Autoriteit
Consument & Markt

ACM & PRIVACY
Openbaar

DPIA – STAPPENPLAN – UITVOERING

Waarom dit document?

Wanneer de verwerking waarschijnlijk hoge risico's voor de rechten en vrijheden van natuurlijke personen met zich meebrengt, dan is het vanuit de AVG verplicht om een Data Protection Impact Assessment (DPIA) uit te voeren. Nadat adhv het stappenplan 'checklist DPIA – Verplicht?' is gebleken dat het verplicht is om een DPIA uit te voeren, dan informeer je de FG + Privacy Officer van jouw directie en doorloop je de onderstaande stappen (1 t/m 14). Jij, als opdrachtgever, blijft verantwoordelijk voor de uitvoering van de DPIA. De Privacy Officer van je directie moet bij de uitvoering betrokken worden, maar je kunt en mag de uitvoering van de DPIA niet zomaar aan de Privacy Officer uitbesteden.

1. Stel een team samen met:
   - kennis van de inhoud van de verwerking/het proces;
   - kennis van de techniek;
   - kennis van de organisatie;
   - kennis van de AVG.

Denk aan:
- *de opdrachtgever/verantwoordelijke voor de verwerking*
- *data-eigenaar (projectleider/proces-verantwoordelijke: verantwoordelijk voor uitvoeren DPIA)*
- *Privacy Officer*
- *de OR of andere vertegenwoordiging van de betrokkenen*
- *informatiebeveiliging*

2. Voer de DPIA uit: Gebruik hiervoor het format van de RijksDPIA. Raadpleeg ook de toelichting bij dit format. Sla de ingevulde versie en alle relevante informatie op in DOX.

3. Stem de inhoud van de DPIA af met: informatiebeveiliging, de opdrachtgever en de data-eigenaar

4. Leg de DPIA voor aan CPO. Stuur relevante informatie mee (zoals protocol, werkproces of concept-verwerkersovereenkomst).

5. Leg de DPIA ter advisering voor aan FG. Stuur relevante informatie mee (zoals protocol, werkproces of concept-verwerkersovereenkomst).

6. Bespreek het FG-advies met het team. Neem het advies van de FG op in je DPIA, geef aan wat je ermee gedaan hebt.

7. Bespreek de DPIA met de opdrachtgever en data-eigenaar. De opdrachtgever geeft akkoord voor de maatregelen die de risico's gaan afdekken. Door dit akkoord neemt hij ook de verantwoordelijkheid voor het uitvoeren van de vermelde maatregelen

8. Stuur de eindversie van de DPIA naar de FG. Geef in de bijbehorende e-mail gemotiveerd aan welke elementen van het FG-advies niet zijn meegenomen. Op deze manier kan de FG kijken wat met het advies is gedaan en welke maatregelen voorgesteld zijn aan en besloten zijn door de opdrachtgever.

9. Stel een implementatieplan op. Beschrijf in dit plan (a) hoe de voorgestelde maatregelen zullen worden geïmplementeerd, (b) door wie en (c) volgens welk tijdschema. In het implementatieplan wordt ook uitgewerkt (en waar nodig gemotiveerd) of de uitgebrachte adviezen wel/niet worden overgenomen (comply or explain)

10. Stel een evaluatietermijn vast van: de (nog te nemen) maatregelen en de DPIA zelf.

11. Controleer of alle documenten in DOX opgenomen zijn: De DPIA, het advies van de FG, het akkoord van de opdrachtgever en het implementatieplan moeten in DOX opgenomen zijn.

12. Neem de DPIA op in: het DPIA-register.

13. Neem de verwerking op in: het verwerkingsregister. Een verwijzing naar het advies van de FG en het akkoord van de opdrachtgever moeten ook in dit register opgenomen worden.

14. Check of de maatregelen zijn genomen.

15. Evalueer de DPIA na 3 jaar, of eerder als hiertoe aanleiding is.

Afsluiting

Het is van belang dat de ACM zich te allen tijden kan verantwoorden naar de relevante partijen (denk aan de Autoriteit Persoonsgegevens en de betrokkenen). Om die verantwoording te kunnen realiseren dient dit document ingevuld op te worden geslagen in het bijbehorende DOX-dossier. Maak een submap ‘Privacy’ aan of label dit document met het tabje ‘Intern - Privacy’ in het DOX-dossier. Zo leg je vast dat er een DPIA is uitgevoerd. Informeer de Privacy Officer van jouw directie na het uitvoeren van de DPIA door een e-mail te sturen met de betreffende link naar de ingevulde versie in DOX.

Toelichting

ntb