

aan DG

cc CPO, CSB-j, directeur CSB

van FG

onderwerp DPIAs bij het CBS

datum 15 december 2022

Advies over het uitvoeren van DPIAs bij het CBS

Aanleiding

De behoefte aan een vastomlijnde procedure rondom DPIAs en een strakkere lijn omtrent hun inhoud is ontstaan door:

- Een toename van het aantal gevallen waarin een specifieke DPIA vanuit het CBS wenselijk is, mede door een grotere behoefte aan transparantie en verantwoording richting betrokkenen en stakeholders
- Een toename van het aantal door samenwerkingspartners uitgevoerde DPIAs waarin het CBS de rol van gezamenlijk verwerkingsverantwoordelijke heeft
- Een toename van het aantal gevallen waarin door bronhouders een DPIA wordt uitgevoerd op de levering van data aan het CBS, waarbij het CBS de rol van ontvanger heeft
- Het ontbreken van beleid over de omgang met DPIAs bij het CBS en een toenemende behoefte aan duidelijkheid over de te volgen procedure

In dit advies komen de volgende punten aan de orde:

- De inhoud van een DPIA
- Persistent hoog risico voor betrokkenen
- DPIAs onder gezamenlijke verwerkingsverantwoordelijkheid
- DPIAs onder CBS-verwerkingsverantwoordelijkheid
- Governance van DPIAs bij het CBS
- Function creep bij DPIAs
- Wanneer een DPIA?

De inhoud van een DPIA

Volgens artikel 35 van de AVG moet een DPIA ten minste de volgende elementen bevatten:

- Een beschrijving van doel en middelen van de verwerking
- Een toets van de proportionaliteit en subsidiariteit van de verwerking in het licht van het doel
- Een beoordeling van de risico's van de verwerking voor de rechten en vrijheden van betrokkenen
- De technische en organisatorische maatregelen om deze risico's te adresseren en te mitigeren



In de praktijk wordt bij het CBS vaak gebruik gemaakt van het rijksoverheids-template voor DPIAs. Daarin komen de bovenstaande punten mede aan bod. Het staat het CBS uiteraard vrij om een eigen sjabloon te maken of een bestaand sjabloon aan te passen, indien wordt voldaan aan de minimeisen voor een DPIA uit de AVG en van de toezichthouders (Autoriteit Persoonsgegevens en European Data Protection Board). Daarnaast dient het CBS zich rekenschap te geven van zijn transparantieverplichtingen, en zich af te vragen of DPIAs proactief gepubliceerd moeten worden. De CBS-brede DPIA is al op de website van het CBS gepubliceerd.

Helaas lijkt bij de Rijksoverheid het maken van een DPIA vaak als een doel in plaats van een middel te worden gezien. Dat leidt tot lijvige documenten waarin vooral politieke en organisatierisico's worden besproken in plaats van een beoordeling van daadwerkelijke risico's voor de rechten en vrijheden van betrokkenen. Het doel van een DPIA is niet een zo lang mogelijk document, maar een adequate risicobeoordeling.

Persistent hoog risico voor betrokkenen

Wanneer in een DPIA wordt geconstateerd dat er een hoog risico voor betrokkenen resteert na het nemen van mitigerende maatregelen, zijn er twee mogelijkheden. De eerste is de voorziene gegevensverwerking niet uit te voeren. De tweede is de gegevensverwerking uit te stellen en de toezichthoudende autoriteit te verzoeken om een voorafgaande raadpleging. Naar aanleiding van de uitkomst daarvan kan de gegevensverwerking dan soms alsnog worden uitgevoerd, na het nemen van de door de toezichthouder geadviseerde maatregelen.

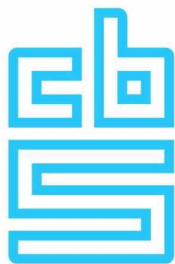
In de praktijk zullen deze situaties zelden ontstaan. Bij het uitvoeren van een DPIA is er doorgaans een wisselwerking tussen de aard van de verwerking en de te nemen maatregelen, waardoor het restrisico door de uitvoerder zelden op 'hoog' zal worden geschat. En de vraag is of de toezichthouder maatregelen kan bedenken die het CBS zelf niet kan voorstellen.¹ Toch moet met zo'n situatie wel degelijk rekening worden gehouden, bijvoorbeeld na een advies van de FG dat stelt dat er een hoog risico resteert.

DPIAs onder gezamenlijke verwerkingsverantwoordelijkheid

Onder de figuur van gezamenlijke verwerkingsverantwoordelijkheid moet duidelijk zijn welke partij zal voldoen aan welke verplichtingen uit de AVG. Dit betekent dat ten minste een deel van de uit te voeren DPIA in onderling overleg tot stand komt en vastlegt welke partij welke maatregelen toepast ter bescherming van de rechten en vrijheden van betrokkenen. Daarbij hoeft overigens geen vertrouwelijke informatie te worden gedeeld (bijvoorbeeld detailinformatie over de werking van technische beveiliging).

Omdat gezamenlijke verwerkingsverantwoordelijkheid een heldere toewijzing vereist van verplichtingen die betrekking hebben op rechten van betrokkenen (bijv. voldoen aan inzagerechten) en op de omgang met incidenten ('datalekken'), dienen bij uitstek risico's die voortvloeien uit die

¹ Zie ook het FG-advies over de voorafgaande raadpleging van 11 juli 2022.



gezamenlijkheid geadresseerd te worden in nauwkeurige afstemming tussen partijen. Het verdient aanbeveling de arrangementen onder gezamenlijke verwerkingsverantwoordelijkheid vanuit het CBS zo veel mogelijk te standaardiseren. Daarmee zijn verplichtingen helder en kan bij incidenten snel worden opgetreden.²

DPIAs onder CBS-verwerkingsverantwoordelijkheid

Indien een verwerking uitsluitend onder CBS-verwerkingsverantwoordelijkheid plaatsvindt, is het aan het CBS zelf om de afweging te maken of een DPIA noodzakelijk is. Het is wenselijk de bestaande algemene criteria daarvoor (afkomstig uit de AVG, van de EDPB en van de Autoriteit Persoonsgegevens) te vertalen naar de CBS-situatie. Idealiter worden deze vertaalde criteria onderdeel van de standaard CBS-DPIA of van een aan te bieden DPIA-sjabloon, zodat deze mede geschikt is als intern instrument om een afweging te maken of een aanvullende, specifieke DPIA noodzakelijk of wenselijk is.

Belangrijk is in dit soort gevallen het bereik van de DPIA niet op te rekken buiten tot buiten het proces waarvoor het CBS verwerkingsverantwoordelijkheid heeft. Bijvoorbeeld: indien de leveringsportal onder beheer van het CBS staat, en deel uitmaakt van de voorziene verwerking, valt deze onder het bereik van de uit te voeren CBS-DPIA. Als de levering plaatsvindt via een middel van een bronhouder, valt dat middel buiten het bereik.

Governance van DPIAs bij het CBS

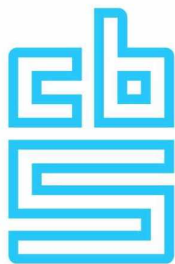
Het is wenselijk dat er beleid wordt gemaakt over de omgang met DPIAs bij het CBS. Dit beleid zou de volgende onderwerpen moeten adresseren:

- Wie is verantwoordelijk voor de beoordeling of een volledige DPIA noodzakelijk is
- Wie is verantwoordelijk voor de uitvoering van de DPIA
- Wie geeft er akkoord op de inhoud van de DPIA
- Wie geeft er akkoord op de uitvoering van het beoordeelde proces of project, gegeven de vastgestelde inhoud van de DPIA
- Welke rol hebben privacycoördinatoren, CPO en FG³

Omdat het uitvoeren van een DPIA geen louter papieren exercitie moet zijn, is het van belang de uitvoering zo dicht mogelijk bij de daadwerkelijke (toekomstige) uitvoering van het project of proces te beleggen. Voor de proportionaliteits- en subsidiariteitstoets is het belangrijk voldoende (interne of externe) tegenspraak te organiseren en goed te kijken naar de algemene beginselen uit artikel 5 van de AVG, waaronder dataminimalisatie.

² In een binnenkort uit te brengen advies zal ik nader ingaan op de figuur van gezamenlijke verwerkingsverantwoordelijkheid in samenwerkingen en de risico's daarvan.

³ Voor wat betreft de rol van de FG adviseer ik deze te raadplegen indien er onduidelijkheid bestaat of een DPIA noodzakelijk of wenselijk is, en te betrekken bij de vraagarticulatie en om advies op het eindproduct te vragen voordat tot goedkeuring van de DPIA in de eerste lijn wordt besloten.



De tegenspraak kan bijvoorbeeld komen van privacycoördinatoren, de CPO, de FG of van een externe terzake deskundige. Afhankelijk van de aard van de verwerking dient interne expertise te worden aangehaakt op het gebied van IT-beveiliging, de allocatie van AVG-rollen, dataminimalisatie en privacy by design.

De rol van de FG zal conform de AVG liggen in de (algemene) advisering over of een DPIA moet worden uitgevoerd, hoe deze in een specifiek geval het beste vorm kan krijgen, en in een advies op het finale product, voorafgaand aan het besluit tot akkoord of niet-akkoord in de eerste lijn.

De standaard-DPIA van het CBS

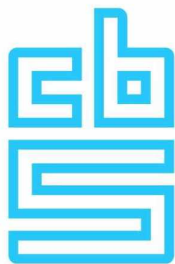
Het CBS werkt met een standaard-DPIA. Deze voorziet in een beoordeling op de criteria uit artikel 35 AVG op standaard statistische processen. Omdat deze DPIA een groot bereik heeft en ook in veel gevallen voldoende inzicht moet bieden aan derde partijen en – in het kader van transparantieverplichtingen uit de AVG – aan betrokkenen, adviseer ik een herziening van de huidige DPIA, waarbij de volgende zaken in aanmerking worden genomen:

- Leg de nadruk op de risico's voor betrokkenen
- Leg uit hoe deze risico's worden verminderd, in zo begrijpelijk mogelijke termen, door een overzicht van technische en organisatorische maatregelen
- Houd de uitleg zo kernachtig mogelijk
- Maak het mogelijk om vanuit specifieke DPIAs op een eenvoudige wijze te verwijzen naar 'bouwstenen' in de standaard-DPIA om dubbel werk te voorkomen
- Eventueel kan worden overwogen een aantal stappen in het statistisch proces duidelijker apart toe te lichten in de standaard-DPIA, zoals bijvoorbeeld dataverzameling en -verwerking
- In specifieke DPIAs zou de nadruk moeten liggen op het beoordelen van proportionaliteit en subsidiariteit, extra risico's voor betrokkenen en mitigering daarvan; zij vormen idealiter uitsluitend een aanvulling op de standaard-DPIA

Function creep bij DPIAs

Zoals hierboven vermeld, wordt een DPIA vaak gebruikt voor andere doeleinden dan waarvoor deze in het leven is geroepen. Hoewel ik daartegen stelling neem, is een DPIA mede geworden tot een politiek indekkingsinstrument. Indien daarvan sprake is, verdient het aanbeveling vast te houden aan de volgende randvoorwaarden:

- De standaard-DPIA van het CBS moet een voldoende instrument zijn om de risico's voor betrokkenen van de standaard-statistische processen te beoordelen en adequaat te mitigeren. Het is niet de bedoeling deze exercitie bij elk nieuw onderzoek opnieuw uit te voeren, *tenzij* er relevante nieuwe kenmerken aan de orde zijn. In dat geval dienen die nieuwe, afwijkende kenmerken beoordeeld te worden, niet het proces als geheel.
- De zelfstandige verwerkingsverantwoordelijkheid van het CBS dient door bronhouders gerespecteerd te worden. Dit brengt met zich mee dat doel en middelen van de verwerking door het CBS bepaald worden en de bronhouder daar niet in mag treden. Doet de bronhouder dit wel, dan loopt zij het risico gezamenlijk verwerkingsverantwoordelijke te worden, met alle eventuele reputatie- en aansprakelijkheidsrisico's vandien.



Wanneer een DPIA?

Een DPIA moet in algemene zin worden uitgevoerd wanneer een verwerking een hoog risico voor de rechten en vrijheden van betrokkenen inhoudt. Deze moet voorafgaan aan de verwerking, dus voor de start van een project of proces, ook als het een pilotproject betreft. Om invulling te geven aan de wens tot meer duidelijkheid over de omstandigheden waaronder een DPIA moet worden uitgevoerd, worden er nadere aanwijzingen gegeven in art. 35 AVG, door de toezichthouders en door de European Data Protection Board. In deze paragraaf noem ik de omstandigheden die voor het CBS het meest van belang zijn:

- Grootschalige verwerking een of meer van de volgende categorieën gegevens:
 - o bijzondere persoonsgegevens, waaronder genetische en gezondheidsgegevens, en strafrechtelijke gegevens;
 - o financiële gegevens waaruit bijvoorbeeld de inkomens- of vermogenspositie van mensen is af te leiden;
 - o locatiegegevens;
 - o communicatiegegevens;
 - o 'internet of things' gegevens, bijv. energiemeters
- Grootschalige controle van werknemers, bijvoorbeeld monitoring
- Profileren van individuen, bijv. door middel van gezondheidsindicatoren
- Grootschalige observatie van gedrag langs geautomatiseerde weg, bijv. door WiFi-tracking of slimme camera's
- Koppeling van databases
- Verwerking van gegevens over kwetsbare personen, bijvoorbeeld kinderen
- Gebruik van nieuwe technologieën

Gemakshalve kunnen we ervan uitgaan dat elk statistisch proces grootschalige verwerking inhoudt en dat er altijd gegevens worden gekoppeld. De afweging of een specifieke DPIA moet worden uitgevoerd kan mede worden gemaakt op basis van de volgende criteria:

- In hoeverre de nieuwe verwerking volledig past in de bestaande primaire processen van het CBS, en bronnen, methoden, technieken en rapportage zijn afgedekt in de standaard-CBS-DPIA
- In hoeverre de input voor een proces zich kenmerkt door nieuwe bronnen met hierboven genoemde gegevenstypen of door een nieuwe wijze van data verzamelen, bijv. met behulp van sensoren, apps of web-scraping
- In hoeverre de verwerking van gegevens door nieuwe koppeling van bronnen (nieuwe dwarsverbanden) of nieuwe verwerkingsmethoden nieuwe risico's voor betrokkenen oplevert, bijvoorbeeld in de vorm van tot het individu herleidbare indicatoren voor de gezondheid, financiële positie of arbeidsmarktkansen (ook als deze slechts binnen het proces tot stand komen en geen onderdeel zijn van de output van het proces)
- In hoeverre de output van een statistisch proces wordt gebruikt of kan worden gebruikt om algoritmes te trainen die geschikt zijn voor de profilering van individuen, indien het CBS daar redelijkerwijs (mede) controle over heeft (bijvoorbeeld bij RA-toegang), of de output op een andere manier nieuwe kenmerken heeft, zoals een wezenlijk nieuwe presentatiewijze of nieuw type aggregaat