doel of de doelen waarvoor de gegevens zijn verzameld nauw samenhangen met het doel van de verdere verwerking bij de inzet van DHE of de inzet van SS;
> c) de verdere verwerking voor een betrokkene redelijkerwijs te verwachten is (daarbij moet acht worden geslagen op het kader[23] waarin de persoonsgegevens zijn verzameld, waaronder de verhouding tussen de betrokkene en de betrokken partij);
> d) er geen gevoelige persoonsgegevens worden verwerkt, denk bijvoorbeeld aan gegevens over ras[24] maar ook financiële gegevens;
> e) het verdere verwerkingsdoel niet op identificatie van betrokkenen is gericht (bijvoorbeeld om betrokkene te identificeren die voldoen aan bepaalde kenmerken);
> f) de voorgenomen verdere verwerking geen of slechts beperkte (rechts)gevolgen heeft voor de betrokkenen; én
> g) de aangeleverde dataset dusdanig is bewerkt dat de kans op (onverhoopte) identificatie van betrokkenen (zeer) klein is. Daarbij moeten ook de nodige passende organisatorische en/of technische maatregelen zijn getroffen die voorkomen dat de gegevens in de dataset (alsnog) feitelijk kunnen worden herleid tot een natuurlijke persoon.

Ook als aan een deel van de voornoemde factoren is voldaan, kan sprake zijn van een verenigbare verdere verwerking.

Verder is van belang dat een verdere verwerking met het oog op onder meer wetenschappelijke of historische of statistische doeleinden (waar ook technologische ontwikkelingen onder kunnen vallen) als een verenigbare rechtmatige verwerking wordt beschouwd.[25] Voorwaarde voor de verdere verwerking voor die doeleinden is wel dat de verwerkingsverantwoordelijke voorziet in passende waarborgen voor de bescherming van de persoonsgegevens van de betrokkenen, bijvoorbeeld maatregelen die pseudonimisering of die uitsluiting van identificatie van betrokkenen omvatten (zie art. 5 lid 1 aanhef en onder b en art. 89 AVG).[26] Een verdere verwerking voor statistische doeleinden is

---

21 De opsomming is niet limitatief. Elk van de genoemde factoren moet - mogelijk in samenhang met andere factoren die in het concrete geval als relevant worden beschouwd - in onderling verband worden beoordeeld en gewogen ter beantwoording van de vraag of sprake is van verenigbaar gebruik.
22 Zie overweging 50 van de considerans bij de AVG.
23 Daarbij moet acht worden geslagen op de mogelijk geldende beleidsregels of privacyverklaring.
24 In dat geval moet ook worden voldaan aan artikel 9 AVG, zie par. 5.4.
25 In dat geval is het niet nodig om te voldoen aan de eisen (b) tot en met (g) hierboven.
26 Zie onder meer overwegingen 50, 156, 157, 159, 160 en 162 van de considerans van de AVG.

bovendien alleen mogelijk voor zover het resultaat van de verwerking voor statistische doeleinden niet uit persoonsgegevens, maar uit geaggregeerde gegevens bestaat. Bovendien mag het resultaat en de onderliggende persoonsgegevens niet worden gebruikt als ondersteunend materiaal voor maatregelen of beslissingen die een bepaalde natuurlijke persoon betreffen (zie overweging 162 van de considerans bij de AVG). Het is met name deze statistisch en wetenschappelijke onderzoeksexceptie die in veel gevallen een gedegen basis zou kunnen vormen voor de onderlinge verstrekking en berekening door middel van SS of DHE. Daarbij dient echter wel steeds kritisch te worden bezien of het betreffende SS- of DHE-project voldoet aan de voorwaarden van 89 AVG.

Indien sprake is van een toelaatbare verenigbare verdere verwerking, dan is bij een interne verdere verwerking (door dezelfde verwerkingsverantwoordelijke) geen afzonderlijke wettelijke grondslag als bedoeld in art. 6 lid 1 AVG vereist.[27] Gaat het bij de verdere verwerking om een (externe) verstrekking aan een andere verwerkingsverantwoordelijke, dan moet de ontvangende verwerkingsverantwoordelijke vanzelfsprekend wel een eigen grondslag hebben om de ontvangen gegevens te verwerken (zie hierna).

Anonieme gegevens

Als de verwerkingen in **stap ii** (*het inladen van de dataset*) en/of - als gevolg van een tussentijdse effectieve anonimiseringsslag - **stappen iv** (*het één voor één doen van berekeningen*) en **v** (*het komen tot een eindresultaat*) bij de inzet van DHE of in **stap iii** (*het opdelen van inputdata en verdelen van shares*) en/of - als gevolg van een tussentijdse effectieve anonimiseringsslag - **stappen iv** (*het doen van berekeningen op de shares*) en **v** (*het komen tot een eindresultaat*) bij de inzet van SS betrekking hebben op anonieme gegevens, moet alleen vastgesteld worden of de wettelijke basis voor het primaire gebruik (of de abbb's, zie **par. 5.7**) in de weg staat aan de verdere verwerking. Die wettelijke basis kan bijvoorbeeld een geheimhoudingsplicht bevatten die verder gebruik van de gegevens (ook al zijn deze anoniem) verbiedt. In sommige gevallen staan geheimhoudingsplichten verder gebruik van gegevens juist toe als deze gegevens anoniem zijn.

> Ter illustratie worden hieronder een aantal geheimhoudingsplichten besproken die verder gebruik van anonieme gegevens wel of juist niet toestaan:
>
> **Art. 65 Pw**
> Het college is bij de verwerking van persoonsgegevens ter uitvoering van de Pw gebonden aan een strikte geheimhoudingsplicht. Het college kan, blijkens het

[27] Zie *Kamerstukken* II 2018/19, 34 851, nr. 3, p. 38 en Afdeling advisering van de Raad van State, 'De rol van gemeenten in de bestuurlijke en integrale aanpak van ondermijning' 20 maart 2019. Deze opmerking is toegevoegd naar aanleiding van het wetgevingsadvies van de Afdeling advisering van de Raad van State (*Kamerstukken* II 2017/18, 34 851, nr. 4, p. 36-38).

eerste lid van art. 65 Pw, informatie die het college bij de uitvoering van de Pw over een persoon heeft verkregen, slechts verder bekend maken voor zover dat voor de uitvoering van de Pw noodzakelijk is dan wel op grond van de Pw is voorgeschreven of toegestaan. Deze geheimhoudingsplicht is, zo blijkt uit art. 65 lid 2 aanhef en onder b Pw, niet van toepassing indien de gegevens niet herleidbaar zijn tot individuele natuurlijke personen.

Art. 67 AWR en art. 67 Ivw
Voor de vraag of en zo ja in hoeverre, art. 67 AWR en art 67 Ivw de verdere verwerking van anonieme gegevens toestaan, zijn twee (overigens tegenstrijdige) passages uit de parlementaire geschiedenis relevant:

Zie enerzijds *Kamerstukken* II 2011/12, 33 003, nr. 83, p. 4-5:

"De geheimhoudingsplicht van artikel 67 AWR staat niet in de weg aan verstrekking van gegevens indien het gegevens betreft die niet herleidbaar zijn tot een individuele belastingplichtige. Dit betekent dat het verstrekken van geaggregeerde gegevens, mits niet herleidbaar tot individuele belastingplichtigen, niet in strijd is met de fiscale geheimhoudingsplicht. De Belastingdienst verstrekt regelmatig geaggregeerde gegevens, zoals bijvoorbeeld de belastingopbrengst in een jaar, of hoeveel personen in een jaar gebruik hebben gemaakt van de inkeerregeling. In het beheersverslag en in de halfjaarsrapportages van de Belastingdienst zijn dergelijke gegevens terug te vinden. Informatie die bijvoorbeeld ziet op een branche die bestaat uit drie bedrijven die goed op de hoogte zijn van elkaars bedrijfsvoering zal echter niet, ook niet in geaggregeerde vorm, kunnen worden verstrekt. Dergelijke informatie valt immers te herleiden tot een individueel bedrijf. Artikel 67 AWR staat dan aan verstrekking in de weg. Ook voor geanonimiseerde gegevens geldt dat deze niet onder de geheimhoudingsplicht vallen, mits de gegevens afdoende anonimiseerbaar zijn. Afdoende anonimiseerbaar betekent in dit verband niet herleidbaar tot een individuele belastingplichtige. Een voorbeeld waarin het verstrekken van geanonimiseerde gegevens plaatsvindt, is in het kader van de behandeling van Wob-verzoeken, zoals bijvoorbeeld het Wob-verzoek van 26 november 2010 inzake BPM-aangiften inzake parallel import van tweedehands auto's en het Wob-verzoek van 17 juli 2009 inzake handhavingsconvenant Belastingdienst en individuele ondernemingen." (onderstreping toegevoegd)

Zie anderzijds *Kamerstukken* II 2005/06, 30 322, nr. 3, p. 20:
"Afdoende anonimisering is namelijk lang niet altijd mogelijk doordat insiders regelmatig uit de omstandigheden van het geval kunnen afleiden om welke belastingplichtige het gaat. Bovendien geldt de geheimhoudingsplicht in principe ook voor geanonimiseerde gegevens." (onderstreping toegevoegd)

Hoewel er enige discrepantie tussen beide passages bestaat, lijkt de huidige opvatting van de wetgever te zijn dat anonimisering – afhankelijk van de aard van de informatie waar het om gaat en het doel van de verdere verwerking – ertoe kan leiden dat de fiscale geheimhoudingsplicht kan worden doorbroken.

Zekerheidshalve kan er evenwel een expliciete grondslag gecreëerd worden voor de doorbreking van de fiscale geheimhoudingsplicht voor de verwerking van (geanonimiseerde) gegevens middels de inzet van MPC. In art. 67 AWR en art. 67 Ivw staat immers dat de geheimhoudingsplichten niet gelden als bij regeling van de minister is bepaald dat bekendmaking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak van een bestuursorgaan (zie in dat verband de al bestaande regeling in (art. 43c van de) Uitvoeringsregeling AWR).

Tip: Hoe om te gaan met de (strategische) plaatsing van een verwerkingsverantwoordelijke met een strikte geheimhoudingsplicht binnen een DHE-project

Indien aan de hand van een geheimhoudingsplicht zou worden vastgesteld dat één van de verwerkingsverantwoordelijken die deelneemt aan een DHE-project geen grondslag heeft om gegevens aan derden te verstrekken, kan het in bepaalde projecten lonen om de desbetreffende verwerkingsverantwoordelijke als laatste partij aan te wijzen die de eindberekening uitvoert met zijn data station (zie data station (c) bij de afbeelding van de werking van DHE, paragraaf 4.1). Op deze wijze hoeft de verwerkingsverantwoordelijke géén van zijn gegevens te verstrekken aan een derden, maar slechts binnen zijn eigen data station de (eind)berekening uit te voeren. Door de strategische plaatsing van de verwerkingsverantwoordelijk kan de berekening binnen het DHE-project toch doorgang vinden. Of en zo ja, in hoeverre de verdere verwerking van de 'eigen gegevens' binnen het data station toelaatbaar is, hangt uiteraard af van de formulering en reikwijdte van de geheimhoudingsplicht en de doelbinding van de desbetreffende wet.

Binnen een MPC-project op basis van secret sharing bestaat er geen mogelijkheid om een strategische keuze te maken in de volgorde van de nodes, aangezien ieder datastation een share verwerkt, bestaande uit gegevens van iedere partij. Een strikte geheimhoudingsplicht zal in dat geval dus relatief sneller leiden tot de conclusie dat de verstrekking niet plaats kan vinden.

5.4 *Hoe kan worden vastgesteld of een wettelijke grondslag bestaat voor de verwerking van (bijzondere of strafrechtelijke) persoonsgegevens bij de inzet van DHE en de inzet van SS?*

Bij de verwerking van persoonsgegevens dient steeds te worden nagegaan of daarvoor een wettelijke grondslag als bedoeld in art. 6 lid 1 AVG bestaat. Zoals reeds besproken, is

voor een gerechtvaardigde interne verdere verwerking (door dezelfde verwerkingsverantwoordelijke) geen afzonderlijke wettelijke grondslag vereist.
Bij de inzet van DHE en SS zal echter ook vaak sprake zijn van een (externe) verstrekking aan een andere verwerkingsverantwoordelijke, waardoor die andere verwerkingsverantwoordelijke een eigen grondslag nodig heeft om de ontvangen gegevens te verwerken.

> Voorbeelden van (externe) verstrekkingen aan een andere verwerkingsverantwoordelijke zijn:
> - Het delen van (tussen- of eind-)resultaten, waaronder mogelijk persoonsgegevens, in **stap iv** en **stap v** bij DHE.
> De verdeling van shares, waaronder mogelijk persoonsgegevens, bij SS in **stap iii** en het delen van tussenresultaten in **stap iv** bij SS.

In art. 6 AVG zijn de mogelijke grondslagen (limitatief) opgesomd:

a. De betrokkene heeft toestemming gegeven;
b. De verwerking is noodzakelijk voor de uitvoering of totstandkoming van een overeenkomst;
c. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting van de verwerkingsverantwoordelijke;
d. De verwerking is noodzakelijk ter bescherming van de vitale belangen van een natuurlijk persoon;
e. De verwerking is noodzakelijk voor de vervulling van een publieke taak die aan de verwerkingsverantwoordelijke is opgedragen; of
f. De verwerking is noodzakelijk voor de behartiging van een gerechtvaardigd belang van de verwerkingsverantwoordelijke of van een derde.

Verder is het van belang dat voorafgaand aan de inzet van MPC wordt nagegaan of er bijzondere persoonsgegevens of persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (strafrechtelijke persoonsgegevens) zullen worden verwerkt door één of meerdere partijen. De verwerking van bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens is verboden[28] tenzij dit verbod door middel van een zogenoemde 'doorbrekingsgrond' of 'uitzonderingsgrond' kan worden doorbroken.

> Bijzondere persoonsgegevens zijn gegevens waaruit ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakbond blijkt, en de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, of gegevens over gezondheid, gegevens met betrekking tot iemands seksuele leven of seksuele gerichtheid.

[28] Art. 10 AVG jo. art. 1 UAVG.

Strafrechtelijke gegevens zijn persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.[29] Volgens vaste jurisprudentie geldt dat voor de vaststelling dat strafrechtelijk persoonsgegevens worden verwerkt niet een veroordeling door een strafrechter is vereist maar dat sprake moet zijn van zodanig concrete feiten en omstandigheden dat zij als een strafbaar feit te kwalificeren bewezenverklaring in de zin van art. 350 van het Wetboek van Strafvordering kunnen dragen. Het gaat er dus om of de te verwerken gegevens in de richting wijzen van een zwaardere verdenking dan een redelijk vermoeden van schuld.[30]

De doorbrekingsgrond kan volgen uit de (Uitvoeringswet) AVG of kan zijn opgenomen in een specifieke (sectorale) wet. Sommige doorbrekingsgronden zien op alle typen bijzondere of strafrechtelijke persoonsgegevens en andere doorbrekingsgronden hebben betrekking op een specifieke categorie van doorbrekingsgronden. Relevante doorbrekingsgronden zijn onder meer:

a. art. 9 AVG jo. art. 24 UAVG resp. art. 10 AVG jo. art. 32 aanhef en onder f UAVG: het verbod om bijzondere persoonsgegevens te verwerken is niet van toepassing, indien:
i) de verwerking noodzakelijk is met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig art. 89 lid 1 AVG;
ii) het onderzoek, bedoeld in onderdeel i), een algemeen belang dient;
iii) het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost; en
iv) bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad, bijvoorbeeld voorschriften met betrekking tot de toegang tot de gegevens, geheimhouding en de presentatie van het resultaat van het onderzoek (dat bij statistisch onderzoek alleen kan bestaan uit geaggregeerde gegevens).[31]

b. art. 9 lid 2 aanhef en onder g AVG resp. art. 10 AVG jo. art. 32 aanhef en onder e UAVG: het verbod is niet van toepassing indien "de verwerking noodzakelijk [is] 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

[29] Art. 10 AVG.
[30] HR 29 mei 2009, ECLI:NL:HR:BH4720 en in navolging daarvan mee recent nog Rechtbank Rotterdam 6 januari 2020, ECLI:NL:RBROT:2020:211 en Gerechtshof Arnhem-Leeuwarden, 28 april 2020, ECLI:NL:GHARL:2020:3374.
[31] Zie in dat kader *Kamerstukken* II 1997/98, 25 892, 3, p. 126.

> belangen van de betrokkene". Met andere woorden: als er een specifieke wettelijke basis is gecreëerd voor de verwerking van bijzondere of strafrechtelijke persoonsgegevens.

Tot slot dient bij de vaststelling of een verwerkingsverantwoordelijke partij persoonsgegevens bij de inzet van MPC mag verwerken, extra zorgvuldigheid te worden betracht bij het verwerken van nationale identificatienummers zoals het BSN. Op grond van art. 46 lid 1 UAVG (jo. art. 87 AVG) moet het gebruik van wettelijke identificatienummers in beginsel bij (formele) wet zijn voorgeschreven en mag het nummer slechts worden gebruikt ter uitvoering van de in de wet genoemde doelstellingen.

Zie in dat kader bijvoorbeeld de Wet algemene bepalingen burgerservicenummer, de Wmo, de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en de Wet langdurige zorg.

5.5 *Leidt de inzet van DHE en/of de inzet van SS tot geautomatiseerde besluitvorming als beschreven in art. 22 AVG?*

Art. 22 AVG geeft de betrokkene, behoudens uitzonderingen, het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking (bijvoorbeeld profilering) gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.[32] De betrokkene hoeft dit recht niet in te roepen. Het recht van de betrokkene komt daarom feitelijk neer op een verbod voor de verwerkingsverantwoordelijke.

> De AVG definieert profilering als 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 om zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.[33]
>
> Van belang is bovendien dat het bij art. 22 AVG gaat om (geautomatiseerde) besluitvorming of profilering gericht tegen natuurlijk personen. Geautomatiseerde besluitvorming of profilering dat enkel gericht is op rechtspersonen en dus geen verwerking van persoonsgegevens betreft of geen rechtsgevolgen geeft voor een betrokkene of de betrokkene anderszins in aanmerkelijke mate treft (bijv. in het kader van een onderzoek naar frauderende B.V.'s) valt niet onder het verbod van art. 22 AVG.

Om te kunnen vaststellen of sprake is van geautomatiseerde besluitvorming als bedoeld in art. 22 AVG dient te worden getoetst of sprake is van (i) een uitsluitend op

---

[32] Art. 22 lid 1 AVG.
[33] Art. 4 aanhef en onder 4 AVG.

geautomatiseerde verwerking gebaseerd besluit (ii) met rechtsgevolgen of dat de betrokkene anderszins in aanmerkelijke mate treft. Hieronder volgt een nadere uitwerking van deze begrippen.

(i) Is sprake van een uitsluitend op geautomatiseerde verwerking gebaseerd besluit?
Als er sprake is van menselijke tussenkomst voordat het besluit wordt genomen, is er geen sprake van een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. Een geautomatiseerd proces dat slechts een aanbeveling doet, die vervolgens door een mens met andere informatie wordt afgewogen bij het nemen van een uiteindelijk besluit, vormt geen geautomatiseerde besluit.

De menselijk tussenkomst moet wel betekenis hebben. Het klakkeloos overnemen van de uitkomst van de geautomatiseerde verwerking geldt niet als betekenisvolle menselijke tussenkomst. De menselijke tussenkomst moet leiden tot zinvol toezicht op de besluitvorming en degene die de menselijke tussenkomst uitvoert, moet alle relevante gegevens bij de herbeoordeling betrekken en bevoegd en bekwaam zijn om een andersluidend besluit te nemen.[34] Er is momenteel in de rechtspraak discussie over de vraag of een geautomatiseerd proces dat slechts een aanbeveling doet (bijv. de aanbeveling dat er toezicht moet worden gehouden) die vervolgens door wordt gebruikt bij het nemen van een uiteindelijk besluit, geautomatiseerde besluitvorming als bedoeld in artikel 22 AVG vormt.

> Zie HvJ Conclusie AG Pikamäe 16 maart 2023, C-634/21 ECLI:EU:C:2023:220, r.o. 42 t/m 47.[35] In zijn conclusie stelt AG Pikamäe dat als het besluit in dusdanig sterke mate wordt bepaald door de score en als het ware doordringt in het besluitvormingsproces, er sprake is van een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. Hij geeft aan dat door de score het besluit in principe vooraf is bepaald en dat het feit dat menselijke tussenkomst nog mogelijk is hier niet af doet omdat de score dusdanig doordringt in het uiteindelijke besluit.
>
> Zie Gerechtshof Amsterdam 4 april 2023, ECLI:NL:GHAMS:2023:793, r.o. 3.18 en 3.19. Het Hof oordeelde dat voorafgaand aan het besluit tot het deactiveren van accounts van Uber-chauffeurs naar aanleiding van fraudesignalen, er geen sprake was van betekenisvolle menselijke tussenkomst omdat de Uber-chauffeurs niet waren gehoord, de besluiten algemeen geformuleerd waren en de door onderzoekmedewerkers geschreven notities niet alle gegevens betrokken.[36]

(ii) Leidt het geautomatiseerde besluit tot rechtsgevolgen of is sprake van een besluit dat een betrokkene anderszins in aanmerkelijke mate treft?

---

[34] Zie Artikel 29-Werkgroep, 'Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679', WP 251rev01, p. 24.
[35] Dit betreft het arrest van de AG waaraan nog geen rechtsgevolgen kunnen worden verbonden. De conclusie van het HvJ zelf dient aldus te worden afgewacht.
[36] Tegen deze uitspraak staat op het moment van schrijven nog een cassatietermijn open.

Indien vastgesteld wordt dat inderdaad sprake is van een uitsluitend op geautomatiseerd verwerking gebaseerd besluit, dient vervolgens te worden gekeken naar de specifieke gevolgen van dat besluit. Het verbod van art. 22 AVG is erop gericht om personen te beschermen tegen aanzienlijke effecten van geautomatiseerde besluitvorming. Het verbod geldt slechts indien sprake is van 'besluitvorming met rechtsgevolgen' voor de betrokkene of 'besluitvorming die de betrokkene anderszins in aanmerkelijke mate treft'.[37]

> Met het begrip besluit doelt de AVG niet alleen op juridische besluiten, het kan ook om feitelijke beslissingen gaan.

Met besluiten waaraan rechtsgevolgen zijn verbonden, wordt volgens de (voormalige) EDPB bedoeld een besluit dat van invloed is op iemands wettelijke rechten (zoals het stemrecht of het recht om rechtsmiddelen in te stellen). De (voormalige) EDPB noemt als voorbeeld rechtsgevolgen die iemands juridische status beïnvloeden, waaronder bijvoorbeeld: (i) het recht op of weigering van een uitkering, zoals kinderbijslag of huurtoeslag of (ii) de weigering tot toelating tot een land of de toekenning van een nationaliteit.[38] Betrekkelijk vager is de categorie besluiten die de betrokkene 'in aanmerkelijke mate treft'. Het gaat hier om besluiten die weliswaar geen rechtsgevolg teweegbrengen, maar de betrokkene toch in vergelijkbare mate kan treffen. De (voormalige) EDPB neemt daarbij als uitgangspunt dat "de effecten van de verwerking groot of belangrijk genoeg moeten zijn om aandacht te verdienen".[39]

> 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. Een en ander zal moeten worden uitgekristalliseerd in de Europese en nationale rechtspraak. De (voormalige) EDPB neemt als uitgangspunt dat sprake kan zijn van een besluit dat een betrokkene in aanmerkelijke mate treft indien het besluit het potentieel heeft om "[i] de omstandigheden, het gedrag of de keuzen van de betrokken personen in aanmerkelijke mate te treffen; [ii] een langdurig of blijvend effect op de betrokkene te hebben; of [iii] in het uiterste geval, tot uitsluiting of discriminatie van personen te leiden."[40]

In de parlementaire geschiedenis van de (U)AVG en in de eerdergenoemde opinie van de (voormalige) EDPB worden de volgende voorbeelden aangehaald:

---

37 Achterliggende gedachte van het verbod is dat "niemand mag worden onderworpen aan de gevolgen van een besluit enkel en alleen op basis van kenmerken van een bepaalde groep waartoe hij of zij behoort. De ratio van deze bepaling is dat het in dit licht bijzonder kwetsbaar is om besluitvorming te baseren op enkele persoonskenmerken". Zie overweging 71 van de considerans van de AVG en *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 39.

38 Zie Artikel 29-Werkgroep, 'Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679', WP 251rev01, p. 25.

39 Artikel 29-Werkgroep, 'Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679', WP 251rev01, p. 25.

40 Artikel 29-Werkgroep, 'Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679', WP 251rev01, p. 10-11.

- de automatische weigering van een (online) ingediende kredietaanvraag[41];
- verwerking van sollicitaties zonder menselijke tussenkomst[42];
- besluiten die iemands financiële situatie treffen, waaronder bijvoorbeeld het in aanmerking komen voor een lening[43];
- besluiten die iemands toegang tot gezondheidszorg treffen[44];
- besluiten waarmee iemand de toegang tot de arbeidsmarkt wordt geweigerd of waarmee hij ernstig wordt benadeeld;
- besluiten die iemands toegang tot onderwijs treffen, bijvoorbeeld de toelating tot een universiteit[45].

In de rechtspraak speelt geregeld een discussie over de vraag wanneer een preselectie leidt tot aanmerkelijke gevolgen van de betrokkene, met name in de situatie dat een geautomatiseerde verwerking het resultaat oplevert dat iemand mogelijk betrokken is bij fraude, maar nader onderzoek moet worden verricht. De vraag rijst in dat geval of het enkele resultaat dat iemand mogelijk fraude pleegt, reeds kan worden aangemerkt als een geautomatiseerd besluit met aanmerkelijke gevolgen.

> Zie HvJ Conclusie AG Pikamäe 16 maart 2023, C-634/21 ECLI:EU:C:2023:220, rov. 34 en 35.[46] In deze recente zaak komt AG Pikamäe tot de conclusie dat een score die aangeeft of een persoon in aanmerking komt voor een lening voorafgaand aan het besluit of de lening wordt toegekend, kwalificeert als een besluit dat een betrokkene in aanmerkelijke mate treft.
>
> Zie Gerechtshof Amsterdam 4 april 2023, ECLI:NL:GHAMS:2023:793, rov. 3.18 en 3.19. In deze zaak werd door het Hof geoordeeld dat een geautomatiseerd fraudesignaal naar aanleiding waarvan het account van een Uber-chauffeur kan worden gedeactiveerd, kwalificeert als een besluit dat de betrokkene in aanmerkelijke mate treft.[47]

Op het verbod uit art. 22 AVG bestaan wel uitzonderingen. Het nemen van een geautomatiseerd besluit is toegestaan als het besluit i) noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke; ii) is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene (zoals art. 40 UAVG dat onder meer een

---

41 Overweging 71 van de considerans van de AVG.
42 Overweging 71 van de considerans van de AVG.
43 Zie *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 26.
44 Zie *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 26.
45 Vgl. Artikel 29-Werkgroep, 'Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679', WP 251rev01, p. 10-11
46 Dit betreft het arrest van de AG waaraan nog geen rechtsgevolgen kunnen worden verbonden. De conclusie van het HvJ zelf dient aldus te worden afgewacht.
47 Tegen deze uitspraak staat op het moment van schrijven nog een cassatietermijn open.

uitzondering bevat voor geautomatiseerde besluitvorming *anders dan op basis van profilering*, die noodzakelijk is voor de vervulling van een taak van algemeen belang[48]); of iii) berust op de uitdrukkelijke toestemming van de betrokkene.

Geautomatiseerde besluitvorming bij de inzet van MPC (waaronder inzet van DHE of SS)

In het geval dat het eindresultaat door betrokken partijen gebruikt wordt ten behoeve van besluitvorming speelt de vraag of de (eventuele) geautomatiseerde selectie en koppeling van bijvoorbeeld persoonsgegevens uit de databestanden in **stap ii** (*inladen van data in het datastation*) en **stap iv** (*het doen van berekeningen*) bij DHE of **stap iii** (*het opdelen van inputdata*) of **stap iv** (*het doen van berekeningen*) bij SS reeds tot gevolg heeft dat de betrokkene rechtsgevolgen ondervindt of sprake is van gevolgen die de betrokkene in aanmerkelijke mate treffen. Verdedigbaar kan zijn dat pas in de uiteindelijke besluitvormingsfase de betrokkene rechtsgevolgen respectievelijk aanmerkelijke gevolgen ondervindt van de (geautomatiseerde) selectie van zijn persoonsgegevens. Immers pas dan wordt door een betrokken ambtenaar de beslissing, waarvan de betrokkene gevolgen ondervindt, genomen door het eindresultaat en andere relevante omstandigheden af te wegen.

Het verdedigbare standpunt (dat de enkele geautomatiseerde selectie en koppeling van databestanden géén aanmerkelijke gevolgen heeft voor de betrokken persoon) zou wel kunnen leiden tot een juridische discussie. Gezien de afwezigheid van bestendige rechtspraak, is de kans aanwezig dat de rechter of de Autoriteit Persoonsgegevens de inzet van slimme technologieën (waarbij databestanden geautomatiseerd worden geselecteerd) *an sich* kan aanmerken als geautomatiseerde besluitvorming als bedoeld in art. 22 AVG.

Relevant in dit verband is dat de Rechtbank Den Haag in haar uitspraak van 5 februari 2020[49] heeft laten doorschemeren dat enkel de geautomatiseerde selectie van een persoon waarbij (mogelijk) een verhoogde kans op sociale zekerheidsfraude bestaat, een 'aanmerkelijk gevolg' zou kunnen opleveren voor de geselecteerde persoon. Het ging in deze uitspraak om de toepassing van het Systeem Risico Indicatie (SyRI), een geautomatiseerd systeem dat – kort gezegd – op basis van aangeleverde data een risicomelding doet over personen. Een risicomelding houdt in dat op basis van een vergelijking van (discrepanties in) bestanden is gebleken dat bij een persoon (mogelijk) een verhoogd risico bestaat op sociale zekerheidsfraude. Deze risicomelding mag

[48] Art. 40, lid 1, UAVG bepaalt: "Artikel 22, eerste lid, van de verordening geldt niet indien de in die bepaling bedoelde geautomatiseerde individuele 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."

[49] Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, rov. 6.59.

vervolgens gedurende een periode van twee jaar door deelnemers van het SyRI-project worden gebruikt om een toezichtsonderzoek naar de betreffende persoon in te stellen. De rechtbank oordeelt op grond van art. 8 lid 2 EVRM dat de selectie als zodanig al een 'aanmerkelijk effect' kan hebben op de persoonlijke levenssfeer van de betrokkene.[50] Daarbij neemt de rechtbank in overweging dat een risicomelding twee jaar wordt opgeslagen en voor twintig maanden door deelnemers van het SyRI-project mag worden gebruikt. Hoewel de rechtbank een aanmerkelijk effect lijkt aan te nemen in de zin van art. 8 EVRM (onder verwijzing naar een opinie van de EDPB over geautomatiseerde besluitvorming als bedoeld in art. 22 AVG), laat de rechtbank uitdrukkelijk in het midden of de selectie van een persoon c.q. de risicomelding voldoet aan de precieze definitie in de AVG van geautomatiseerde besluitvorming.

De analyse van de databestanden met behulp van SS of DHE kwalificeert overigens sowieso als profilering als aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijk persoon, bijvoorbeeld het gedrag, (geautomatiseerd) worden geëvalueerd. Voor zover het gedrag louter geautomatiseerd wordt geanalyseerd, is niet alleen sprake van 'profilering', maar kan ook van geautomatiseerde profilering als bedoeld in art. 22 lid 1 AVG sprake zijn.

5.6 *Hoe verhoudt de inzet van DHE en de inzet van SS zich tot het dataminimalisatiebeginsel en welke maatregelen kunnen worden getroffen om te borgen dat voldaan wordt aan privacy by design & default?*

De persoonsgegevens die met behulp van MPC worden verwerkt, moeten steeds toereikend zijn, ter zake dienend en beperkt zijn tot het strikt noodzakelijk (ook wel het beginsel van minimale gegevensverwerking genoemd; art. 5 lid 1 aanhef en onder c AVG). Dat betekent dat alleen *need to know* informatie mag worden verwerkt, en dus geen *nice to know* informatie.

> Dat geldt ook voor toepassing van de DHE of SS voor onderzoeksdoeleinden. Zie art. 89 lid 1 AVG.

Op grond van art. 25 van de AVG dient de toepassing van MPC te voldoen aan de beginselen van *privacy by design* en *privacy by default*. Dat houdt in dat reeds bij het ontwerpen van een nieuw of te wijzigen systeem waarmee gegevens worden verwerkt 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

[50] Art. 8 EVRM regelt de bescherming van het recht op privéleven. Hoewel het recht op gegevensbescherming ontbreekt in de letterlijke tekst van art. 8 EVRM, wordt in de rechtspraak van het Hof voor de Rechten van de Mens (EHRM) aangenomen dat ook gegevensbescherming onderdeel vormt van art. 8 EVRM. Het EHRM gebruikt hiervoor de term 'gegevens die het privéleven raken'. De mate van bescherming van 'gegevens die het privéleven raken' is afhankelijk van de aard van de gegevens, de omvang van de gegevensverwerking, de wijze waarop de gegevens worden gebruikt, het doel van het gebruik, en de mogelijkheden die de verwerking biedt. De bescherming van art. 8 EVRM is voorts niet absoluut en kan worden beperkt, mits wordt voldaan aan de uitzonderingsclausule van art. 8 lid 2 EVRM. De rechtbank heeft in geval van SyRI geoordeeld dat de geautomatiseerde selectie een aanmerkelijk effect heeft voor de betrokkene in de zin van art. 8 EVRM, wat betekent dat moet worden voldaan aan eisen van art. 8 lid 2 EVRM. Hoewel deze eisen enigszins vergelijkbaar zijn met de AVG, is relevant om op te merken dat de AVG op bepaalde aspecten strenger én concreter is, zeker voor zover het gaat om geautomatiseerde besluitvorming.

mogelijke privacyrisico's proactief voorkomen worden en dus al in een zo vroeg mogelijk stadium privacywaarborgende maatregelen worden getroffen.

Het naleven van de beginselen van *privacy by design* & *default* betreft een zeer algemene verplichting, waarbij de verwerkingsverantwoordelijken aan de hand van verschillende factoren (en voorafgaand aan toepassing) een belangenafweging moeten maken ten aanzien van de technische en organisatorische aspecten van gegevensverwerkingen. 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[51]) voor de rechten en vrijheden van de betrokkenen. De verplichting van *privacy by design* & *default* is het best te begrijpen als een zorgplicht om een zo beperkt mogelijke inbreuk op de persoonlijke levenssfeer te maken bij de verwerking van persoonsgegevens.[52]

Dataminimalisatie bij de inzet van MPC (waaronder de inzet van DHE of SS)

Een voordeel van MPC is dat partijen waardevolle inzichten uit hun data kunnen verkrijgen zonder dat de data in leesbare vorm onderling wordt uitgewisseld. Voordat de data onderling wordt gedeeld en vergeleken worden de data immers eerst (bij **stap iv** DHE) versleuteld of (bij **stap iii** SS) opgedeeld in *shares*. Bij DHE worden bij **stap iv** bovendien alleen die attributen of dat deel van de versleutelde dataset gedeeld die het (tussen)resultaat is van de berekening. In beginsel draagt toepassing van MPC dus bij aan dataminimalisatie en komt MPC de beginselen van *privacy by design* en *default* ten goede. Het voorgaande neemt niet weg dat altijd moet worden geborgd dat enkel *need to know* informatie bij de inzet van MPC wordt verwerkt.

Reeds voordat de inputdata wordt ingeladen in het datastation (**stap ii** bij DHE) of wordt opgedeeld (**stap iii** bij SS), moet onder meer worden bezien of deze data passen binnen het (welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde) doel of doelen waarvoor de DHE of SS worden ingezet.

Ook voor de vraag of DHE of SS langs verschillende datastations mag gaan om onderzoek te doen naar de verwantschap tussen de gegevens bij de verschillende betrokken partijen (**stap iv** bij DHE en **stap iii** en **stap iv** bij SS) is bepalend of de betreffende verwerkingen noodzakelijk zijn voor het doel van het onderzoek.

---

51 Zie voor een concretisering hiervan de overwegingen 75 en 76 van de considerans van de AVG.

52 In de (toelichting bij overweging 78 van de considerans bij) de AVG worden de volgende maatregelen genoemd: het minimaliseren van de verwerking van persoonsgegevens, het zo spoedig mogelijk pseudonimiseren van persoonsgegevens, het voor de betrokkene 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.

5.7 *Welke (aanvullende) eisen stellen de beginselen van behoorlijk bestuur van de Awb aan de inzet van DHE en de inzet van SS binnen het publieke domein?*

Hoofdregel is dat voor zover de verwerking van persoonsgegevens bij de inzet van MPC, zoals de inzet van SS of de inzet van DHE, voldoet aan de regels van de AVG, vaak ook wordt voldaan aan de algemene beginselen van behoorlijk bestuur (abbb's). Bij een verwerking van persoonsgegevens die voldoet aan de AVG is een nadere toets van de abbb's dus niet in alle gevallen strikt noodzakelijk.

Deze nadere toets van de abbb's is echter wel noodzakelijk bij de verwerking van anonieme gegevens. Dit overheidshandelen (feitelijke handelingen of rechtshandelingen) hoeft namelijk niet te voldoen aan de AVG (zie par. 5.1) maar moet wel voldoen aan abbb's. Daaraan kan ook worden getoetst door de daartoe bevoegde rechter op de vordering van een justitiabele die daarbij belang stelt te hebben en stelt dat sprake is van onrechtmatige verwerking van anonieme gegevens. Een aantal algemene beginselen zijn, vertaald naar de verwerking van *anonieme* gegevens, in het bijzonder van belang:[53]

Zorgvuldigheidsbeginsel
Op grond van het zorgvuldigheidsbeginsel moet de overheid bij de voorbereiding van de inzet van MPC de nodige kennis omtrent de relevante feiten en de af te wegen belangen vergaren. Het beginsel noopt ertoe dat de af te wegen belangen zorgvuldig worden bepaald, er een geschikte methode is om de belangen af te wegen en de belangenafweging in het kader van de vraag of de MPC zorgvuldig kan worden ingezet, vervolgens ook volledig is.

Evenredigheidsbeginsel
Bij de inzet van de MPC moet rekening worden gehouden met de belangen die spelen. De gevolgen van de verwerking mogen voor een belanghebbende niet onevenredig zijn in verhouding tot de te dienen doelen. Het evenredigheidsbeginsel vraagt dus van bestuursorganen dat zij stilstaan bij de vraag of een overheidshandeling in de concrete omstandigheden van dat specifieke geval niet leidt tot onevenredige gevolgen.

Motiveringsbeginsel
In het geval dat de inzet van MPC worden gebruikt ter motivering van een besluit, is ook het motiveringsbeginsel van belang. Een besluit van een bestuursorgaan moet gedragen worden door een deugdelijke motivering. Uit de motivering moet zowel blijken dat de feitenvaststelling juist is, als dat de vastgestelde feiten hebben kunnen leiden tot het genomen besluit.

---

[53] Voor zover de aard van de handelingen zich daartegen niet verzet, zie art. 3:1 lid 2 Awb. De abbb's zijn gecodificeerd in hoofdstuk 3 van de Awb.

Beperkte normering door abbb's bij inzet van DHE en SS

Als we de verwerking van anonieme gegevens ten behoeve van de inzet van MPC beschouwen vanuit het normerend perspectief dat de algemene beginselen van behoorlijk bestuur bieden, dan zien we de volgende normen en aandachtspunten.

De inzet van MPC is alleen mogelijk voor zover de anonieme gegevens die worden verzameld en gebruikt relevant zijn om het doel van de inzet te bereiken. De gegevens moeten actueel en juist zijn, en geschikt zijn voor het beoogde doel. Onder omstandigheden moet het bestuursorgaan transparant zijn over de wijze waarop MPC wordt inzet en het doel daarvan, en dat kenbaar maken aan betrokkenen. Daarbij moet de overheid desgevraagd kunnen motiveren waarom MPC wordt ingezet.

De verwerking van de anonieme gegevens en de inzet van MPC mag voor belanghebbenden geen onevenredige gevolgen hebben in verhouding tot de met de verwerking te dienen doelen. Ook dat moet de overheid kunnen motiveren. Dat brengt volgens ons met zich dat bij de inzet van MPC de relevante doelen, variabelen en de waardering van variabelen zorgvuldig moeten worden gekozen én gevalideerd. Ook moet de inzet van MPC voortdurend worden gemonitord/geëvalueerd.

De wijze waarop MPC wordt ingezet is overigens ook van betekenis voor de vraag of de gegevens en resultaten als bewijs kunnen worden gebruikt. Dat is niet het geval als de wijze waarop deze gegevens en resultaten zijn verkregen zozeer indruist tegen hetgeen van een behoorlijk handelende overheid mag worden verwacht, dat dit gebruik onder alle omstandigheden als ontoelaatbaar moet worden geacht.[54] Van schending van dit zogenoemde "zozeer indruist criterium" is niet snel sprake.

Worden de resultaten van de inzet van MPC gebruikt ten behoeve van de motivering van een besluit, dan moet aan de burger toegankelijk worden toegelicht welke resultaten hebben geleid tot de beslissing en of, en zo ja welke, automatische beslisregels zijn gebruikt. Ook moet worden toegelicht of het besluit mede voortbouwt op (geautomatiseerde) besluiten of gegevens van andere bestuursorganen. In het kader van het zorgvuldigheidsbeginsel moet bij de besluitvorming eveneens rekening worden gehouden met feiten en omstandigheden, desnoods in afwijking van geautomatiseerde beslisregels.[55]

[54] Zie het arrest van de Hoge Raad van 1 juli 1992, nr. 26331, BNB 1992/306, later onder meer bevestigd in de arresten ECLI:NL:HR:2004:AF5556 en ECLI:NL:HR:2015:643.

[55] Raad van State, 'Digitalisering. Wetgeving en bestuursrechtspraak', mei 2021, raadpleegbaar via: https://www.raadvanstate.nl/publicaties/studies-onderzoeken, p. 19 en 35.

6 CONCLUSIE

Door toepassing van MPC kunnen gegevens op een vertrouwelijke wijze beschikbaar worden gesteld voor berekeningen, zonder dat andere betrokken partijen inzage verkrijgen in de gegevens. Ook hoeft een groot deel van de gegevens niet (meer) te worden gedeeld met andere betrokken partijen. Voordeel van de toepassing van MPC is aldus dat de data-aanbieder meer regie houdt over zijn gegevens. Een ander voordeel van de toepassing van MPC is dat de privacyinbreuk van de beoogde berekeningen wordt verkleind.

Dat de data-aanbieder meer regie heeft en de privacyinbreuk wordt verkleind neemt niet weg dat er de (verdere) verwerkingen van de (persoons)gegevens bij toepassing van MPC moeten voldoen aan toepasselijke wet- en/of regelgeving. Toepassing van MPC kan evenwel met zich meebrengen dat juridische obstakels in de praktijk kunnen worden weggenomen. Afhankelijk van de context waarin een MPC wordt gebruikt en welke MPC wordt ingezet, kunnen juridische obstakels weggenomen worden door wijziging van bepaalde fundamenten van de MPC, bijvoorbeeld in de positionering van de datastations, de selectie van de inputdata en – in meer algemene zin – de inzet van SS in plaats van DHE of andersom. Deze wijzigingen van de fundamenten van MPC kunnen relevant zijn voor de vraag of een bepaalde verdere verwerking verenigbaar is conform artikel 6 lid 4 AVG, in strijd is met een geheimhoudingsplicht (zie paragraaf 5.3), voldoet aan het dataminimalisatiebeginsel (zie paragraaf 5.6) en of er bij die verdere verwerking bijzondere of strafrechtelijke gegevens worden verwerkt ten aanzien waarvan een zgn. verwerkingsverbod geldt (zie paragraaf 5.4). Mede om die reden adviseren wij vanaf de start van het MPC-traject de juridische aspecten – in samenhang met de technische aspecten – in ogenschouw te nemen.

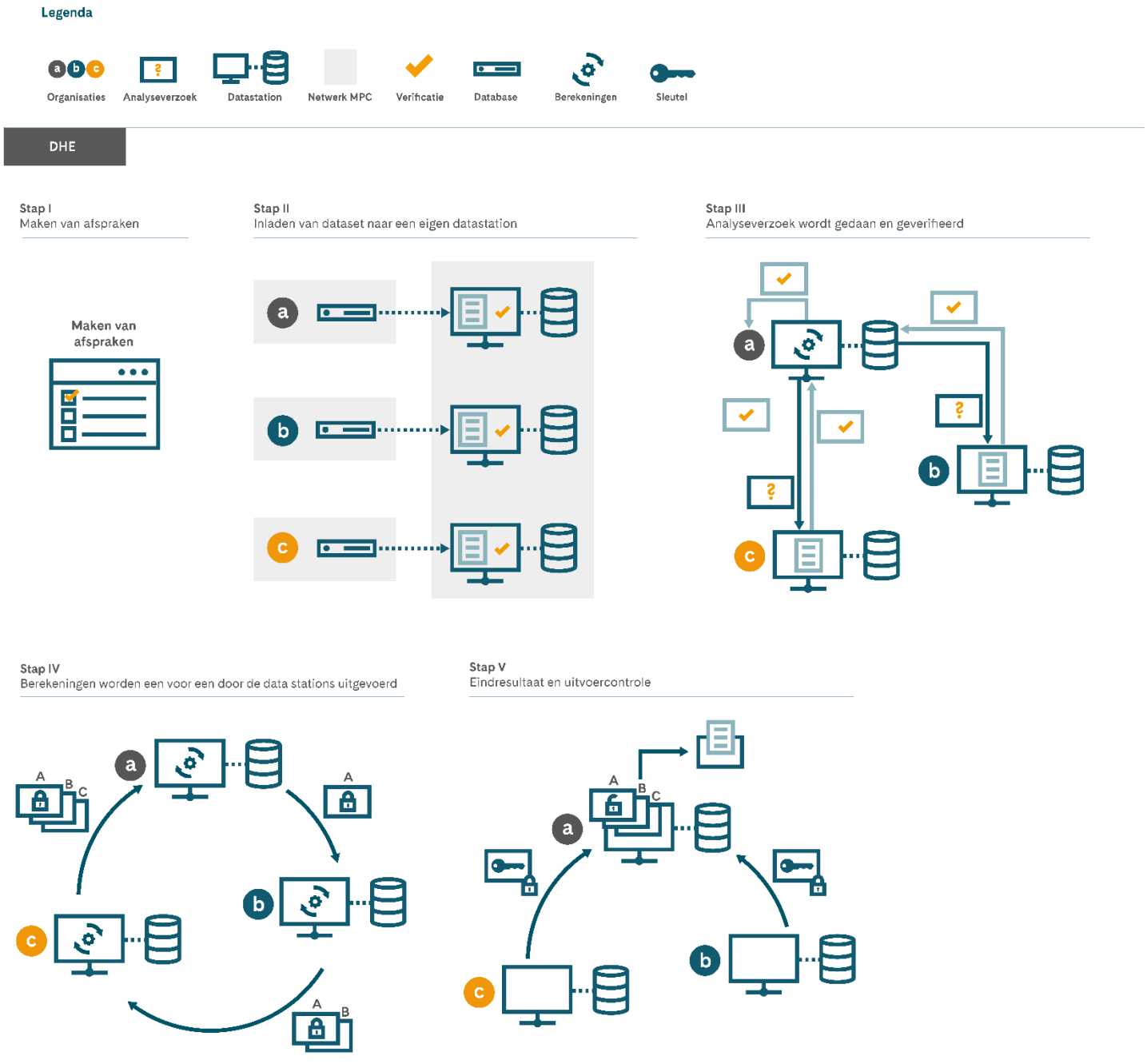
Disclaimer

Dit *whitepaper* is opgesteld door Pels Rijcken in opdracht van de Nederlandse Gaia-X hub, inmiddels onderdeel van het zogenaamde Centre of Excellence for Data Sharing & Cloud (www.coe-dsc.nl). Derden kunnen aan dit onderzoeksrapport geen rechten ontlenen. Mocht u vragen hebben over dit *whitepaper* of menen dat het *whitepaper* onjuistheden bevat, dan zijn wij daarvoor graag beschikbaar.

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.

Bijlage 1

Schematische weergave DHE



Bijlage 2

Schematische weergave SS