Duthler Associates
law, ICT & organisation

Factsheet

Uitvoeren van een Data Protection Impact Assessment (DPIA)

Gegevensbescherming is een ‘boardroom issue’

De Europese Algemene verordening gegevensbescherming (AVG) heeft gevolgen voor de verwerking van persoonsgegevens door organisaties. Er mag niet gestart worden met het verwerken van persoonsgegevens alvorens een onderzoek naar de risico’s voor de betrokkenen heeft plaatsgevonden. Uit dit onderzoek kan blijken dat een Data Protection Impact Assessment (DPIA) verplicht is of anders verstandig is om deze uit te voeren.

De kwaliteit van de DPIA is bepalend voor de latere beheersing van de risico’s die gepaard gaan met de verwerking. De verwerkingsverantwoordelijke is verantwoordelijk voor de uitvoering van de DPIA en loopt risico’s als later blijkt dat niet of niet effectieve beheersmaatregelen zijn getroffen. Dit kan leiden tot datalekken met boetes van de Autoriteit Persoonsgegevens (AP) of claims van betrokkene als gevolg.

Wat is een DPIA?

Met een DPIA kan een organisatie vooraf de risico’s van een verwerking van persoonsgegevens in kaart brengen om daarna maatregelen te kunnen nemen om de risico’s te verkleinen. Een belangrijk kenmerk van een DPIA is dat de risico’s vanuit het belang van de betrokkene worden benoemd. De DPIA moet uitgevoerd zijn alvorens gestart wordt met de verwerking.

Wanneer is een DPIA verplicht?

Onder de AVG, de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg) kunnen organisaties verplicht zijn een DPIA uit te voeren. Voor de AVG geldt voor een aantal categorieën verwerkingen dat een DPIA verplicht is. De AP heeft een lijst van soorten verwerkingen opgesteld waarvoor het uitvoeren van een DPIA ook verplicht is. Ook op Europees niveau is een lijst opgesteld van verwerkingen waarvoor een DPIA verplicht is. In de niet verplicht gestelde situaties moet de organisatie zelf beoordelen of de verwerking een hoog privacyrisico oplevert voor de betrokkene. Als dit risico als hoog is vastgesteld, moet ook voor deze verwerking een DPIA worden uitgevoerd.

Een DPIA uitvoeren

De uitvoering van de DPIA is vormvrij mits deze voldoet aan de basisvereisten zoals die in de AVG staan beschreven. De DPIA moet een systematische beschrijving van de voorgenomen gegevensverwerking geven, een beoordeling van de privacyrisico’s en de maatregelen om de risico’s aan te pakken. Uiteraard moet vastgesteld worden dat de verwerking rechtmatig zal zijn.

De DPIA wordt uitgevoerd door een team van (externe) medewerkers onder leiding van een ervaren deskundige op het aandachtsgebied van het beschermen van persoonsgegevens. Een team dat samengesteld is uit diverse geledingen uit de organisatie biedt de meeste toegevoegde waarde. Een

neveneffect is dat bij deze teamleden de awareness voor het beschermen van persoonsgegevens toeneemt. Als de organisatie een FG heeft, moet de FG om advies worden gevraagd.

Het resultaat van de DPIA wordt vastgelegd en dient als verantwoording van inzichten en keuzes. Ook bij eventuele datalekken kan de DPIA getoond worden als risicoanalyse als de organisatie zich moet verantwoorden bij een toezichthouder of rechtbank.

De DPIA wordt periodiek herhaald, minimaal een keer per drie jaar. Het kan gewenst zijn om de DPIA eerder te actualiseren, bijvoorbeeld als voor de verwerking een nieuwe technologie wordt gebruikt of het doel van de verwerking wijzigt.

De uitkomsten van de DPIA opnemen in de processen

De DPIA mag geen papieren tijger worden. De DPIA is pas afgerond als de maatregelen die in de DPIA zijn voorgesteld om de risico's af te dekken, daadwerkelijk effectief blijken te werken. Deze verantwoording past in het waarborgen en aantonen dat de AVG wordt nageleefd.

Aanpak van de DPIA

De DPIA start met het samenstellen van het team en het aanwijzen van de teamleider. De professionals van Duthler Associates kunnen als teamlid of als teamleider participeren. Als teamlid wordt met de deskundigheid van gegevensbescherming een taak uit de DPIA opgepakt. Als het gaat om de rol van teamleider dan coördineert deze medewerker de gehele DPIA. De teamleider verzorgt dan ook de documentatie en de eindrapportage.

Meer informatie en contact

Wij ondersteunen en voeren al meer dan 20 jaar DPIA's bij veel verschillende opdrachtgevers uit. Wij hebben ervaring in verschillende sectoren en beschikken over kennis en kunde. Wij werken efficiënt en effectief om de opdrachtgever zo goed mogelijk te bedienen.

Ingeval van vragen of u wilt een vrijblijvende offerte ontvangen, aarzelt u niet contact met ons op te nemen. Dit kan via +31 (0)70 – 392 22 09 of info@duthler.nl.

Pagina: https://duthler.nl/diensten/beschermen-van-bedrijfsgeheimen-en-persoonsgegevens/data-protection-impact-assessment/

Duthler Associates
law, ICT & organisation

Afspraak maken en contact

Wilt u meer weten? Neem dan contact op met ons op via de onderstaande gegevens.

Kantoor:

Frankenslag 137

2582 HH Den Haag

+31 (0) 70 392 22 09

info@duthler.nl

https://www.duthler.nl