

De AVG en PPT:

een winstwaarschuwing van de FG bij verwerking persoonsgegevens met Privacy Perserving Techniques.

5.1.2.e

5.1.2.e

CBS

projectnummer Klik en typ projectnummer
 Klik en typ sector
 29 september 2020

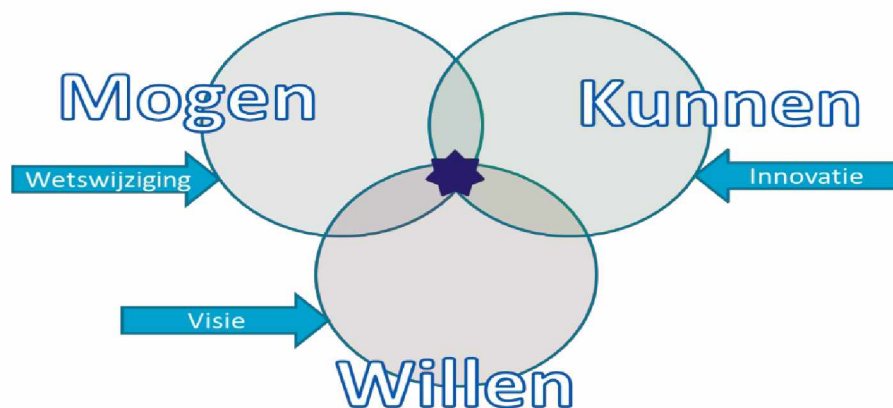
samenvatting Klik en typ de samenvatting
trefwoorden Klik en typ de trefwoorden

1. Inleiding

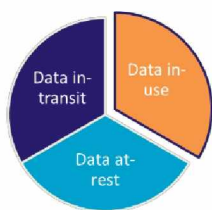
Privacy Perserving Techniques (PPT) worden steeds meer onderzocht en toegepast. Soms bestaat het idee dat bij PPT de AVG niet of minder van toepassing is. In deze nota krijgt PPT de plek welke het toekomt. Bij iedere verwerking van persoonsgegevens horen er drie vragen gesteld te worden:

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**'.

PPT worden gebruikt om persoonsgegevens te verwerken voor het maken van berekeningen zonder dat deze gedecrypt hoeft te worden en vallen daarmee onder het derde punt: 'kunnen'. Maar er bestaat een link met de eerste twee punten: willen en mogen. In deze notitie gaat het met name om het aspect 'mogen'.



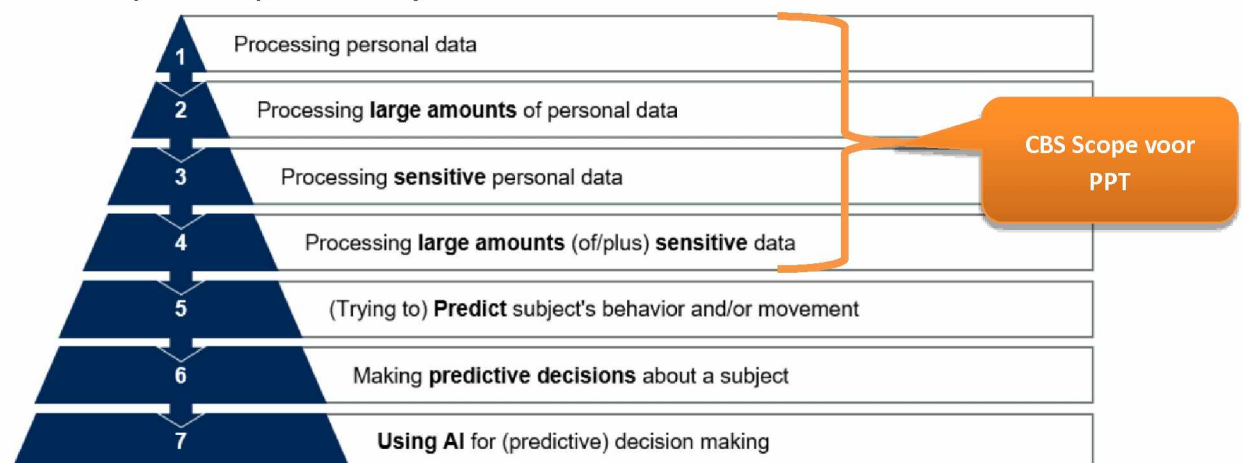
2. PPT in het kort



De scope van PPT is data-tijdens-gebruik, data-tijdens-transport en data-in-rust vallen buiten de scope en zullen dan ook hier niet verder besproken worden.

PPT omhelst een waaier van verschillende oplossingen gericht op het terugdringen van risico's in de verwerkingen. Blockchain, encryptie, data op locatie bij bron maken onderdeel uit van deze waaier en zijn zeer goede ideeën om Privacy by design en Privacy by default zorgvuldig te implementeren.

Gartner: Aspects of Impact on Privacy Risks



Source: Gartner

Het is goed om bij PPT naar twee verschillende aspecten te kijken: het **proces** en de **uitkomst**. Als beide niet (nooit!!) kunnen leiden tot identificatie van personen dan is de AVG niet van toepassing.

Maar ik ken geen voorbeelden van verwerkingen op brondata met persoonsgegevens waarbij vooraf de inrichting zodanig is dat de **uitkomst** nooit kan leiden tot identificerende persoonsgegevens.

Voor 1 cyclus van verwerkingen is het misschien nog mogelijk, maar bij opeenvolgende cycli op dezelfde brondata wordt het steeds moeilijker aan deze eis te voldoen. Het vraagt een analyse op alle uitkomsten uit het verleden. Wat mogelijk helpt is een zeer strikte procesgang waarbij weinig vrijheidsgraden zijn in de verwerkingsopties: standaard concepten en classificaties, vast doelgroepen/populaties. Dit alles om vooraf te kunnen bepalen of de uitkomst anoniem zal zijn. Dit is een essentieel verschil met hoe het CBS nu de output anonimiseert. Tabellen worden nu achteraf geanonimiseerd. Bij PPT moet dit vooraf gebeuren en dat is veel lastiger en misschien maar in een paar geïsoleerde gevallen mogelijk!

Over het proces van PPT hieronder meer.

3. Mogen: Eisen AVG en CBS aan de verwerking

De AVG stelt dat verwerkingen van persoonsgegevens legitiem moeten zijn. Daarnaast stelt de AVG dat de verwerking geen onacceptabele risico's voor de betrokkenen mag opleveren. Dit geheel wordt beoordeeld door verwerkingsverantwoordelijke (het CBS) en vastgelegd in een DPIA (bij verwerkingen met mogelijk hoog risico voor betrokkenen). Indien de risico's onvoldoende afgedekt kunnen worden moet de AP geraadpleegd worden voor de verwerking start. Sleutelwoorden zijn Privacy by design en by default. Kortom:

1. De verwerking legitiem moet zijn;
2. De risico's moeten afdoende afgedekt zijn;
3. Bij een te hoog risico moet de AP geraadpleegd worden.

De legitimiteit van de verwerkingen bij het CBS zit in de CBS-wet. Daarin staat dat het CBS persoonsgegevens mag verwerken voor statistische en wetenschappelijke doeleinden: Grondslag en Doel.

Het CBS kent een groot aantal maatregelen waarmee risico's gemitigeerd worden. Denk hierbij aan het hele IT-beleid (geen eigen software, geen USB, wachtwoordbeleid, etc), verrinnen (pseudonimiseren), beperking recht op bestanden (VARONIS, DSC levert niet zomaar uit, GAP, e.d.), data minimalisatie, beperking op de externe input (minimaliseer uitvraag aan derden), verwijderen van bestanden/data welke niet meer nodig zijn (data retention), logging, awareness medewerkers, etc. Sommige maatregelen zijn van technische aard, andere zijn van organisatorische aard.

In het 'reguliere' statistiekproces leiden deze set van maatregelen tot een aanvaardbaar risico voor de betrokkenen. Bij afwijkende statistische processen zullen er aanvullende vragen gesteld moeten

worden of de standaard maatregelen nog steeds een afdoende reductie van de risico's opleveren. Denk hierbij aan cloudoplossingen. Wat precies regulier is en wat onder afwijkend valt zou nader gepreciseerd kunnen worden.

Het CBS heeft daarmee tot op heden de AP terecht niet geraadpleegd: de risico's zijn afdoende afgedekt.

4. Waarom zou het CBS PPT willen gebruiken?

Eerder is opgemerkt dat het tot op heden nog onmogelijk lijkt te vooraf garanderen dat de uitkomst van een PPT-proces op basis van persoonsgegevens altijd anoniem is. Dit betekent dat de AVG van toepassing zal zijn. Maar waarom dan PPT toepassen?

Het antwoord is dat PPT een mitigerende maatregel kan zijn om risico's voor betrokkenen terug te dringen. Daarmee verruimt PPT de scope van mogelijke verwerkingen aangezien voor alle verwerkingen van persoonsgegevens geldt dat de risico's afdoende afgedekt moeten zijn door de verwerkingsverantwoordelijke. Een verwerkingsverantwoordelijke is dan eerder geneigd een verwerking te willen uitvoeren. Dit geldt niet alleen voor de verwerkingsverantwoordelijke welke geïnteresseerd is in de uitkomst van het proces maar zeker ook voor de verwerkingsverantwoordelijken welke zeggenschap hebben over de brondata.

Daarnaast pleit het natuurlijk voor PPT dat in het algemeen de risico's bij de verwerkingen verlaagd worden. In de zin van de AVG, minimaliseer het risico, zou daarmee PPT toegepast moeten worden.

5. Conclusie PPT en AVG

Als we PPT willen inzetten bij verwerkingen van persoonsgegevens dan blijft nog steeds de drietraps aanpak zoals eerder vermeld geldig. Als het een verwerking van persoonsgegevens in de zin van de AVG betreft dan moet:

1. De verwerking legitiem zijn;
2. Het risico¹ afdoende afgedekt zijn;
3. Bij een te hoog risico de AP geraadpleegd worden.

Het idee is dat PPT de risico's verlaagt. Dat is zeer aanbevelingswaardig: hoe lager het risico des te beter. Maar dit zit in stap 2 en niet in stap 1. De verwerking moet nog steeds legitiem zijn.

De inzet van PPT kan wel bij zeer risicovolle verwerkingen betekenen dat de risico's zodanig verlaagd worden, dat de verwerking uitgevoerd kan en mag worden zonder de stap naar de AP (stap 3). PPT verruimt daarmee de mogelijkheden om persoonsgegevens te verwerken.

¹ Conform de AVG bepaalt de Verwerkingsverantwoordelijke (het CBS) of een risico aanvaardbaar is.

Als de verwerking zodanig ingericht kan worden dat de verwerkingsverantwoordelijke niet meer met persoonsgegevens in de zin van de AVG werkt (proces én uitkomst), dan is de hele AVG niet meer van toepassing. Ik ken nog geen praktische/theoretische toepassing in deze richting. Kortom: PPT helpt maar is (nog) niet de oplossing voor alles.