Algemeen

De Drechtsteden nemen deel aan een pilot rondom het gebruik van IRMA, genaamd “IRMA bellen”. Andere partners in deze pilot zijn de gemeenten Arnhem en Nijmegen.

Meer informatie over het initiatief van IRMA en de werking ervan in zijn algemeenheid is onder andere terug te vinden via: <https://privacybydesign.foundation/irma-uitleg/>

Het verzoek is om voor de pilot een DPIA uit te voeren. Afspraak is om te starten met een voorstel hoe het traject om te komen tot een DPIA eruit kan zien. Het is om een aantal redenen belangrijk om voor “IRMA bellen” eerst over het traject na te denken. Om te beginnen heeft dit project een grotere reikwijdte dan alleen de Drechtsteden regio. De ontwikkeling van IRMA als identificatiemiddel heeft een landelijk belang. Er wordt met andere gemeenten samengewerkt, het Ministerie van BZK is betrokken en er zijn derde partijen betrokken. Deze complexe context betekent dat het niet voldoende is om ‘slechts’ de gebruikelijke processtappen binnen de Drechtsteden te doorlopen. Een ander belangrijk kenmerk van het project “IRMA bellen” is het experimentele karakter ervan. Aangezien het gaat om een pilot die met meerdere partners wordt uitgevoerd, zullen gedurende de pilot nieuwe inzichten worden verzameld, nieuwe risico’s worden benoemd en nieuwe oplossingen worden uitgeprobeerd.

Voorstel

Een DPIA is een levend document, een risico analyse een doorgaand proces. Dat is des temeer het geval bij een pilot, een project waarbij - met persoonsgegevens - wordt geëxperimenteerd. Het hier om de ontwikkeling van een privacyvriendelijk identificatiemiddel voor burgers. Daarmee kun je vaststellen dat borging en toetsing van de privacy van de burger tijdens het experiment zelf ook onderwerp is van het project. Met andere woorden, deels wordt de risicoanalyse die tijdens de DPIA gedaan behoort te worden, deel uit van de uitvoering.

Daarom wordt voorgesteld om het traject in twee delen uiteen te splitsen:

* een *voortraject*, dat inzicht moet geven in de randvoorwaarden van de pilot voor wat betreft compliance aan de AVG; een werkgroep van privacy professionals, informatie beveiligingsadviseurs, uitvoerenden van de pilot en betrokkenen dient hieraan te werken; hiervoor is nodig een dit deel wordt separaat bij de FG ter advisering voorgelegd, en na de advisering door de FG en eventueel uitvoering van extra maatregelen wordt de pilot opgestart; dit deel heeft een deadline die ligt voor de start van de pilot;
* een *project traject,* waarbij tijdens de looptijd van de pilot door een werkgroep (eventueel dezelfde, maar niet noodzakelijk) van privacy professionals, informatie beveiligingsadviseurs, uitvoerenden van de pilot en betrokkenen de borging van de privacy wordt getoetst aan eventuele nieuwe bevindingen die tijdens de pilot worden opgedaan en waarbij in overleg met projectleiding en/of FG direct bijgestuurd kan worden in het project; dit traject levert feitelijk een voortdurende aanvulling en wijziging van de DPIA tekst op. Na afloop van pilot kan een evaluatie worden toegevoegd en het geheel opnieuw aan de FG worden voorgelegd. Het voordeel van deze aanpak is wanneer na de pilot “IRMA bellen” een blijvertje zou blijken te zijn, er al een degelijke aanzet is voor een DPIA op het structurele proces en eventuele verbreding van gebruik van IRMA als identificatiemiddel.

Concrete stappen

Voortraject DPIA:

* inrichting van een werkgroep, waarbij in elk geval twee personen van de inhoudelijke projectgroep, twee privacy en twee informatiebeveiligingsadviseurs lid zijn;
* mogelijk is het verstandig om hier van de andere twee gemeenten een lid extra aan te wijzen, of eventueel extra leden in verband met de partners;
* deze DPIA werkgroepleden hebben nodig van de projectgroep “IRMA bellen”: een duidelijk overzicht van alle betrokken partners en hun rol; een concept projectplan (hoe wordt de pilot georganiseerd? denk ook aan: wie doen er mee met het experiment, hoe is de voorlichting geregeld naar deze betrokkenen toe e.d.) met procesbeschrijving in stappen van het daadwerkelijke IRMA bellen proces (denk aan een uitwerking van het document “testen telefonie oplossing.docx” en “DigID proef”);
* het is verstandig voor deze werkgroep een structuur te bepalen (voorzitter, rol privacy etc);
* de werkgroep verband buigt zich over vragen die samenhangen met de juridische en maatschappelijke basis en risico’s (stap 1), waarbij zaken aan de orde zullen komen zoals o.a. grondslag, doel en doelbinding, noodzaak en evenredigheid, analoge alternatieven, dataminimalisatie, betrokkenen en hun rol, hoe betrokkenen te betrekken bij de PIA, betrokken partijen en hun verschillende rollen en eventueel al dan niet verplicht te sluiten overeenkomsten; in deze stap kan mogelijk met minder IB-ers gewerkt worden;
* de werkgroep vormt zich aan de hand van een globale procesbeschrijving een beeld van de informatieketen, data in rest and transit, data flow life cycle en informatiebeveiligingsrisico’s (stap 2); in deze stap zijn de IB-ers aan zet en kan eventueel met één privacyfunctionaris worden volstaan;
* de werkgroep stemt na afloop van dit traject af met de FG en vervolgens levert de DPIA werkgroep de projectleiding een DPIA concept dat deze ter advisering aan de FG moet voorleggen.
* Na positief advies en eventueel implementatie van extra maatregelen kan de pilot van start gaan.

Het inrichten van het “project traject” zou wellicht het beste kunnen worden gedaan door hierover van gedachten te wisselen tijdens het “voortraject” en deze inrichting als onderdeel van de DPIA aan de FG aan te bieden.