



# Kaders voor innovatieve projecten, ASD en samenwerken met derden.

5.1.2.e

projectnummer    Klik en typ projectnummer  
                          Klik en typ sector  
                          3 mei 2021

samenvatting    Klik en typ de samenvatting  
trefwoorden    Klik en typ de trefwoorden

## 1. Inleiding

CBS zoekt actief naar nieuwe wegen om statistiek te maken. De enorme toename van de hoeveelheid beschikbare data en de enorme verscheidenheid daarin bieden daarvoor ruimschoots mogelijkheden. Onderzoek op big data staat volop in de belangstelling, ook buiten de eigen organisatie. Ook onderzoek waarbij meerdere partijen actief participeren bij het verwerken van soms decentraal opgeslagen data komt steeds vaker voor. Samenwerking ligt dus voor de hand. Multi party computation (MPC) is vaak een gebruikte term.

De RA-omgeving van het CBS is een voorbeeld waarbij andere partijen onderzoek doen op CBS-data. Om dit mogelijk te maken zijn er regels opgesteld waarbij als belangrijke pijlers de betrouwbare geïsoleerde IT-omgeving, de inputcontrole (incl. projectplan, instelling, onderzoeker) en de outputcontrole op onthulling.

Dergelijke waarborgen zullen ook gezocht moeten worden bij nieuwe type verwerkingen waarbij de data niet meer allemaal op het CBS staat, waarbij de onderzoekers uit verschillende instellingen afkomstig zijn en natuurlijk waarbij vertrouwelijke CBS-data verwerkt wordt. Uitgangspunt blijft nog steeds dat het CBS geen data host en dat het CBS geen TTP is. De CBS-wet blijft het kader maar vraagt wel een nieuwe vertaling naar maatregelen om aan de wettelijke eisen te voldoen.

Deze nota is bedoeld als een soort handleiding welke door projectleiders nagelopen kan worden als eerste aanzet om te komen tot een afgewogen projectplan en -aanpak.

## 2. Wettelijke kaders

Bij het CBS hebben we voornamelijk te maken met de CBS-wet en de AVG. Maar als meerdere partijen betrokken zijn en met name ook als de data op locatie buiten het CBS staat bij de bronhouder, dan zijn er vaak ook andere wetten en kaders van toepassing.

Als de statistische eenheid personen zijn, gaat het al snel om veel zeer privacygevoelige informatie. Maar ook als het niet gaat om privacygevoelige data is het garanderen van de vertrouwelijkheid er van vaak wel een vereiste.

Door de omvang van de hoeveelheid data, de aard van die data en het feit dat die data soms real-time beschikbaar is, is het traditionele instrumentarium voor het waarborgen van de privacy van actoren mogelijk niet automatisch bruikbaar of effectief. Een vaste, of standaard werkwijze is daardoor vermoedelijk ook niet altijd mogelijk. Bescherming van de privacy en beveiliging van informatie zijn voor CBS echter wel absolute voorwaarden. Daarom is hieronder getracht om onze (niet onderhandelbare) uitgangspunten op dit gebied te verwoorden. Deze kunnen worden gehanteerd als handleiding om binnen een samenwerkingsproject te beoordelen of aan de eisen voor privacybescherming en informatiebeveiliging wordt voldaan.

### 3. Statement

CBS garandeert dat gegevens die voor statistisch onderzoek worden gebruikt vertrouwelijk blijven. De gegevens worden waar mogelijk geanonimiseerd en uitsluitend medewerkers die dat voor hun werk nodig hebben, krijgen er toegang toe. Er wordt volledig voldaan aan de eisen van de privacy wetgeving. Voor de afscherming en beveiliging van de gegevens zijn strikte maatregelen getroffen die voldoen aan alle gangbare beveiligingsnormen.

### 4. Taken CBS

Het CBS kan derden op verschillende manieren ten dienste staan conform de CBS-wet:

1. Op de reguliere wijze met anonieme statistische informatie al dan niet ASD (artikel 37)
2. Met microdata welke passend beschermd is conform artikel 41 van de CBS-wet (RA en fysieke levering) aan een selectie groep instanties.
3. Paragraaf 3 CBS-wet geeft nog een paar specifieke uitzonderingen aan met wetenschappelijke of technische ondersteuning (artikel 3 lid 2 van de CBS-wet).
  - a. Dit kan puur technisch zonder dat er data verwerkt wordt;
  - b. Bij verwerking van data kan het louter op data welke de derde partij al daadwerkelijk bezit. Het liefst op locatie bij die derde. Maar er is ook een optie om de data tijdelijk naar het CBS te halen, te verwerken en daarna te retourneren. Deze laatste optie is beschreven in Basisprincipes bij verwerkingen van microgegevens bij werk voor derden v3.docx. Optie 3.1. In beide gevallen zou het CBS zou dan verwerker moeten zijn. Ook kan het in een samenwerkingsvorm met goede afspraken over governance.
4. Er zijn een paar specifieke uitzonderingen in de CBS-wet genoemd. Denk aan doodsoorzaken, DNB en Eurostat. Ook zijn er andere wetten, richtlijnen waarvoor

uitzonderingen zijn (Buitenlandsehandel, Onderwijs, Gemeenten, WOZ-waarde, Bijstandsuitkeringen etc.

## 5. Uitgangspunten / checklist

De belangrijkste wettelijke kaders voor verwerking van vertrouwelijke data zijn de CBS-wet en de privacy verordening (AVG).

De AVG gaat er vanuit dat voor (nieuwe) verwerkingen van persoonsgegevens een 'privacy impact assessment', de **DPIA**, wordt uitgevoerd als op grote schaal bijzondere persoonsgegevens of strafrechtelijke gegevens verwerkt worden. Daarmee worden de privacy en beveiligingsaspecten getoetst. Het CBS heeft een standaard DPIA welke voor het merendeel van de huidige type verwerkingen van toepassing is. Voor nieuwe type verwerkingen, denk aan geheel nieuwe manieren van verwervingen of analyses (Big Data, AI zijn een voorbeeld) is het vereist te starten met een DPIA. Bij samenwerkingsverbanden is het aan te bevelen ook daar een DPIA uit te voeren.

Bij iedere verwerking van persoonsgegevens horen er drie vragen gesteld te worden:

1. **Willen** wij als organisatie deze verwerking uitvoeren? Dit is een vraag voor het '**beleid**';
2. **Mogen** wij als organisatie deze verwerking wettelijk uitvoeren? Een vraag voor de **juristen**;
3. **Kunnen** wij deze verwerking daadwerkelijk uitvoeren? Een vraag voor de '**technici**'.

**Zowel de CBS-wet als de AVG stellen:**

- Bij de verwerking van vertrouwelijke gegevens worden maatregelen getroffen ter beveiliging tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens.

**Belangrijkste eisen ontleent aan de CBS-wet:**

- Door CBS verzamelde en aan CBS ter beschikking gestelde gegevens worden gebruikt voor statistisch onderzoek.
- CBS publiceert alleen statistische informatie als individuele personen, bedrijven of instellingen niet herkenbaar of herleidbaar zijn. Output moet worden gecontroleerd op onthulling.
- CBS levert nooit gegevens over individuele personen, bedrijven of instellingen aan derden, ook niet aan andere overheidsinstellingen. Uitzonderingen vallen onder artikel 41 van de CBS-wet of andere wet- en regelgeving (zie hoofdstuk 4 punt 4).
- Ten behoeve van eigen onderzoek of onderzoek in samenwerking met CBS kunnen geautoriseerde instellingen onder strenge voorwaarden toegang krijgen tot (geanonimiseerde of gepseudonimiseerde) microdatabestanden van CBS.
- De resultaten van dergelijk onderzoek worden openbaar gemaakt onder dezelfde voorwaarden als die voor CBS publicaties gelden.
- Ten behoeve van dergelijk onderzoek kunnen gegevens op persoons- of bedrijfsniveau worden gekoppeld met eigen gegevens van de geautoriseerde instelling, mits deze gegevens rechtmatig

mogen worden verwerkt (denk aan specifieke wetgeving, voorwaarden waaronder gegevens zijn verstrekt, noodzaak van informed consent, etc.).

**Belangrijkste eisen voortvloeiend uit de privacywetgeving:**

- Voor verwerking van persoonsgegevens moet een grondslag bestaan. De uitvoering van een publiekrechtelijke taak in het algemeen belang, zoals de **taak van het CBS**, geldt als rechtmatige grondslag.
- Dataminimalisatie is binnen de privacywetgeving een belangrijk criterium. Vooraf dient aangegeven te worden met welke doel persoonsgegevens worden verwerkt en dient te worden onderzocht of er geen andere wegen open staan om eenzelfde resultaat te bereiken met minder of zonder persoonsgegevens. De verwerking moet **noodzakelijk** zijn om het doel te bereiken.
- Voor bewerkers van persoonsgegevens geldt een wettelijke geheimhoudingsplicht (zij ondertekenen daartoe een geheimhoudingsverklaring). De geheimhoudingsplicht geldt ook nadat het onderzoek is afgerond.
- Voor de verwerking van **bijzondere persoonsgegevens** is nadrukkelijke toestemming van betrokkenen vereist, tenzij:
  - het onderzoek een algemeen belang dient,
  - de verwerking voor het betreffende onderzoek of de betreffende statistiek noodzakelijk is,
  - het vragen van uitdrukkelijke toestemming onmogelijk is of een onevenredige inspanning kost,
  - bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.
- Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.
- Een inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.
- Let op bij het verwerken van **BSN**. Daar kunnen aanvullende regels voor gelden bij de derde partij.

De eis “tot beveiliging tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens” is geoperationaliseerd in een groot aantal maatregelen. Als norm voor het niveau van de beveiliging geldt de Baseline informatiebeveiliging Overheid (BIO) of een vergelijkbaar (gelijkwaardig) niveau.

**Belangrijkste eisen met betrekking tot de beveiliging:**

- Verwerking van vertrouwelijke gegevens vindt uitsluitend plaats binnen de goed beveiligde IT-omgeving van het CBS.
- Voor toegang tot vertrouwelijke gegevens is toestemming van de eigenaar noodzakelijk.
- Toegang tot de beveiligde IT-omgeving is afgeschermd door middel van minimaal twee-factor-authenticatie.
- Het is niet toegestaan om vertrouwelijke gegevens buiten die beveiligde IT-omgeving te brengen.
- Vertrouwelijke gegevens die zich (met toestemming) buiten de beveiligde IT-omgeving bevinden (op datadragers, mobiele apparatuur, tijdens transport, etc.) zijn altijd versleuteld.

- Het gebruik van de **cloud** wordt vooraf door het CBS getoetst. Dit geldt ook voor **IT-tools** welke niet tot de standaard behoren van het CBS. **Raadpleeg SSC.**

#### **Samenwerken met derden en ASD.**

Ook bij samenwerken geldt nog steeds de geldende wet- en regelgeving. Onder het mom van samenwerking mag bijvoorbeeld nog steeds geen **onthullende** individuele data met derden gedeeld worden. Ook geldt dat het CBS **onafhankelijk** blijft in de keuze van de statistische methoden, publicatievorm en publicatietijdstip zoals geformuleerd in de CBS. Dit is met name bij **ASD** een aandachtspunt. Er is aanvullende regelgeving m.b.t. cont(r)acten met commerciële partijen. Neem bij twijfel contact op met de accountmanager en/of de CSB-juristen., CNO. ASD kent ook een **stuurgroep** voor High impact ASD.

#### **Ethische commissie**

Het CBS heeft een ethische commissie die in geval van ethische dilemma's om advies gevraagd kan worden.