Data Protection Impact Assessment

Wat is een Data Protection Impact Assessment?

Als u de privacyrisico's van een bedrijfsproces in een vroeg stadium in beeld wilt brengen, kunt u ons een DPIA laten uitvoeren. Bij een DPIA "keurt de slager niet zijn eigen vlees", maar treedt BKBO op als onafhankelijk keurmeester. Op een gestructureerde en heldere manier brengen wij voor u de belangrijke risico's in beeld en geven u aanbevelingen om de aangetroffen risico's te verminderen of weg te nemen. Een DPIA wijst uit welke persoonsgegevens worden gebruikt, welke beschermende maatregelen zijn genomen, wat de impact is op de betrokkene(n) en uw organisatie en welke verbetermaatregelen kunnen worden genomen.

Met een DPIA krijgt u antwoord op vragen als:

- Welke persoonsgegevens worden gebruikt en zijn ze nodig?
- Wat is de impact van het bedrijfsproces op de privacy?
- Wat zijn de risico's voor de betrokkenen en voor de organisatie?
- Zijn de taken, bevoegdheden en verantwoordelijkheden belegd?
- Zijn uw maatregelen om de privacy te beschermen adequaat?
- Zijn er bewerkers en zijn daarmee overeenkomsten gesloten en worden deze nageleefd?
- Hoe zit het met de gebruikte applicaties. Ondersteunen deze het proces of wordt ook gebruik gemaakt van andere minder betrouwbare voorzieningen? Is het veilig, wordt er gelogd, worden de persoonsgegevens versleuteld?
- Welke verbeteringen zijn mogelijk? Is een aanpak mogelijk die minder gevolgen heeft voor de privacy?

Verplicht op basis van de AVG

Vanaf 25 mei 2018 -de inwerkingtreding van de Algemene Verordening Gegevensbescherming is een DPIA wettelijk vereist vóór ingebruikname van een nieuwe persoonsgegevensverwerking onder bepaalde condities. Een DPIA moet worden uitgevoerd als bij de verwerking van persoonsgegevens een groot privacyrisico ontstaat voor de mensen. Een DPIA is in elk geval verplicht als:

- U als organisatie uitvoerig en systematisch persoonlijke gegevens beoordeelt; daarbij kan het bijvoorbeeld gaan om beroepsprestaties, prognoses, persoonlijke voorkeuren, gezondheid, of het gedrag;
- U als organisatie op een grote schaal bijzondere gegevens van personen verwerkt;
- U als organisatie systematisch en op grote schaal mensen volgt in een publiek toegankelijk gebied, bijvoorbeeld met camera's.

De Autoriteit Persoonsgegevens heeft een lijst opgesteld van verwerkingen waarvoor een DPIA verplicht is.

1. Heimelijk onderzoek

Grootschalige en/of systematische verwerkingen van persoonsgegevens waarbij informatie wordt verzameld door middel van onderzoek zonder dat de betrokkene daarvan vooraf op de hoogte te

stellen.
Bijvoorbeeld heimelijk onderzoek door particuliere recherchebureaus, onderzoek in het kader van fraudebestrijding en onderzoek op internet in het kader van bijvoorbeeld online handhaving van auteursrechten. Heimelijk cameratoezicht door werkgevers in het kader van diefstal- of fraudebestrijding door werknemers (bij deze laatste verwerking dient ook in incidentele gevallen een DPIA te worden uitgevoerd).

2. Zwarte lijsten
Verwerkingen waarbij persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag of gegevens over slecht betalingsgedrag door organisaties of particulieren worden verwerkt en gedeeld met derden.

Bijvoorbeeld zwarte lijsten of waarschuwingslijsten, zoals deze bijvoorbeeld gebruikt worden door verzekeraars, horeca-bedrijven, winkelbedrijven, telecomproviders als ook zwarte lijsten die betrekking hebben op onrechtmatig gedrag van werknemers, bijvoorbeeld in de zorg of door uitzendbureaus).

3. Fraudebestrijding
Grootschalige en/of systematische verwerkingen van (bijzondere) persoonsgegevens in het kader van fraudebestrijding. Bijvoorbeeld fraudebestrijding door sociale diensten of door fraudeafdelingen van verzekeraars.

4. Creditscores
Grootschalige en/of systematische gegevensverwerkingen die leiden tot of gebruik maken van inschattingen van de kredietwaardigheid van natuurlijke personen, bijvoorbeeld tot uitdrukking gebracht in een creditscore.

5. Financiële situatie
Grootschalige en/of systematische verwerkingen van financiële gegevens waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden. Bijvoorbeeld overzichten van bankoverschrijvingen, overzichten van de saldi van iemands bankrekeningen of overzichten van mobiele- of pinbetalingen.

6. Genetische persoonsgegevens
Grootschalige en/of systematische verwerkingen van genetische persoonsgegevens. Bijvoorbeeld DNA-analyses ten behoeve van het in kaart brengen van persoonlijke kenmerken, bio-databanken.

7. Gezondheidsgegevens
Grootschalige verwerkingen van gegevens over gezondheid (bijvoorbeeld door instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, arbodiensten, reïntegratiebedrijven, (speciaal)onderwijsinstellingen, verzekeraars, en onderzoeksinstituten) waaronder ook grootschalige elektronische uitwisseling van gegevens over gezondheid.

Individuele artsen en individuele zorgprofessionals zijn op grond van overweging 91 van de AVG uitgezonderd van de verplichting een DPIA uit te voeren.

8. Samenwerkingsverbanden

Het delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard (zoals gegevens over gezondheid, verslaving, armoede, problematische schulden, werkloosheid, sociale problematiek, strafrechtelijke gegevens, betrokkenheid van jeugdzorg of maatschappelijk werk) met elkaar uitwisselen. Bijvoorbeeld in wijkteams, veiligheidshuizen of informatieknooppunten.

9. Cameratoezicht

Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten met behulp van camera's, webcams of drones.

10. Flexibel cameratoezicht

Grootschalig en/of systematisch gebruik van flexibel cameratoezicht. Bijvoorbeeld camera's op kleding of helm van brandweer- of ambulancepersoneel, dashcams gebruikt door hulpdiensten.

11. Controle werknemers

Grootschalige en/of systematische verwerking van persoonsgegevens om activiteiten van werknemers te monitoren. Bijvoorbeeld controle van e-mail en internetgebruik, GPS-systemen in (vracht)auto's van werknemers of cameratoezicht ten behoeve van diefstal- en fraudebestrijding.

12. Locatiegegevens

Grootschalige en/of systematische verwerking van locatiegegevens van of herleidbaar tot natuurlijke personen. Bijvoorbeeld door (scan)auto's, navigatiesystemen, telefoons, of verwerking van locatiegegevens van reizigers in het openbaar vervoer.

13. Communicatiegegevens

Grootschalige en /of systematische verwerking van communicatiegegevens inclusief metadata herleidbaar tot natuurlijke personen, tenzij en voor zover dit noodzakelijk is ter bescherming van de integriteit en de veiligheid van het netwerk en de dienst van de betrokken aanbieder, of het randapparaat van de eindgebruiker.

14. Internet of things
Grootschalige en/of systematische verwerkingen door verantwoordelijken van persoonsgegevens die worden gegenereerd door apparaten die verbonden zijn met internet en die via internet of anderszins gegevens kunnen versturen of uitwisselen. Bijvoorbeeld 'internet of things'- toepassingen, zoals slimme televisies, slimme huishoudelijke apparaten, connected toys, smart cities, slimme energiemeters, medische hulpmiddelen, etc.

15. Profilering
Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering). Bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag.

16. Observatie en beïnvloeding van gedrag
Grootschalige verwerkingen van persoonsgegevens waarbij op systematische wijze via geautomatiseerde verwerking gedrag van natuurlijke personen geobserveerd, verzameld, vastgelegd of beïnvloed wordt, inclusief gegevens die voor het doel online behavioural advertising worden verzameld.

Wat kunnen wij u bieden?

Wij kennen de markt, de situatie waarin u zich bevindt en waar u tegenaan loopt. Wij weten als geen ander wat het belang is van privacybescherming voor de burger, uw klant of de consument. Wij combineren kennis van uw bedrijfsprocessen met onze ervaring als IT-auditor. De DPIA start met een gegevensanalyse, welke persoonsgegevens worden wanneer gebruikt in uw bedrijfsproces. Dat gaan we aan het scherm na met uw functioneel beheer. Vervolgens interviewen we de sleutelfiguren uit uw bedrijfsproces en de CISO , FG en het management. Vanuit kwaliteitsoogpunt zet BKBO voor de uitvoering van de DPIA gecertificeerde register IT-auditors in. Dit betekent dat we veel werk steken in de herleidbaarheid van onze conclusies en dat informatiebeveiliging steeds onze aandacht zal hebben. Vanzelfsprekend werken we conform de richtlijnen van de Autoriteit Persoonsgegevens.

Wat is uw voordeel?

Na het uitvoeren van een DPIA, kunt u gerichte verbeteringen aanbrengen. Hierdoor worden kostbare aanpassingen in een later stadium voorkomen. Bijvoorbeeld een volledig herontwerp van het bedrijfsproces of een migratietraject dat moet worden stopgezet. We steken veel tijd en energie in het op maat maken van aanbevelingen om de privacyrisico's te beperken.

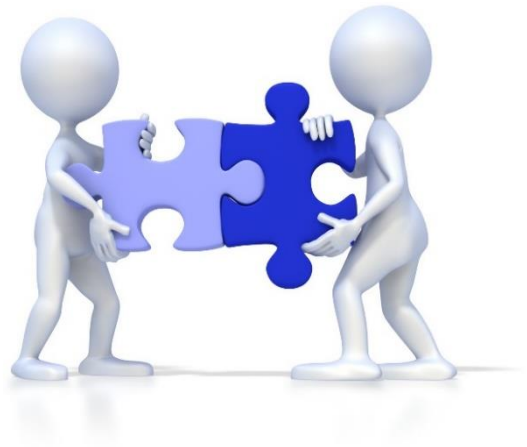
Onderscheidend van onze aanpak ten opzichte van de vele privacy adviesbureaus is dat wij als auditors uw privacy issues klip en klaar blootleggen en aanbevelingen doen zonder het belang om vervolgens in een langdurig adviestraject de zaak op te lossen. Uiteraard werken we wel samen met een aantal gerenommeerde privacy adviseurs.

Data Protection Impact Assessment

Wat kunt u met een DPIA bereiken?

- betere kwaliteit van gegevens doordat de gegevensstromen kritisch worden geanalyseerd;
- betere besluitvorming doordat u zich op actuele, volledige en tijdige gegevens baseert;
- meer privacy bewustzijn binnen uw organisatie;
- betere haalbaarheid van een project doordat privacy in de ontwerpfase wordt meegenomen;;
- meer vertrouwen van uw cliënten en medewerkers, in hoe omgaat met privacy;
- geen verrassingen doordat u laat zien privacy serieus te nemen en de risico's te beperken.

Hoe pakken wij dat aan?



De basis wordt gelegd door een gestructureerd documentenonderzoek, waarbij we gedegen werken volgens de Norea Documentatie-richtlijn waarbij elke conclusie terug te voeren is op bewijsvoering zodanig dat een andere auditor tot dezelfde uitkomst zou komen. Daarna volgen de interviews. We hanteren de DPIA-vragenlijst van de NOREA. Alle interviews worden opgenomen, door ons uitgewerkt en ter accordering voorgelegd. We hebben slechts een beperkt aantal sessies nodig om samen met u de situatie te doorgronden. Na een technisch onderzoek, stellen wij een concept-rapportage op en beoordelen uw bedrijfsproces met name op vertrouwelijkheid. In een eindbespreking nemen we het rapport door aan de hand van een presentatie. Gezamenlijk bekijken we de risico's en lichten wij onze aanbevelingen toe. De resultaten van het eindgesprek worden vervolgens door ons verwerkt in een eindrapportage. De doorlooptijd van de DPIA is drie tot vier weken.

Wat is uw investering?

De kosten van de DPIA zijn afhankelijk van de omvang en complexiteit van het project of bedrijfsproces, het aantal personeelsleden van uw organisatie dat moet worden geïnterviewd en het aantal vestigingen. Normaal gesproken liggen de kosten tussen de € 6.500,- en € 12.000,-. Wanneer de omstandigheden tijdens de looptijd veranderen, is het raadzaam de DPIA te herhalen. U vindt een handreiking op de website van de beroepsorganisatie van IT-auditors (NOREA).

Wilt u meer weten?

Dit product wordt voor uw situatie geheel op maat gemaakt. Daarom kunnen wij ons voorstellen dat u nog vragen heeft. Wij staan voor u klaar en gaan graag met u in gesprek om tot een definitieve offerte te komen. U kunt direct bellen met BKBO op telefoonnummer: 073 – 211 03 37. Is het voor u duidelijk? Dan kunt u ook direct een offerte aanvragen. Ga naar de site: https://bkbo.nl/producten/privacy-impact-assessment