

aan Directeur SVV, Hoofd SVV
 cc CPO, privacycoördinatoren SER
 van FG en plvFG

onderwerp Advies FG op DPIA verkrijging en verwerking ANPR-gegevens tbv VESDI
 datum 7 augustus 2023

Ik heb kennisgenomen van de inhoud van de DPIA die door Privacy Company in samenwerking met andere partijen is opgesteld, en waarvan de definitieve versie is vastgelegd op 13 juli 2023. In overleg met het hoofd SVV heb ik al enkele opmerkingen doorgesproken en daarop feedback ontvangen. Mede naar aanleiding daarvan geef ik in dit document mijn definitieve advies bij de DPIA. Als FG hecht ik de meeste waarde aan enerzijds de proportionaliteits- en subsidiariteitstoets van de verwerking en anderzijds de inventarisatie van risico's voor betrokkenen en de mitigering daarvan.

Nadere opmerkingen over risico's uit de DPIA

Allereerst plaats ik een aantal opmerkingen over de risico's die in de DPIA zijn genoemd:

Risico 1 Niet voldoen aan beginsel van dataminimalisatie

In de DPIA wordt het vermijden van opentekstvelden als mitigerende maatregel genoemd. Navraag leert dat deze er, zoals te verwachten viel, in het beoogde proces niet zijn. Als ze er zouden zijn, zouden ze moeten worden uitgefilterd voor levering of direct bij binnenkomst bij het CBS. Behoudens uitzonderingen zijn opentekstvelden niet bruikbaar voor het maken van statistieken en mogen zij dus ook niet bewaard worden door het CBS. Deze mitigerende maatregel treft dus geen doel.

Over dataminimalisatie valt in dit traject meer te zeggen. Ik sluit hierbij aan op mijn recente advies over dataminimalisatie bij het CBS d.d. 26 juni 2023. Toegepast op de casus gelden dan onder meer de volgende aanwijzingen:

- Zo vroeg mogelijk pseudonimiseren van identificerende gegevens. De filtering van personenvoertuigen moet zo vroeg mogelijk plaatsvinden. Dat zou betekenen dat gemeenten of hun verwerkers over dit kenmerk moeten kunnen beschikken. De filterverwerking vindt dan gedistribueerd over alle deelnemende gemeente plaats, met extra risico's vandien. Gekozen is voor centrale filtering en verwijdering bij het CBS. Dat is later in het proces, maar gaat met minder (verschillende) verwerkingen gepaard. Het CBS pseudonimiseert de kentekens direct daarna. De herkeningsrisico's op basis van andere attributen (tijd en plaats) worden iteratief geadresseerd door dynamisch te aggregeren.
- Hoe dichter statistieken bij de werkelijkheid komen, hoe meer er moet worden gelet op onthullingsrisico. Daarbij moet er goed worden gelet op de verbodsbepaling uit art. 37 lid 3 CBS-wet. Bedrijfsmobiliteitsstatistieken op gemeentelijk niveau dragen een verhoogd risico in zich van onthulling van gegevens van individuele bedrijven. Zoals gebruikelijk is in het traject waarop de DPIA ziet een CBS-expert op het gebied van statistische geheimhouding



aangehaakt. De granulariteit van zowel tijdvensters als locaties dient op een voldoende laag niveau te worden gehouden.

- De filtering van personenwagenkentekens en de daarbij behorende tijd- en locatie-attributen dient zo snel mogelijk en onomkeerbaar te worden uitgevoerd. De toegang tot deze bestanden dient tot het minimale aantal personen gereduceerd te worden.

Risico 3 Beveiliging van de verwerking ontoereikend en Risico 4 Onduidelijkheid wijze van verstrekken

Uit het CBS-incidentenregister blijkt dat gemeenten regelmatig verzamelde microdata per e-mail opsturen. Dat is onvoldoende veilig en mogelijk een symptoom van de kennis en het bewustzijn over informatiebeveiliging bij gemeenten. Ook is er bij het CBS aandacht nodig voor dit probleem – de oppervlakkige lezer van veel CBS-webpagina's ziet een prominent vermeld e-mailadres (voor informatie over leveringen) maar zou de indruk kunnen krijgen dit adres dient om microdata toe te sturen. De frequentie van dit type incidenten zou aanleiding moeten zijn om als CBS de communicatie over het eigen leveringsbeleid te evalueren.

Risico 5 Verstrekking van locatiegegevens door CBS op basis van opsporingsverzoeken

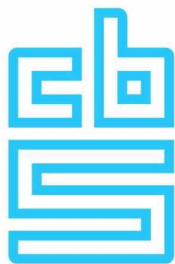
De frequentie waarmee overheidsinstellingen aan de poort van het CBS blijven rammelen is een punt van zorg. Kennelijk leeft niet bij alle overheidsinstellingen het besef dat het CBS alleen kan bestaan bij de gratie van het vertrouwen van burgers en bedrijven dat de verstrekte gegevens alleen voor statistisch en wetenschappelijk onderzoek mogen worden gebruikt, en dat microdata nimmer voor andere doeleinden mogen worden verstrekt. Zulks zou rechtstreeks in strijd zijn met de letter en geest van de CBS-wet, meer specifiek de taak in art. 3 en het verbod op doorverstrekking uit art. 37 lid 2. Ook onder art. 41 is uitsluitend statistisch en wetenschappelijk onderzoek op microdata toegestaan. In principe is dit risico niet alleen van toepassing op de verwerking die onderwerp is van deze DPIA. Het risico inclusief mitigerende maatregelen zou dan ook aandacht moeten krijgen in een nieuwe versie van de CBS-brede DPIA.

Overige risico's

Daarnaast heb ik een aantal aanvullende risico's geïdentificeerd. Wellicht kan SVV, voor zover mogelijk, nog een aantal aanvullende mitigerende maatregelen bedenken om deze risico's te adresseren, voorzover de sector het bestaan van deze risico's erkent.

Aanvullend risico A: verzamelwoede

De inzet van ANPR-camera's heeft specifieke doeleinden voor gemeenten. Hier speelt het bekende en in de DPIA geïdentificeerde risico van 'function creep'. Staan de camera's er eenmaal, dan worden ze ook voor andere doeleinden ingezet. Het gebruik van eenmaal geregistreerde gegevens voor gebruik voor statistische en wetenschappelijke doeleinden is geregeld in art. 5 lid 1 onder b jo. art. 89 lid 1 AVG. Dat gebruik is legitiem. Het risico dat ik met betrekking tot de voorziene verwerking identificeer, is 'collection creep' ofwel 'verzamelwoede'. Dit is het risico dat met het oog op een verlengd statistisch of wetenschappelijk doel de mate waarin gegevens worden verzameld wordt opgerekt, niet voor het primaire doel, maar voor het verlengde gebruik.



Een voorbeeld hiervan: een ANPR-camera wordt gebruikt voor matching tegen een 'blacklist' van gesignaleerde voertuigen. Voor dit doel kan na herkenning van het kenteken en het ontbreken van een overeenkomst met de blacklist dat kenteken meteen verwijderd worden. Zou je nu de zelfde ANPR-camera ook willen gebruiken voor tellingen van voertuigen gegroepeerd naar categorie (personenwagen, bestelbus, autobus, vrachtwagen), dan zul je ofwel relatief onbetrouwbare beeldherkenningssoftware moeten inzetten, ofwel elk kenteken tegen het kentekenregister van de RDW moeten houden. De mogelijkheid om meteen daarna de kentekens weg te gooien, bestaat nog steeds, maar dan is er geen latere mogelijkheid tot nadere categorisering (bijv. elektrisch voertuig versus voertuig op fossiele brandstof). Het wordt dan erg verleidelijk geen van de verzamelde kentekens weg te gooien. Dat is een geval van verzamelwoede.

Hoewel het gebruik van microdata door het CBS als verlengd gebruik in principe altijd legitiem is als de proportionaliteits- en subsidiariteitstoets met betrekking tot het verlengd gebruik zijn geslaagd en voldaan wordt aan de overige beginselen uit art. 5 AVG, ontkomen wij niet geheel aan een toets van het voor- en natraject van de statistische verwerking. Dit betekent dat het CBS de ogen open moet houden voor de rechtmatigheid van de gegevensverzameling en voor het verdere gebruik van de aggregaten na publicatie.

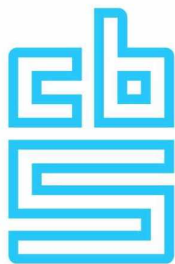
Aanvullend risico B: volgen routes van individuele bestuurders

Naarmate er gegevens worden verzameld van bedrijven met een kleinere vloot van bedrijfswagens, wordt de kans op herkenning van routes van individuele bestuurders groter. Dat geldt des te meer naarmate ritten en routes over een langere periode worden bewaard. Ook het verRINnen (vervangen van kentekens door een vast pseudoniem) staat niet principieel in de weg aan een herkenningsrisico. Vraag is dan ook of een aanvullende mitigerende maatregel zoals het per dag pseudonimiseren, met wisselende pseudoniemen, van ritten en routes mogelijk zou zijn, zoals toegepast in de verwerking van OV-chipkaartdata.

Aanvullend risico C: hogeresolutiestatistieken

De weg van statistieken op basis van steekproeven en enquêtes naar statistieken op basis van registers en 'smart surveys', waaronder de inzet van sensoren, leidt potentieel tot een steeds grotere nauwkeurigheid van gebruikte data, en daarmee ook tot meer specifieke statistieken. De doelstellingen van statistisch onderzoek voor de energietransitie kunnen dan ook opgerekt worden naar een niveau waarop minder of geen sprake is van aggregaten. Een beleidskwestie als 'het aantal benodigde laadpalen' kan zomaar worden vertaald naar de 'exacte locatie van elk van de benodigde laadpalen'.

De neiging om hogeresolutiestatistieken te vragen (hoe preciezer de uitkomst, hoe beter) leidt op haar beurt ook weer tot een hogere benodigde precisie van de gebruikte data. En hoe hoger de precisie van gebruikte data en specificiteit van de statistiek, hoe groter het onthullingsrisico. Gegeven het onthullingsverbod op persoons-, huishouden- en instellingsniveau ex art. 37 lid 3 CBS-wet moet het CBS zich rekenschap geven van de risico's die het loopt om bij hogeresolutiestatistieken te sterk in te zoomen op de werkelijkheid. Dit risico is ook al aangegeven bij de bespreking van risico 1 (dataminimalisatie) maar zou ook onderwerp moeten zijn van een bredere discussie, mede naar



aanleiding van de 'invoering' van de vierde enquetemodaliteit 'smart surveys' over waar de grenzen van de waarneming en van de statistiek liggen.

Aanvullend risico D: papieren tijger

Hoewel het instrument van de DPIA een wettelijk gegeven is, waarvan de inzet in art. 35 AVG wordt geadresseerd, heb ik mij samen met de interne initiatoren van de DPIA verbaasd over de beperkte werkbaarheid van het toetsingsmodel. Het uitvoeren van een DPIA is als zwemmen op het droge. In het geval van het maken van een statistiek ontcom je er niet aan om voor een goede beoordeling van benodigde gegevens interactie te hebben tussen bronhouder en CBS. Eigenlijk zou een deel van de DPIA pas uitgevoerd moeten worden tijdens de experimentele/proof of concept fase van het maken van de statistiek.

Zonder deze aanvullende fase loop je het risico dat de uitgevoerde DPIA in de praktijk een papieren tijger blijkt. Uiteraard houdt het CBS zich aan de wet, en voert dus vooraf een DPIA uit. Toch zou ik het toejuichen als een iteratief proces wordt gekoppeld aan de initiële DPIA, waarbij gaandeweg de experimentele fase een hernieuwde beoordeling van geconstateerde risico's voor de betrokkene plaatsvindt. Dat doet ook meer recht aan de geest van de DPIA, die immers hopelijk door niemand als 'afgetekende papieren exercitie die in een lade verdwijnt' wordt gezien. Zo'n papieren tijger zal de rechten van betrokkenen maar beperkt kunnen beschermen.

Ook bij het beëindigen van een DPIA aan het begin van de uitvoering van het statistische proces kan nog een adequaat vervolg worden gegeven aan de geïdentificeerde risico's. Door periodiek bij te houden hoe de voorgestelde maatregelen adequaat de risico's voor betrokkenen mitigeren, kan de PDCA-cyclus voor de privacyborging van het proces vorm krijgen. Ik heb hierbij een hogere frequentie voor ogen dan de vaak geadviseerde 3-jaars periodieke herziening van de DPIA zelf.