FG-advies DPIA Gedeelde Zorg

Aan: de proceseigenaar Gegevensonderzoek gedeelde zorg
Van: de functionaris gegevensbescherming (FG Gouda)
Betreft: DPIA Gedeelde Zorg (versie 8 oktober 2020)
Datum: 9 februari 2021

Status

De functionaris gegevensbescherming is de toezichthouder op de naleving van de AVG van Gemeente Gouda. Artikel 35.2 AVG bepaalt dat bij de uitvoering van AVG-risicoanalyses (DPIA's) de FG om advies moet worden gevraagd. Het Privacybeleidskader Gemeente Gouda bevat hierover nadere afspraken. FG-advies op een DPIA vindt doorgaans op een informele manier plaats, zoals een e-mail. In dit geval heb ik gekozen voor formeler advies.

Algemeen

Sterke punten in de DPIA Gedeelde Zorg zijn het zicht op de feitelijke gegevensverwerking en het oog voor risico's, zowel mét als zónder beheersmaatregelen. Tegelijk onderbreekt het nog aan sociaal-maatschappelijk onderzoek: welke schade kan de aanpak bij het uitblijven van beheersmaatregelen *concreet* veroorzaken voor mens en organisatie?

Weliswaar wordt bijvoorbeeld aangegeven dat data zonder beschermingsmaatregelen in verkeerde handen terecht kan komen, maar onder welke omstandigheden zou dat dan zijn (reële praktijkscenario's)? Welke lichamelijke, materiële en/of immateriële schade is dan voorzienbaar? Welke afbreuk- en aansprakelijkheidsrisico's brengt dat met zich mee voor de opdrachtgevers (voor de deelnemende gemeenten: het college)? Wat is vervolgens de AVG-risicoscore op de 'Schaal van erg'?

Pas wanneer de in de DPIA genoemde beheersmaatregelen goed *matchen* met de reële praktijkscenario's, kan er sprake zijn van passende gegevensbescherming de zin van de AVG.

De huidige combinatie van risico's en beschermingsmaatregelen mist nog het doordringen tot de kern van de zaak: het persoonlijk en bestuurlijk leed dat kan ontstaan. Ter vergelijking de schadelijke effecten van onterechte terugvorderingen in de toeslagenaffaire, die voor zowel ouders als bestuurders voorzienbaar waren.

Service level afspraken

Hou in de gaten dat de dienstverleningsovereenkomst met de Stichting Dataplatform Midden-Holland (Stichting DMH) al de verwerkersovereenkomst *is* (vestiging verwerkerschap). De vraag is of er ook de juiste service level-afspraken zijn gemaakt in de zin 28.3 AVG. Daarnaast is onduidelijk of tussen de opdrachtgevers (zie paragraaf 4.2 van de DPIA) passende artikel 26-afspraken zijn gemaakt (afbakening gezamenlijke verantwoordelijkheden).

Maak aan het einde van de DPIA daarom een lijst van alle benodigde organisatorische en technische maatregelen die in de DPIA de revue zijn gepasseerd. Stichting DMH heeft aannemelijk te maken dat in de maatregelen zijn voorzien voordat de gemeente gegevens verstrekt voor onderzoeks-doeleinden. In welke mate heeft de Stichting MDH de maatregelen nu al genomen en wat moet er nog gebeuren? Aan de hand van de lijst van maatregelen kan Stichting MDH dat aangeven.

Enerzijds de DPIA op onderzoek, anderzijds de DPIA op bestuurlijke innovatie

Alle in de DPIA genoemde maatregelen overziend en het voorgaande in aanmerking genomen, wekt de Stichting MDH een betrouwbare indruk. Voor het gegevensonderzoek, volstaat eventueel de huidige DPIA en lijkt de Stichting MDH een afdoende veilige onderzoeksomgeving te bieden.[1]

'Spannender' wordt het wanneer de uitkomsten van het onderzoek worden omgezet in nieuwe werkprocessen, al dan niet geheel of gedeeltelijk geautomatiseerd met behulp van algoritmen. Baken duidelijker af wat onderzoek is en wat vervolg is (wat is het omslagpunt tussen onderzoek en nieuw gebruik?), stel een succesdefinitie op: wanneer is het onderzoek geslaagd? Formuleer een niet mis te verstaan protocol voor gegevensvernietiging van overbodige gegevens na afloop van het onderzoek.

Hou er rekening mee dat er met name een DPIA nodig is op het nieuwe gebruik, dus de innovatie die dankzij het onderzoek mogelijk is geworden. Pas dan blijkt pas echt wat hiervan de effecten zijn, en welke vormen van gegevensbescherming noodzakelijk zijn.

Vereenvoudig voortaan DPIA's

Laat het NOREA-format los. DPIA's dienen rechttoe recht aan te worden uitgevoerd. Uitleg over de AVG en DPIA's kunnen achterwege worden gelaten. Doorloop systematischer de vier stappen van een DPIA (zie artikel 35.7 AVG). Voeg de beheersmaatregelen pas toe in stap 4, als logische oplossing voor de vastgestelde risico's in stap 3. Stap 3 verwoordt de bruto risico's.

Voeg relevante informatie uit andere stukken in de DPIA in, zodat overzicht en inzicht ontstaat. Proceseigenaren en FG's moeten niet hoeven te zoeken naar informatie. De informatie in paragraaf 7.3.3 van het onderzoeksprotocol had de startparagraaf kunnen (moeten!) zijn van stap 2 in de DPIA, om vervolgens te komen tot overzichtelijke benoeming en onderbouwing van de benodigde datasets.

Rechtmatigheidstoetsing is geen onderdeel van een DPIA. Laat rechtmatigheidstoetsing voortaan weg of voeg – voorzover rechtmatigheidstoetsing functioneel is – dit toe als bijlage.

Legitimiteit van de gegevensverwerking

Het doel van het gegevensonderzoek door de Stichting DMH is om indicatoren van 'escalatie van zorggebruik te ontwikkelen'. De ambitie is om zulke escalaties te voorkomen door slimmere benutting van data (zie DPIA, p. 14). Paragraaf 7.3.3. van het onderzoeksprotocol benoemt de maatschappelijke relevantie van dergelijk onderzoek.

Als zodanig is het gegevensonderzoek welbepaald en specifiek. Karakteristiek aan dit soort onderzoek is dat met behulp van statistische methodieken naar patronen/correlaties in de data wordt gezocht (fase I), om te ontdekken of uit de data nuttige informatie kan worden gedestilleerd. Er is zowel noodzaak om dergelijk onderzoek te verrichten (wat kunnen we leren uit de data?) als

[1] Let wel: dit is een inschatting op afstand. Het is de proceseigenaar die namens het college besluit over de acceptatie van risico's.

noodzaak om vervolgens 'datagedreven' te werken (fase II), mócht de proeffase nuttige indicatoren opleveren.

De EU-wetgever bedoelde de AVG om dit soort innovaties te stimuleren in plaats van te blokkeren. Belangrijk is de notie in overweging 4: 'Gegevensverwerking moet ten dienste van de mens staan. Het recht op bescherming van persoonsgegevens heeft geen absolute gelding, maar moet worden beschouwd in relatie tot de functie ervan in de samenleving en moet conform het evenredigheidsbeginsel tegen andere grondrechten worden afgewogen'. Denk bij die andere grondrechten aan het recht op preventieve gezondheidszorg en medische verzorging (artikel 35 EU Handvest grondrechten).

De bevoegdheid van Gemeente Gouda om gegevens uit het sociaal domein te gebruiken voor statistisch onderzoek, vloeit voort uit diverse nationale wetten in hun onderlinge samenhang, hier met name de Gemeentewet, de Wet maatschappelijke ondersteuning en eventueel de Wet publieke gezondheid.

Artikel 6.4 AVG staat verdere verwerking van gegevens nadrukkelijk toe, mits rekening wordt gehouden met een aantal afwegingsfactoren, waaronder de verenigbaarheidstoets.

Het hier beoogde onderzoek *is* verenigbaar, aangezien het gaat om verdere verwerking voor statistisch onderzoek en in het algemeen belang.

Dat de bij Stichting DMH aan te leveren data ook bestaat uit gegevens in de bijzondere gegevenscategorieën van artikel 9 AVG, is niet het probleem omdat zowel voor gewone persoonsgegevens als voor bijzondere persoonsgegevens geldt dat verdere verwerking voor statistisch onderzoek en in het algemeen belang is toegestaan.

Toestemming is bij dergelijk onderzoek niet aan de orde en kan zelfs een inbreuk inhouden op de AVG. Mogelijk geldt dit strak ook voor nieuw gebruik van gegevens, na afloop van het onderzoek.

Afdoende garanties

De in dit FG-advies gedane aanbevelingen hebben tot strekking om duidelijker beeld te scheppen van de gevolgen voor de betrokkenen en het bestaan van passende waarborgen – dit zijn de resterende afwegingsfactoren van artikel 6.4 AVG.

Verbetering van de DPIA geeft hiervan scherper beeld. Tegelijkertijd laat de voorgestelde aanpak ook nu al zien dat het onderzoek door de Stichting DMH geen noemenswaardige risico's voor betrokkenen met zich meebrengt – dit dankzij de beloofde beschermingsmaatregelen, waaronder pseudonimisering.

Vooralsnog lijkt de Stichting DMH daarmee 'privacy by design' te garanderen, dus een onderzoeksaanpak die spoort met artikel 25 AVG. Indien die zekerheid geboden wordt, in combinatie met de ketenregie van artikel 24-28 AVG, heeft het onderzoek het groene licht van de Algemene verordening gegevensbescherming.

Hier ligt mijn belangrijkste vraag: biedt de Stichting DMH daadwerkelijk afdoende garanties? Waar blijkt dat uit?

BIJLAGE – checklist goede DPIA

Kernelementen I	Kernelementen II	Verwerkt	Vindplaats (paragraaf)	Opmerkingen
1. Systematische beschrijving van de gegevensverwerking (35.7a AVG)	a) Feitelijke beschrijving werkproces(sen) — eventueel geclusterd.	+/–	4.5-7	Op zich beeld van onderzoeksaanpak (fase I) maar nog geen doorkijk naar eventueel vervolg (fase II)
	b) Feitelijke beschrijving informatiedeling en gegevensverwerking (informatiestromen), inclusief duiding bijzondere gegevenscategorieën	+	4.3	Duidelijke weergave datasets
	c) Feitelijke beschrijving van het ICT-landschap (zowel high tech als low tech) incl. vormen van uitbesteding en geografische locaties van servers	+	4.5-8	Voldoende beschreven inclusief geografische locatie MS-servers (west-europa)
2. Analyse noodzaak en evenredigheid (35.7b AVG)	a) Analyse organisatiebelang en persoonlijk belang	–	2, 4.4.1 (voorw. 2)	Zet in de DPIA steviger in de verf wat de maatschappelijke meerwaarde is van het onderzoek (nut en noodzaak).
	b) Analyse functionele informatiebehoefte(n) (artikel 5.1c-d AVG)	+/–	4.3, 4.4.1 (voorw. 3-4)	Onderbouwing datasets ontbreekt in de DPIA of onvolledig
3. Objectieve risicobeoordeling (35.7c AVG)	a) Toewerken van bruto- naar nettorisico (‘wat is passend?’)	+/–	6	Bruto-/nettorisico zijn opgenomen maar lopen door elkaar
	b) Objectieve beoordeling op basis van realistische schadeveroorzakende praktijkscenario’s (overweging 76 AVG)	+/–	6	Voeg de praktijkscenario’s toe (ontbreken nu nog). Zie echter ook 6.3-8.
	c) Relatering aan kansvergrotende aspecten (overweging 75 AVG)	–	?	Niet uitgewerkt
	d) Analyse aard en	–	?	Niet uitgewerkt

	omvang voorziene schade (overweging 75 AVG)			
	e) Risicoclassificatie (overweging 76 AVG)	+/–	6	Objectieve beoordeling is nog een verbeterpunt
4. SMART-geformuleerd pakket van passende organisatorische en technische maatregelen (35.7c AVG en 35.11)	a) Organisatorische maatregelen (artikel 24-25 AVG)	+/–	4-7	Passendheid van maatregelen moet blijken uit reële risico's (praktijkscenario's). Zijn er passende verwerkersafspraken? Hoe zit het met artikel 26-afspraken?
	b) Technische maatregelen (artikel 24-25 AVG)	+/–	4-7	Passendheid van technische maatregelen moet blijken uit reële risico's (praktijkscenario's)
5. Incalculatie eigen beleidsafspraken (39.1b AVG)		?	?	Leg de relatie met privacybeleidskader Gemeente Gouda.
6. Incalculatie beschermingsregimes gerelateerde wetgeving (39.1b AVG)		+	4.4.1	Verwijzing naar 7:458 BW en 24 UAVG
7. Incalculatie artikel 40-gedragscodes (35.8 AVG)		n.v.t.	n.v.t.	n.v.t.
8. Incalculatie centrale DPIA's 6.1c/6.1e AVG (35.10 AVG)		n.v.t.	n.v.t.	n.v.t.
9. Betrekken doelgroep (35.9 AVG)		–	?	Betrek een of meerdere bestaande adviespanels in het sociaal domein, of doe dit bij DPIA vervolgaanpak (fase II)
10. FG-advies gevraagd (35.2 AVG)		+/–	Mail 29 januari 2021	Betrek de FG naar behoren en tijdig

Privacy
Management
Partners
Coöperatie UA
adres
Vondellaan 58
3521 GH Utrecht
telefoon
+31 85 401 38 66
e-mail
info@pmpartners.nl
website
www.pmpartners.nl