DATA PROTECTION IMPACT ASSESSMENT

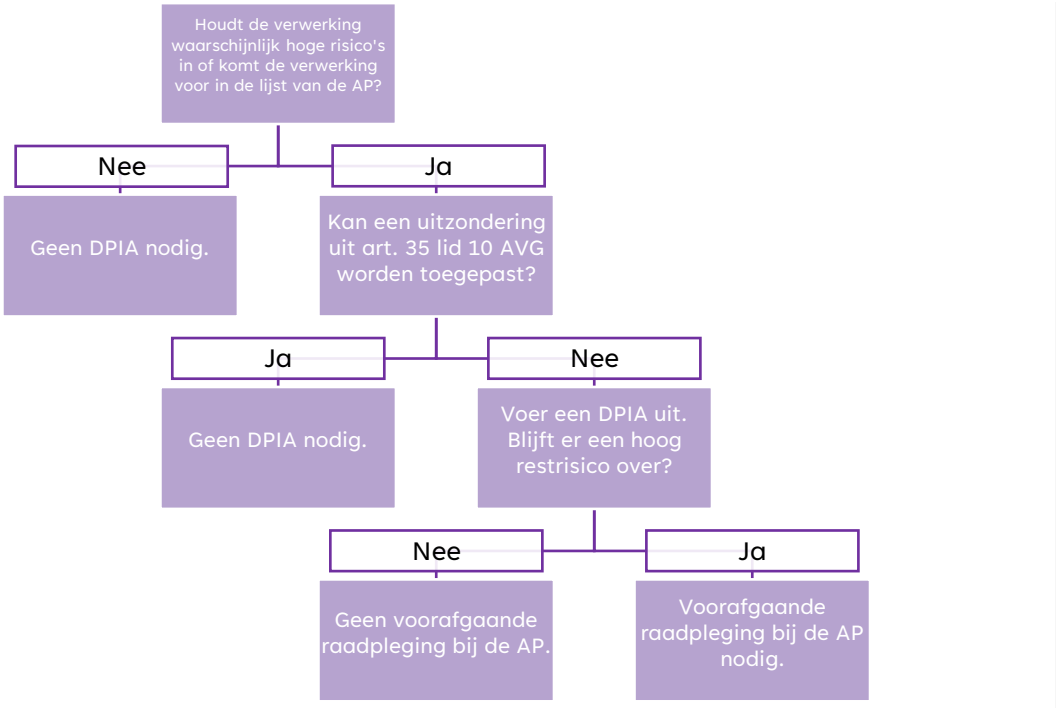
Factsheet

Een Data Protection Impact Assessment, zodat u de AVG niet schendt.

Inleiding

De AVG bevat verschillende nieuwe verplichtingen voor organisaties. Een van die verplichtingen, een DPIA, (Gegevensbeschermingseffectbeoordeling -GEB- of Privacy Impact Assessment –PIA- of Data Protection Impact Assessment -DPIA-) heeft tot doel om enkel op zo'n manier gegevens te verwerken dat deze verwerking geen hoog risico voor de betrokkenen met zich meebrengt. Door het uitvoeren van een DPIA krijgen organisaties beter inzicht in de privacy risico's die verwerkingen met zich meebrengen en de mitigerende maatregelen die genomen moeten worden om deze risico's te beperken.
In deze factsheet gaan wij in op de vraag wat het doel is van een DPIA, hoe je een DPIA uitvoert, wat de risico's zijn van het niet uitvoeren van een DPIA en welke raakvlakken er zijn met andere AVG verplichtingen.

Stappenplan



Doel van een DPIA

Volgens de officiële 'Guidelines on Data Protection Impact Assessment' van het Europees Comité voor Gegevensbescherming (ECGB of in het Engels EDPB) kan het doel van de DPIA in één zin worden samengevat: "*Een gegevensbeschermingseffectbeoordeling is een proces voor het verwezenlijken en aantonen van naleving*" van de AVG.[i] De DPIA is een proces dat bedoeld is om de verwerking van persoonsgegevens dusdanig te beschrijven, inclusief doel en verantwoording, dat er op basis van een risico-inschatting voor de rechten en vrijheden van betrokkenen een afgewogen en onderbouwde beslissing gemaakt wordt of een verwerking al dan niet uitgevoerd kan worden, of dat er maatregelen genomen dienen te worden die bepaalde risico's wegnemen of verlagen.
Art. 35 lid 1 AVG vult dit aan met het volgende: "*Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.*" [ii]
Uit het bovenstaande volgt dat het doel van de DPIA is om vooraf de privacy risico's van een gegevensverwerking helder te krijgen en preventieve maatregelen te kunnen nemen.

Verschillende DPIA-modellen

Bij het uitvoeren van een DPIA kunnen verschillende methoden en modellen worden gebruikt als hulpmiddel om aan de eisen uit de AVG te voldoen. Er kan niet één standaard worden gegeven. Verschillende instanties hebben uitgebreide modellen ontwikkeld voor het uitvoeren van een DPIA. Enkele bekende modellen zijn:

- NOREA;
- ISO29134;
- Rijksmodel GEB;
- ICO;
- CNIL.

Wij zullen de bovengenoemde modellen kort toelichten.

- **NOREA**[iii]

De Nederlandse Orde van Register EDP-Auditors (NOREA) is de beroepsorganisatie voor IT-Auditors in Nederland. In samenwerking met o.a. de Auditdienst Rijk (ADR) en de Autoriteit Persoonsgegevens (AP) heeft NOREA een 'Handreiking voor de uitvoering van een PIA' gepubliceerd. In eigen woorden onderscheidt het DPIA model van NOREA zich door het volgende: "*Terwijl in de andere handleidingen risicomanagement een black box blijft, beschrijft NOREA een concrete, praktische methode om de risico's te beoordelen (risk assessment) en te behandelen (risk treatment). Dit leidt tot doordachte maatregelen. Bovendien ontstaat voor iedereen een herkenbaar risicobeeld, wat bijdraagt aan een breed draagvlak bij alle stakeholders van de DPIA. Illustratieve praktijksituaties vereenvoudigen het toepassen van de handreiking.*"[iv]
Het NOREA-model bestaat, naast de Handreiking Data Protection Impact Assessment, uit een daarbij behorend raamwerk, bestaande uit twintig pagina's, welke gemakkelijk ingevuld kan worden. Met diverse afbeeldingen is getracht een makkelijk leesbaar en duidelijk model te creëren. Voordeel van dit model is dat de stappen, de toelichting en het invulveld in één document staan. Daarbij is het NOREA-model geschikt voor zowel de private als de publieke sector. Een nadeel is dat het een vrij omvangrijk document is en dat het invullen veel expertise en tijd vereist.

- **ISO29134:2023**[v]

In het kort omschrijft de International Organization for Standardization (ISO) zich als organisatie die samen met zijn leden (National Standards Bodies van 165 landen) experts van over de hele wereld samenbrengt om internationale standaarden te creëren. Hierbij volgt de ISO trends in de markt en waar er behoefte aan guidance is, baseren ze zich op hun netwerk van experts en zijn hun standaarden uiteindelijk een product van overstemming.
Het ISO29134:2023 model is een uitgebreid model dat zich met name richt op het geven van guidance op de verschillende aspecten van een DPIA. Er komen geen specifieke vragen aan bod waarlangs een DPIA kan worden uitgevoerd. Het document is, door zijn tekstuele en uitleggende karakter, zeer geschikt voor bedrijven die besluiten om een eigen DPIA model te creëren. Dit kost namelijk veel tijd en vereist voldoende kennis van privacy en met name de DPIA.

- **Model DPIA Rijksdienst**[vi]

Doordat de Rijksoverheid in al zijn verschillende openbare lichamen veel te maken krijgt met het uitvoeren van DPIA's hebben zij hier hun eigen model voor geschreven. Dit model wordt door de gehele rijksdienst gebruikt en zorgt daarmee voor een uniforme toepassing van privacyregelgeving binnen de dienst. Het Model DPIA Rijksdienst heette voorheen het Rijksmodel GEB en is in 2021 geactualiseerd.
Het Rijksmodel GEB bestaat uit drie verschillende onderdelen, namelijk:

1. het eerste onderdeel bevat een algemene inleiding op het DPIA model en een beschrijving van het proces van de uitvoering van de DPIA
2. het tweede onderdeel bevat het model om een DPIA uit te voeren aan de hand van zeventien punten; en
3. het derde onderdeel geeft een toelichting van het model

Onderdeel twee bevat een korte opsomming van de zeventien verschillende stappen. Onder iedere stap is een korte toelichting gegeven en een uitgebreide uitleg kan bij onderdeel 3 gevonden worden. Dit model bevat dus een checklist bestaande uit zeventien verschillende punten en een uitgebreide toelichting. Een bruikbaar raamwerk, zoals NOREA hanteert, ontbreekt. Dit model is, zoals de naam al zegt, wat meer toegesneden op overheden en is daarom minder makkelijk in gebruik voor andere organisaties.
Sinds de actualisering hebben er een aantal wijzigingen plaatsgevonden. Niet alleen de benaming is gewijzigd van PIA naar DPIA, maar ook de wijze waarop het document geschreven is waardoor de tekst in een begrijpelijkere taal is geschreven. Tevens zijn er geen beperkingen meer als het aankomt op de tekstblokken en schrijven van de tekst. Hierdoor is het document makkelijker te gebruiken. Tot slot zijn er meer verwijzingen naar relevante artikelen uit de AVG en de UAVG.

- **ICO**[vii]

We kennen de Information Commissioner's Office (ICO) als de Engelse privacy toezichthouder. Net als alle andere Europese privacy toezichthouders is een van de taken van de ICO het geven van guidance. Op de website heeft de ICO een uitgebreide pagina waar zij alles omtrent de DPIA uitlegt. Van wat een DPIA is tot hoe een DPIA uitgevoerd moet worden en wanneer de ICO om advies gevraagd moet worden.
Het DPIA model van de ICO is wat minder uitgebreid. De zeven door de ICO genoemde stappen komen allemaal aan bod in het document. Echter, met in veel gevallen maar één vraag per stap krijg je niet het gevoel dat er diep op de verwerking wordt ingegaan. Het ICO model is dan ook een uitkomst voor die verwerkingen die in eerste instantie geen hoog risico met zich meebrengen maar waarvan een organisatie toch graag een DPIA zou willen uitvoeren. Je zou dit model daarom als een pre-DPIA kunnen zien.

- **CNIL**[viii]

De Franse privacy toezichthouder, beter bekend als de Commission nationale de l'informatique et des libertés (CNIL), heeft evenals de ICO en andere privacy toezichthouders guidance omtrent DPIA's gepubliceerd. Op zijn site heeft de CNIL meerdere 'PIA (Privacy Impact Assessment) Guides' gepubliceerd die niet alleen op het invullen van een DPIA ingaan maar ook uitgebreide tekst en uitleg geven. Daarnaast is het mogelijk om 'PIA Software' van de CNIL te downloaden die moet helpen bij het uitvoeren van een DPIA en algehele compliance met de AVG moet laten zien.
Het DPIA model zelf is als volgt vormgegeven. Via verschillende hoofdstukken met thema specifieke vragen word je aan de hand meegenomen door de DPIA. Bij veel vragen is het een kwestie van een invuloefening om tot beantwoording van de vraag te komen. Zeker in combinatie met de achtergrondinformatie is dit model geschikt om aan werknemers met weinig kennis van privacy mee te geven. De keerzijde is wel dat je hierdoor maar weinig kan afwijken van het model wat bij sommige complexere verwerkingen wenselijk kan zijn. Desalniettemin een zeer uitgebreid en overzichtelijk model om mee te werken.
Bij L2P hebben we deze vijf modellen en onze praktijkervaringen als adviseur en externe FG gebruikt om tot één compleet model te komen. Daarbij hebben we de verschillende modellen naast elkaar gelegd, overeenkomsten samengevoegd en unieke stappen/vragen verwerkt voor zover deze van toepassing bleken te zijn. Op deze manier hebben we beoogd een compleet basismodel DPIA te hebben gecreëerd. Ook hebben wij hierbij een uitgebreide toelichting geschreven.

Hoe voer je een DPIA uit?

Voor de uitvoering van een DPIA zijn een aantal stappen van belang. Voordat je hieraan toekomt is het belangrijk om een risico inschatting te maken. Deze risico inschatting geeft aan of je wel of niet verplicht bent om een DPIA uit te voeren. Organisaties zijn verplicht om een DPIA uit te voeren op een verwerking in het geval de verwerking waarschijnlijk een hoog privacy risico oplevert voor betrokkenen.[ix] Volgens de AVG moet er hoe dan ook een DPIA worden uitgevoerd als er sprake is van:[x]

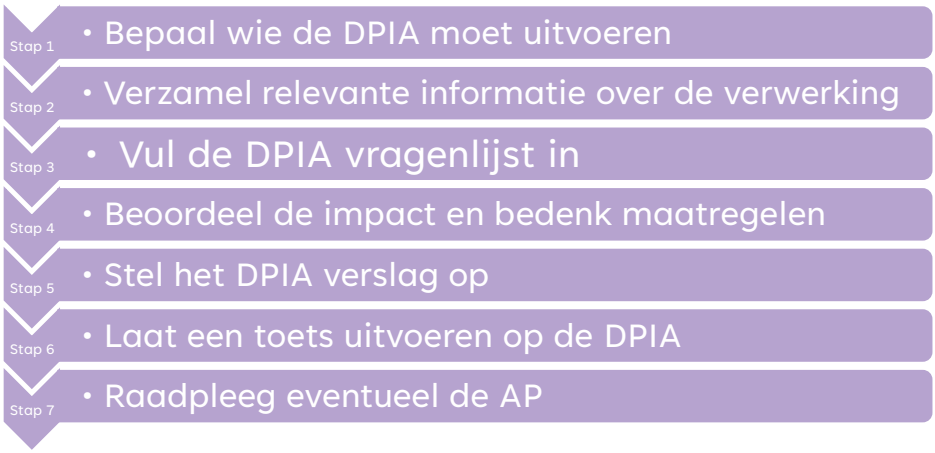
- *Een systematisch en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die gebaseerd op geautomatiseerde verwering, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke personen rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;*
- *Grootschalige verwerking van bijzondere categorieën van bijzondere persoonsgegevens of gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten;*
- *Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.*

De EDPB heeft een lijst met negen criteria opgesteld waaruit afgeleid kan worden of een DPIA verplicht is.[xi] De vuistregel die wordt gehanteerd is dat een DPIA naar alle waarschijnlijkheid moet worden uitgevoerd als de verwerking aan twee of meer van de negen criteria voldoet.

Daarnaast zegt de AVG dat ook de Toezichthoudende Autoriteiten een lijst kunnen en mogen publiceren van verwerkingen waarbij een DPIA verplicht moet worden uitgevoerd. Let daarbij op dat op het moment dat je een verwerking doet waarbij ook een andere Toezichthoudende Autoriteit betrokken is, in geval van een grensoverschrijdende verwerking, je altijd checkt of hier andere verplichtingen gelden. De AP heeft de volgende lijst van verwerkingen opgesteld waarvoor het uitvoeren van een DPIA altijd verplicht is voordat er met de verwerking begonnen wordt:[xii]

1. Heimelijk onderzoek;
2. Zwarte lijsten;
3. Fraudebestrijding;
4. Creditscores;
5. Financiële situatie;
6. Genetische persoonsgegevens;
7. Gezondheidsgegevens;
8. Samenwerkingsverbanden;
9. Cameratoezicht;
10. Flexibel cameratoezicht;
11. Controle werknemers;
12. Locatiegegevens;
13. Communicatiegegevens;
14. Internet of Things;
15. Profilering;
16. Observatie en beïnvloeding van gedrag;
17. Biometrische gegevens.

Voer je als organisatie een van bovenstaande verwerkingen uit dan ben je volgens de AP verplicht om een DPIA uit te voeren.
Als er bepaald is dat er inderdaad sprake is van een hoog risico of een van bovenstaande situaties dan zal er een DPIA uitgevoerd moeten worden. De te nemen stappen voor de uitvoering van een DPIA zijn als volgt:



Stap 1: Bepaal wie de DPIA moet uitvoeren en hoe dit gaat gebeuren

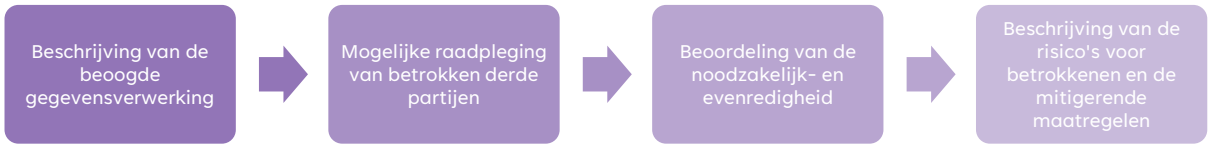
Allereerst is het van belang dat er aan het begin van een project bepaald wordt wie de DPIA gaat uitvoeren. Vaak is er een persoon per project of in de gehele organisatie die het invullen van de DPIA begeleidt. Dit betekent niet dat hij of zij ook alle antwoorden weet. In veel gevallen is het invullen van een DPIA een samenspel waarbij er één coördinator is die het overzicht houdt en bekend is met het invullen van een DPIA en een aantal sleutelfiguren uit het project/de verwerking die voor de invulling kunnen zorgen.

Stap 2: Verzamel en bestudeer relevantie informatie over het project/de verwerking

Zorg dat de juiste mensen bij worden betrokken bij het invullen van de DPIA. Er dient zoveel mogelijk informatie bekend te zijn over de werking, uitvoering en toekomst van het project om tot een volledige en correcte invulling van de DPIA te komen. Denk hierbij aan projectmanagers, IT en beleidsmanagers. Als coördinator vraag je daarnaast alle beschikbare documentatie op van het project. Op die manier kan je de DPIA-vragen met een zo'n breed mogelijke kennis van het project invullen. Waar nodig kan een interview met eerdergenoemde experts duidelijkheid geven over hoe bepaalde vragen beantwoord dienen te worden.

Stap 3: Vul de DPIA vragenlijst in

Het is van belang om vooraf als organisatie een heldere DPIA vragenlijst te hebben. Het is uiteraard mogelijk om hier zelf een vragenlijst voor te ontwikkelen maar het is ook zeker aan te raden gebruik te maken van het L2P-DPIA model of een van de andere hierboven genoemde modellen. Ondanks dat de vragenlijsten op inhoud hier en daar kunnen verschillen is de opzet veelal hetzelfde en bestaat deze uit een aantal stappen. De AVG stelt dat een DPIA minimaal aan de volgende vereisten moet voldoen:[xiii]



1. Beschrijving van de beoogde gegevensverwerking

De AVG vereist dat een systematische beschrijving van de gegevensverwerking wordt gegeven en dat hierbij rekening wordt gehouden met de aard, omvang, context en doelen van de gegevensverwerking.[xiv] Daarnaast wordt aangegeven dat de beoordeling tenminste een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden bevat, waaronder de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd.[xv] Deze stap moet dus een duidelijke en complete beschrijving bevatten van de voorgenomen gegevensverwerkingen. Onder een gegevensverwerking wordt verstaan elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, dus opslaan, verzamelen, wissen, ordenen etc.[xvi]
Besteed aandacht aan het volgende:

1. Het voorstel waar de DPIA op ziet en beschrijf in hoofdlijnen de context waarbinnen deze ziet.
2. Beschrijving van de categorieën van persoonsgegevens die worden verwerkt en geef per categorie aan op wie deze betrekking hebben.[xvii]
3. Beschrijving van de gegevensverwerking. Hierdoor moet duidelijk worden welke handeling of handelingen met betrekking tot de persoonsgegevens worden gedaan.
4. Beschrijving van de verwerkingsdoeleinden. In deze stap moeten het expliciete en legitieme doel van de gegevensverwerking worden aangegeven. Voorbeelden van verwerkingsdoeleinden zijn beveiligen van gebouwen en objecten, het opsporen van strafbare feiten en doen van leveringen en bestellingen.[xviii] Belangrijk is om de verwerkingsdoeleinden zo veel mogelijk toe te spitsen op de concrete verwerking door uit te leggen voor welk specifiek doel je welke persoonsgegevens gebruikt. Houd hierbij wel altijd het overkoepelende doel voor ogen.[xix]
5. Beschrijving van de betrokken partijen. Maak hier een overzicht van de organisaties die betrokken zijn bij de gegevensverwerking en noteer hun rol hierin.[xx]
6. Beschrijving van de belangen bij de gegevensverwerking waardoor het duidelijk wordt welke belangen de verwerkingsverantwoordelijke en anderen hebben bij de verwerking.[xxi]
7. Beschrijving van de verwerkingslocaties. Hieruit moet duidelijk worden in welke landen de gegevensverwerking plaatsvindt.
8. Techniek en methode van verwerking.
9. Beschrijving juridisch en beleidsmatig kader. Benoem de eventuele toepasselijke wet- en regelgeving naast de AVG. Het kan voorkomen dat sectorspecifieke wet- of regelgeving specifiek iets regelt over de gegevensverwerking.
10. Beschrijving van de bewaartermijnen die gelden.

2. *Mogelijke raadpleging van betrokken derde partijen*

In sommige gevallen moet je, als verwerkingsverantwoordelijke, betrokken derde partijen raadplegen. Uit art. 35 sub 9 AVG volgt dat: "*de verwerkingsverantwoordelijke vraagt in voorkomend geval de betrokkenen of hun vertegenwoordigers naar hun mening over de voorgenomen verwerking, met inachtneming van commerciële of algemene belangen of de beveiliging van verwerkingen*".
Indien betrokkenen en/of hun vertegenwoordigers worden geraadpleegd, leg dan de gegeven reactie vast en leg ook, indien tegen de mening van de betrokkenen en/of hun vertegenwoordigers wordt ingegaan, de redenen hiervoor vast.
Indien op de vraag of een dergelijke raadpleging schadelijk kan zijn voor het commerciële- of algemene belang of voor de beveiliging van de verwerking met ja kon worden beantwoord, dan hoeven de individuen niet geraadpleegd te worden.

3. *Beoordeling van de noodzakelijkheid en evenredigheid van de gegevensverwerking*

Belangrijk is om na te gaan of de beoogde gegevensverwerking noodzakelijk is voor het verwezenlijken van de verwerkingsdoeleinden. Dit gaat samen met het uitgangspunt van dataminimalisatie uit de AVG.[xxii] In deze stap moet gekeken worden naar de eisen van proportionaliteit en subsidiariteit. Bij proportionaliteit weeg je of de realisatie van de verwerkingsdoeleinden zodanig gewicht heeft dat de gegevensverwerking, gelet op de mate waarin deze privacy beperken, gerechtvaardigd is.[xxiii] Bij de eis van subsidiariteit bekijk je of de beoogde gegevensverwerking met minder ingrijpende middelen kan worden bereikt.

4. *Beschrijving van de geïdentificeerde risico's voor betrokkenen en de bestaande en toekomstige beheersmaatregelen*

Aan de hand van de aard, het toepassingsgebied, de context en de doeleinden van de gegevensverwerking dient de waarschijnlijkheid en de ernst van de geïdentificeerde risico's voor de rechten en vrijheden van betrokkenen te worden bepaald.[xxiv] Begonnen wordt met het identificeren van de risico's waarbij je de kans op het optreden van een negatief gevolg voor de rechten en vrijheden van betrokkenen als gevolg van de verwerking van persoonsgegevens beoordeeld. Daarna kom je bij het inschatten van de risico's. Ingeschat wordt wat de kans is dat het geïdentificeerde risico intreedt en wat de mogelijke gevolgen daarvan zijn voor betrokkenen. Om deze vraag te beantwoorden dient een afweging te worden gemaakt. De laatste stap voor de beschrijving van de risico's voor betrokkenen is het beoordelen van de risico's en of deze aanvaardbaar zijn. Nadat de risico's zijn beschreven en beoordeeld moet gekeken worden welke maatregelen genomen kunnen worden om de risico's te voorkomen of te verminderen. Welke maatregelen er uiteindelijk genomen worden hangt af van de belangenafweging die de verwerkingsverantwoordelijke maakt. Beschrijf per maatregel welk risico het aanpakt en wat het eventuele restrisico is nadat de maatregel is uitgevoerd. In het geval dat de maatregel het restrisico niet helemaal afdekt, moet worden gemotiveerd waarom het restrisico acceptabel is.[xxv]

Stap 4: Beoordeel de impact en bedenk waar nodig (aanvullende) maatregelen

Tijdens het proces van invullen van de DPIA vragenlijst komen er een aantal vragen aan bod die risico's blootleggen. Het is de bedoeling van een DPIA dat er aan de hand van deze risico's en genomen/te nemen maatregelen wordt bepaald wat de impact van de verwerking is op betrokkenen en in hoeverre deze in verhouding staan tot het bedrijfsbelang. Uiteindelijk zal de organisatie het overgebleven risico moeten accepteren of er voor moeten kiezen dat dat de verwerking in zijn huidige vorm niet geaccepteerd kan worden. Om dit proces in goede banen te leiden zal er een interne risico-eigenaar moeten worden aangewezen. De interne risico-eigenaar valideert de risico's en begeleidt het proces omtrent de mitigerende maatregelen.

Stap 5: Stel het DPIA verslag op

Om te zorgen voor een goede vastlegging en ter verantwoording naar de AP, zal alles wat hierboven besproken is moeten worden vastgelegd in een zogenaamd DPIA verslag. In veel gevallen, zoals bij het L2P-DPIA model, worden antwoorden in het model gegeven net zoals het bijhouden van risico's en getroffen maatregelen. Op deze manier ontstaat er één document met alle informatie die van belang is. Het is aan te raden om daarnaast ook een management samenvatting te schrijven met daarin de overwegingen en uiteindelijke conclusie. Dit ondersteunt zowel de interne als externe verantwoording.

Stap 6: Laat eventueel een (onafhankelijke) toets op de DPIA uitvoeren

Het kan voorkomen dat er een conflict is tussen het belang van de organisatie en de privacy van de betrokkenen. In die gevallen is het aan de organisatie om een afweging te maken om al dan niet te besluiten de verwerking uit te voeren. In sommige gevallen is dit vanuit de organisatie niet haalbaar. Het kan zo zijn dat de FG of een andere privacyfunctionaris een negatief advies geeft maar het bestuur of hoger management aangeeft toch door te willen gaan. In die gevallen, maar zeker ook in gevallen waarin onzekerheid bestaat over een juiste afweging, is het aan te raden om advies te vragen aan een onafhankelijke externe partij. De DPIA zal dan in Auditvorm onder handen worden genomen en er zal een onafhankelijk advies worden gegeven waarbij zowel de privacy van betrokkenen als de belangen van de organisatie in worden meegenomen.

Stap 7: Voorafgaande raadpleging

Indien uit de DPIA naar voren is gekomen dat de beoogde verwerking een hoog netto risico oplevert, is het aan de verwerkingsverantwoordelijke om maatregelen op te stellen die het risico wegnemen of in ieder geval in sterke mate verminderen. In sommige gevallen lukt het niet altijd om dit soort maatregelen op te stellen. In dit geval kan er met de AP overlegd worden voordat een verwerking wordt gestart, dit heet de 'voorafgaande raadpleging'.[xxvi] Bij voorafgaande raadpleging geeft de AP de organisatie advies in welke mate en op welke manier de risico's van de verwerking beperkt kunnen worden. Tenzij de AP adviseert om van de verwerking af te zien kan, indien gehoor wordt gegeven aan de door de AP opgelegde maatregelen, begonnen worden met de verwerking.

Een verzoek om voorafgaande raadpleging kan worden ingediend bij de AP via het daarvoor bestemde aanvraagformulier.[xxvii] Naast het aanvraagformulier dienen ook de DPIA en het privacy statement van de organisatie meegestuurd te worden. De AP neemt een verzoek tot voorafgaande raadpleging niet in behandeling wanneer er geen sprake is van een verwerking van persoonsgegevens, de verwerking waar het om gaat geen hoog risico oplevert, het aanvraagformulier onjuist is ingevuld, de verstrekte informatie tegenstrijdig is of een DPIA ontbreekt en/of niet aan de eisen voldoet.

Wat levert een DPIA op en wat doe je er mee?

Door het uitgebreide karakter van een DPIA, geeft een DPIA inzicht in het datalandschap en de datastromen van de organisatie. Doordat verschillende verwerkingen elkaar vaak aanvullen/opvolgen kan je door middel van het uitvoeren van DPIA's vaak precies zien hoe persoonsgegevens door de organisatie bewegen. Het is vaak ook een goede manier om te controleren of je systeemhuishouding in orde is. Tijdens een DPIA komen de meest recente en te gebruiken systemen aan bod en kom je systemen tegen die niet gebruikt hoeven te worden en/of verouderd zijn. Systemen die niet gebruikt hoeven te worden of verouderd zijnkunnen worden meegenomen in een grote schoonmaak. Vaak staan hier nog grote datasets in opgeslagen die allang verwijderd hadden moeten worden.

Zoals eerder al aan bod is gekomen, zorgt een DPIA voor inzicht in de privacy risico's van een bepaalde verwerking. In veel gevallen zullen er mitigerende maatregelen worden genomen om deze risico's weg te nemen. Dit proces van mitigerende maatregelen is niet enkel een kwestie van het benoemen van de maatregelen, maar deze maatregelen zullen ook actief gemonitord moeten worden door een aangewezen risico-eigenaar. De risico-eigenaar is verantwoordelijk voor het implementatieproces rondom de mitigerende maatregel(en), hij of zij zal er daarnaast voor moeten zorgen dat er periodieke controle plaatsvindt of de getroffen maatregel(en) nog wel doeltreffend zijn.

Deze periodieke controle gaat vaak samen met een algehele herbeoordeling van de DPIA. Tijdens zo'n herbeoordeling zal er gekeken moeten worden of en in hoeverre de verwerking onveranderd is. Er zal met name gekeken moeten worden naar het doel en de middelen van de verwerking. Als deze veranderen zullen er hoogstwaarschijnlijk ook andere risico's ontstaan. Daarnaast is het van belang dat er gecontroleerd wordt of de bestaande risico's nog steeds voldoende worden weggenomen door de mitigerende maatregel(en).

Gevolgen van het niet uitvoeren en/of een niet goed uitgevoerde DPIA

Op het moment dat een DPIA (deels) niet goed wordt uitgevoerd, kan dit leiden tot een verkeerde risico-inschatting. Deze verkeerde risico-inschatting kan op zijn beurt ervoor zorgen dat betrokkenen een te groot risico lopen. Ondanks dat een hoog risico niet altijd hoeft te resulteren in een schending van de rechten van betrokkenen of een datalek kan dit wel een reden zijn voor de AP om, na onderzoek, een waarschuwing of zelfs een boete op te leggen. Indien achteraf blijkt dat een DPIA niet goed genoeg uitgevoerd is of in zijn geheel niet uitgevoerd is wanneer deze wel uitgevoerd had moeten worden, kan de AP een boete opleggen en de verwerking per direct stopzetten.

De AP heeft in haar Boetebeleidsregels van 10 februari 2019 bepaalt dat de basisboete op het niet uitvoeren van een DPIA door overheidsinstanties voorafgaand aan een verwerking in Categorie II van het Boetebesluit valt en dus €310.000,- bedraagt, welke uiteraard naar boven of beneden bijgesteld kan worden op basis van de specifieke omstandigheden van het geval.[xxviii] Voor het berekenen van de op te leggen boete aan bedrijven, ziekenhuizen en particuliere scholen, berekent de AP de hoogte van de boete van het niet uitvoeren van een DPIA op basis van de fining guidelines van het EDPB.[xxix]

Maar controleren toezichthouders ook daadwerkelijk op het wel of niet uitvoeren van een DPIA? Jazeker! De AP heeft op 30 april 2020 een productiebedrijf een boete opgelegd van €725.000 voor de onrechtmatige verwerking van vingerafdrukgegevens. Voor een nieuw aanwezigheids- en tijdsregistratiesysteem moeten werknemers namelijk hun vingerafdrukken laten scannen. Vingerafdrukken worden aangemerkt als bijzondere persoonsgegevens waarvoor een verwerkingsverbod geldt tenzij een uitzonderingsgrond kan worden aangetoond.[xxxv] De AP heeft geconcludeerd dat het productiebedrijf op geen enkele wettelijke uitzondering een beroep kan doen, er geen voorafgaande DPIA is uitgevoerd voorafgaand aan de verwerking en dat verder toestemming niet is aangetoond.[xxxi] Daarnaast ziet de controleert de AP niet alleen op de naleving van de DPIA verplichting in de AVG, maar ook op de DPIA verplichting uit nationale specifieke wetgeving, blijkt uit de boete van €50.000,- die de AP op 17 november 2022 heeft opgelegd.[xxxii] De boete heeft de AP opgelegd omdat de politie geen DPIA uit heeft gevoerd alvorens het inzetten van camera auto's. De AP heeft geconcludeerd dat een DPIA uitvoeren van DPIA op grond van de Wet politiegegevens wel verplicht was. De politie had namelijk kunnen weten dat het inzetten van de camera-auto's een hoog risico voor de privacy van betrokkenen kon opleveren; bij de inzet van de camera's heeft de politie gebruik gemaakt van nieuwe technologieën. Maar ook andere Europese toezichthouders handhaven. Zo heeft de Franse Autoriteit (CNIL) voor Gegevensbescherming een boete opgelegd aan DISCORD INC. van €800.000,- voor het niet naleven van de verplichtingen uit de AVG, waaronder de verplichting om een DPIA uit te voeren. DISCORD INC. was van mening dat het uitvoeren van een DPIA voor de voice over IP (technologie waarmee gebruikers kunnen chatten via hun microfoon en/of

webcam op het internet) waar zij gebruik van maken, niet nodig was. De CNIL concludeerde echter dat gezien de hoeveelheid gegevens DISCORD INC. verwerkt, en door het gebruik van de diensten van DISCORD INC. door jonge gebruikers, het uitvoeren van een DPIA wel noodzakelijk is. Het niet uitvoeren van een DPIA levert daarom een breuk van artikel 35 van de AVG op.[xxxiii]

Raakvlakken met andere AVG thema's

De DPIA hangt samen met verschillende thema's uit de AVG. Zo zijn een deel van de vereisten die volgens de AVG in een DPIA moeten terugkomen ook in het verwerkingsregister vastgelegd. Denk aan de verwerking gekoppeld aan de persoonsgegevens die er verwerkt worden, de systemen die voor de verwerking gebruikt worden, de individuen die het betrekt maar ook verwerkers en subverwerkers die gebruikt worden voor de verwerking. Daarnaast geeft het verwerkingsregister input voor de DPIA en kan het je helpen met de vaststelling van de scope van de DPIA.

Hetzelfde geldt voor de koppeling naar je contractmanagement (vendormanagement). Binnen een ideale organisatie wil je dat zowel je vendormanagement als je verwerkingsregister als je systeem- en dataregister met elkaar gelinkt zijn. Op die manier kan je uit je vendormanagementsysteem halen welke partijen er betrokken zijn bij een bepaalde verwerking, of daar wel een contract of verwerkingsovereenkomst mee is afgesloten en welke gegevens zij verwerken.

Bovenstaande zie je terug in een DPIA. De DPIA beschrijft namelijk van één verwerking welke partijen, systemen, data en individuen hierbij betrokken zijn. Om een goede en complete DPIA te kunnen opstellen is het dan ook van belang om de eerdergenoemde systemen up-to-date te hebben.

Conclusie

Om de privacy risico's voor betrokkenen te minimaliseren binnen een organisatie is het nodig dat DPIA's worden uitgevoerd op verwerkingen die vanuit hun aard een hoog risico met zich meebrengen. Het proces omtrent een DPIA bestaat uit het achterhalen van de kern van de verwerking, welke risico's deze met zich meebrengt en hoe die het beste gemitigeerd kunnen worden. Het is niet zozeer een kwestie van het invullen van een Word document met een paar risico's en wat maatregelen ('ticking the box'). De DPIA zal de vorm moeten hebben van een audit op die specifieke verwerking waarbij er door experts binnen die verwerking antwoord is gegeven op vragen over alle verschillende kanten van het proces. Veel organisaties hebben dan ook moeite met het opstellen van een compleet document om dergelijke vragen te beantwoorden en om op die manier zo zorgvuldig mogelijk te zijn. Gelukkig staat de uniforme aard van een DPIA het toe dat bedrijven niet per se hun eigen document hoeven te ontwikkelen maar gebruik kunnen maken van een basismodel, zoals we die eerder al in deze factsheet beschreven hebben.
Wilt u meer informatie over het uitvoeren van een DPIA, de er mee gepaard gaande tijd en kosten of heeft u vrijblijvend interesse in ons L2P-model? Neem dan contact met ons op.

Gezonde groet,
L2P
+31 (0) 26 848 3118
info@l2p.nl

Geraadpleegde bronnen

I. Groep Gegevensbescherming artikel 29, WP 248, *Groep artikel 29* Goedgekeurd op 4 april 2017 en laatstelijk gewijzigd en vastgesteld op 4 oktober 2017.
II. Art. 35 AVG.
III. NOREA, 'Privacy Impact Assessment (PIA)', *NOREA* november 2015.
IV. NOREA, 'Nieuwe NOREA-Handreiking Data Protection Impact Assessement (DPIA), *NOREA augustus 2019*
V. ISO/IEC 29134:2023 Information technology – Security techniques – Guidelines for privacy impact assessment.
VI. Rijksoverheid, 'Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA)', *Rijksoverheid* september 2017.
VII. Information Commissioner's Office, 'Data Protection Impact Assessment (DPIAs)', (Ico.org.uk).
VIII. CNIL, 'Privacy Impact Assessment (PIA)', (CNIL.fr).
IX. Art. 35 AVG.
X. Art. 35 lid 3 AVG.
XI. EDPB, 'The list of types of personal data processing operations, for which carrying out a Data Protection Impact Assessment (DPIA) is required', (Edpb.europa.eu); Autoriteit Persoonsgegevens, 'Data protection impact assessment (DPIA)', *Autoriteitpersoonsgegevens.nl*.
XII. Autoriteit Persoonsgegevens, 'Data protection impact assessment (DPIA)', (autoriteitpersoonsgegevens.nl)
XIII. Art. 35 lid 7 AVG.
XIV. Overweging 90 AVG.
XV. Art. 35 lid 7 onder a AVG.
XVI. Art. 4 AVG.
XVII. Rijksoverheid, 'Model DPIA Rijksdienst', *Rijksoverheid* november 2021.
XVIII. Informatiebeveiligingsdienst, 'Handreiking DPIA', *IBD* augustus 2020.
XIX. Idem.
XX. Idem.
XXI. Rijksoverheid, 'Model DPIA Rijksdienst', *Rijksoverheid* november 2021.
XXII. Art. 5 lid 1 sub c AVG.
XXIII. Idem.
XXIV. Idem.
XXV. Idem.
XXVI. Autoriteit Persoonsgegevens, 'Voorafgaande raadpleging', (autoriteitpersoonsgegevens.nl).
XXVII. Idem.
XXVIII. Boetebeleidsregels Autoriteit Persoonsgegevens 2019, 14 maart 2019.
XXIX. Autoriteit Persoonsgegevens, 'Nieuw boetebeleid voor overtredingen AVG', (autoriteitpersoonsgegevens.nl).
XXX. Art. 9 lid 1 AVG.
XXXI. Autoriteit Persoonsgegevens, 'Boete vingerafdrukken personeel', (autoriteitpersoonsgegevens.nl).
XXXII. Autoriteit Persoonsgegevens, 'Boete mobiele camera-auto's Rotterdam', (autoriteitpersoonsgegevens.nl).
XXXIII. CNIL, 'Sanction de 800 000 euros à l'encontre de la société DISCORD INC.' , (cnil.fr).

L2P
Stadsplateau 7
3521 AZ Utrecht

+31 (0) 26 848 3118
info@l2p.nl