Leergeschiedenis AVG en bijbehorende DPIA-SWO-Privacy protocol

Nadieh Pennings- projectleider proeftuin Gelderland Zuid locatie Nijmegen-Dukenburg

In het kader van de uitvoering van het landelijk Toekomstscenario in Gelderland Zuid locatie Nijmegen-Dukenburg, heb ik als projectleider als eis van de gemeente Nijmegen een Samenwerkingsovereenkomst, privacyprotocol en DPIA moeten opstellen. Dit in het kader van de Algemene Verordening Gegevensbescherming (AVG). De AVG legt een sterke nadruk op de bescherming van persoonlijke gegevens en geeft individuen meer controle over hun gegevens. De overheid, gemeenten en dus ook uitvoeringsorganisaties moeten transparant zijn over hun gegevensverwerkingspraktijken en strenge maatregelen nemen om de privacy en veiligheid van persoonsgegevens te waarborgen. Hieronder zal ik per deel uiteenzetten wat ik heb geleerd van het opstellen van deze documenten.

DPIA

Een Data Protection Impact Assessment (DPIA), of gegevensbeschermingseffectbeoordeling, is een belangrijk instrument onder de AVG om de privacyrisico's van gegevensverwerkingsactiviteiten te identificeren en te mitigeren. Het uitvoeren van een DPIA binnen een project als de proeftuin die een netwerksamenwerking beoogt, is erg lastig gebleken. Mijn advies is dan ook, om dit gelijk in duoschap met een senior jurist/ juridisch adviseur te doen, en gelijk de Functionaris Gegevensbescherming van de opdrachtgever (gemeente) te betrekken. Dit om verschillende redenen:

1. Complexiteit van de verwerking

Gegevensstromen: Het in kaart brengen van alle gegevensstromen is ingewikkeld.

Technische details: Het begrijpen en documenteren van de technische aspecten van gegevensverwerking, zoals hoe gegevens worden verzameld, opgeslagen, verwerkt en gedeeld, vereist vaak specialistische kennis.

2. Juridische en regelgevende kennis

Interpretatie van de wet: Het correct interpreteren van de eisen van de AVG en deze toepassen op specifieke gegevensverwerkingsactiviteiten kan lastig zijn, vooral omdat de wet complexe juridische taal en concepten bevat.

Regelgevende updates: De wet- en regelgeving rondom gegevensbescherming evolueren voortdurend, wat het moeilijk maakt om altijd up-to-date te blijven en te voldoen aan de laatste vereisten.

3. Identificatie van risico’s

Risicobeoordeling: Het identificeren en evalueren van potentiële privacyrisico's vereist een grondige analyse van hoe gegevens kunnen worden misbruikt of gelekt, en welke gevolgen dit kan hebben voor de betrokkenen.

Risicomanagement: Het ontwikkelen van passende maatregelen om geïdentificeerde risico's te mitigeren vereist een goed begrip van zowel technische als organisatorische beveiligingsmaatregelen.

4. Interne coördinatie

Multidisciplinaire inzet: Een DPIA vereist vaak de betrokkenheid van verschillende afdelingen binnen een organisatie, waaronder IT, juridische zaken, compliance, en operationele afdelingen. Dit vraagt om goede coördinatie en communicatie.

Veranderingsbeheer: Het implementeren van de aanbevelingen uit een DPIA kan aanzienlijke veranderingen vereisen in bestaande processen en systemen, wat kan leiden tot weerstand of vertragingen binnen de organisatie.

5. Documentatie en transparantie

Grondige documentatie: Een DPIA moet gedetailleerd en nauwkeurig gedocumenteerd worden. Dit omvat het beschrijven van de gegevensverwerkingsactiviteiten, de betrokken systemen, de risico's, en de genomen maatregelen.

Transparantie: Organisaties moeten transparant zijn over hun gegevensverwerkingspraktijken, zowel intern als extern, wat kan leiden tot aanvullende documentatie- en rapportageverplichtingen.

Tips

Het uitvoeren van een DPIA is een grondig en veeleisend proces dat nauwkeurigheid, samenwerking en een diepgaand begrip van zowel technische als juridische aspecten vereist. Hoewel het een uitdaging kan zijn, is het een essentieel onderdeel van de naleving van de AVG. Een DPIA kan sneller worden voltooid door de volgende dingen van te voren te regelen:

Templates en recycling: Maak gebruik van bestaande DPIA-templates en tools die zijn goedgekeurd door FG's. Gebruik delen van eerder uitgevoerde DPIA's voor vergelijkbare projecten als basis voor de nieuwe beoordeling.

Multidisciplinair team: Stel een team samen met vertegenwoordigers uit verschillende afdelingen (IT, juridische zaken, compliance, enz.) om expertise en input te centraliseren en stel één verantwoordelijke persoon aan om het DPIA-proces te coördineren en voortgang te bewaken. Zorg ervoor dat betrokken teamleden goed zijn opgeleid in het uitvoeren van DPIA's en de vereisten van de privacywetgeving.

Geautomatiseerde tools: zoek uit of er softwaretools zijn die specifiek zijn ontworpen voor DPIA's. Deze tools kunnen helpen bij het identificeren van risico's, het bieden van standaard antwoorden en het genereren van rapporten.

Vooraf gedefinieerde maatregelen: Definieer vooraf standaardmitigatiemaatregelen voor veelvoorkomende risico's.

Review, feedback en deadine: Laat de DPIA in fasen beoordelen door het team en vraag om feedback. Dit kan helpen om problemen vroegtijdig te identificeren en op te lossen, waardoor latere herzieningen worden geminimaliseerd. Communiceer vooraf duidelijk deze fases en werk naar een deadline. Dit voor jezelf, maar ook om de feedback te clusteren en eindeloze feedback te voorkomen en de FG niet op je dak te krijgen omdat het te lang duurt..

Samenwerkingsovereenkomst (SWO) en privacy protocol

Een samenwerkingsovereenkomst is een juridisch document waarin de afspraken en voorwaarden worden vastgelegd tussen meerdere partijen die besluiten samen te werken aan een gemeenschappelijk project of doel. Dit type overeenkomst is bedoeld om de verantwoordelijkheden, rechten en plichten van de betrokken partijen duidelijk te definiëren en om eventuele misverstanden of geschillen te voorkomen.

Belangrijke onderdelen van een samenwerkingsovereenkomst zijn onder andere:

- Partijen: De namen en gegevens van de partijen die de overeenkomst aangaan.
- Doel en reikwijdte: Een omschrijving van het doel van de samenwerking en de reikwijdte van de gezamenlijke activiteiten.

- Duur: De looptijd van de overeenkomst en de voorwaarden voor verlenging of beëindiging.
- Verantwoordelijkheden: Een gedetailleerde beschrijving van de taken en verantwoordelijkheden van elke partij.
- Financiële afspraken: Informatie over de verdeling van kosten, winsten en eventuele financiële bijdragen van elke partij.
- Intellectueel eigendom: Afspraken over het eigendom en het gebruik van intellectuele eigendommen die tijdens de samenwerking worden gecreëerd.
- Vertrouwelijkheid: Bepalingen over de behandeling van vertrouwelijke informatie.
- Geschillenbeslechting: Procedures voor het oplossen van eventuele geschillen die tijdens de samenwerking kunnen ontstaan.
- Beëindiging: Voorwaarden waaronder de overeenkomst kan worden beëindigd door een of beide partijen.

Het opstellen van een SWO is niet lastig gebleken. Als bovenstaande elementen er in terug komen, alswel belangrijke elementen als monitoring, en het gebruik van systemen, is het al snel een goed SWO. Het opstellen van een samenwerkingsovereenkomst helpt om duidelijke verwachtingen te scheppen en biedt een juridisch kader waarbinnen de partijen kunnen opereren. Het is vaak aan te raden om juridisch advies in te winnen bij het opstellen van een dergelijke overeenkomst om ervoor te zorgen dat alle relevante aspecten worden gedekt en dat de belangen van alle betrokken partijen worden beschermd. In dit geval raad ik aan om dit met alle juristen van de betrokken partijen te doen. Dit betekent in de praktijk dat de opdrachtgever (gemeente) een format opstelt, waar de juristen van de uitvoeringspartijen feedback op mogen geven. Ik heb de SWO laten tekenen in de stuurgroep.

Het privacyprotocol is een bijlage van de SWO. Een privacyprotocol is een document of reeks richtlijnen die beschrijft hoe de betrokken organisaties omgaan met persoonlijke gegevens van de cliënten. Het is ontworpen om de privacy en bescherming van persoonlijke informatie te waarborgen, in overeenstemming met wettelijke vereisten. Deze was ook niet lastig om op te stellen. Je zou kunnen zeggen dat het een uitvoeringsverklaring is van de DPIA. Belangrijke elementen van een privacyprotocol zijn onder andere:

- Inzameling van gegevens: Gedetailleerde informatie over welke persoonlijke gegevens worden verzameld, hoe ze worden verzameld, en de bron van deze gegevens.
- Gebruik van gegevens: Uitleg over hoe de verzamelde gegevens zullen worden gebruikt, inclusief de doeleinden waarvoor de gegevens worden verwerkt.
- Delen van gegevens: Informatie over met wie de gegevens kunnen worden gedeeld, zoals derde partijen, en onder welke omstandigheden.
- Bescherming van gegevens: De maatregelen die worden genomen om de gegevens te beschermen tegen ongeoorloofde toegang, verlies of diefstal.
- Bewaartermijnen: Hoe lang de persoonlijke gegevens worden bewaard en de criteria die worden gebruikt om deze perioden te bepalen.
- Rechten van individuen: Uitleg over de rechten die individuen hebben met betrekking tot hun persoonlijke gegevens, zoals het recht op inzage, correctie, verwijdering en bezwaar tegen verwerking.
- Toestemming en transparantie: Hoe toestemming wordt verkregen van individuen voor de verwerking van hun gegevens en hoe transparantie wordt gewaarborgd.
- Beveiligingsmaatregelen: De technische en organisatorische maatregelen die zijn geïmplementeerd om de veiligheid van persoonlijke gegevens te waarborgen.
- Contactinformatie: Gegevens over hoe individuen contact kunnen opnemen met de organisatie voor vragen of klachten over het privacybeleid.