ORGANISEERT DE EERSTE LIJN

HANDREIKINGDATA PROTECTION IMPACT ASSESSMENT (DPIA)

Wanneer moet een DPIA worden uitgevoerd?
Een 'Data Protection Impact Assessment' (DPIA, ook wel PIA of GEB genoemd) wordt in twee situaties uitgevoerd:

1 IN EEN STABIELE SITUATIE

In een stabiele situatie moet een DPIA worden uitgevoerd, om de actuele situatie van de gegevensbescherming in kaart te brengen. Deze DPIA is eenvoudiger, omdat minder vragen relevant zijn. Aanbevolen wordt om dit onderdeel te maken van het (kwaliteits)proces voor de gegevensbescherming (de 'PDCA cyclus'), zodat bijvoorbeeld de maatregelen en overeenkomsten regulier tegen het licht worden gehouden.

2 BIJ EEN VERANDERING

Bijvoorbeeld bij: organisatorische verandering (fusie), ICT verandering (nieuwe techniek) of verandering met betrekking tot verwerking (samenvoegen van administraties). In de DPIA worden in dit geval de effecten van een verandering vastgelegd en worden maatregelen beschreven om eventuele negatieve gevolgen te mitigeren. Bij een verandering moet een groot aantal vragen beantwoord moet worden met betrekking tot de mogelijk negatieve effecten op betrokkenen. Aanbevolen wordt om dit onderdeel te laten uitmaken van het veranderingsproces/project.

1 STAPPENPLAN DPIA IN EEN STABIELE SITUATIE

De volgende stappen kunnen worden gevolgd voor het uitvoeren van een DPIA in een stabiele situatie:

1 Register van verwerkingen

Maak het register van verwerkingen (verwerkingsregister). InEen heeft via LINK een voorbeeld verwerkingsregister beschikbaar gesteld.

RESULTAAT
Overzicht van alle verwerking en per verwerking:
a De doelen van de verwerking.
b Categorieën betrokkenen (de personen waarover gegevens worden vastgelegd).
c De categorieën persoonsgegevens.

Wanneer u het register van verwerkingen al heeft gemaakt hoeft u alleen te beoordelen of deze actueel en compleet is. Na (eventueel) actualiseren en aanvullen stelt u het register opnieuw vast.

2 Benoemen bijzondere categorieën

Wijs de verwerkingen aan die bijzondere categorieën van persoonsgegevens (vaak patiëntgegevens of personeelsgegevens) bevatten. Op deze bijzondere gegevens is een DPIA van toepassing.

RESULTAAT
U weet nu waar de DPIA op van toepassing is.

3 Beoordeel de doelbinding

Beoordeel of de doelen van elke verwerking (zie 1a) overeenstemmen met de categorieën persoonsgegevens (1b). Doe dit door het beantwoorden van de vraag: Zijn alle gegevens die ik registreer noodzakelijk voor het realiseren van de doelen van de verwerking?

Als het antwoord JA is: ga door naar stap 4.
Als het antwoord NEE is: verwijder de categorieën persoonsgegevens, die niet nodig zijn voor de gestelde doelen uit de verwerking.

RESULTAAT
U weet dat u voldoet aan de eis 'doelbinding' (u mag alleen persoonsgegevens verwerken ten behoeve van een vooraf gesteld doel).

4 Beoordeel de risico's en maatregelen

Gebruik de handreiking van InEen 'Handreiking risicobeoordeling' om:
a Een risicobeoordeling uit te voeren.
b Passende beveiligingsmaatregelen vast te leggen.

Wanneer u al een risicobeoordeling heeft uitgevoerd en de beveiligingsmaatregelen heeft geïmplementeerd of gepland: beoordeel of deze nog actueel zijn en leg dit vast.

RESULTAAT
U weet wat uw beveiligings- en privacy risico's zijn en u heeft grotere zekerheid dat u hiertegen passende maatregelen heeft genomen.

5. Toezicht en evaluatie

Plan periodiek, bijvoorbeeld als onderdeel van de PDCA cyclus (tenminste jaarlijks):
a Actualiseren van het Register van verwerkingen.
b Her-evaluatie van de beoordeling van de doelen in relatie tot de categorieën persoonsgegevens.
c Bijstellen van de risicobeoordeling en de geplande /geïmplementeerde maatregelen.
d De controle op de juiste werking van de maatregelen.
e Documenteren van punten a tot en met d

RESULTAAT
U heeft aantoonbaar maatregelen genomen om te voldoen aan de AVG.

2 STAPPENPLAN DPIA BIJ EEN VERANDERING

De volgende stappen kunnen worden gevolgd voor het uitvoeren van een DPIA in een stabiele situatie:

Vooraf
Het is belangrijk om een DPIA in een vroeg stadium van een verandering uit te voeren. Bijvoorbeeld aan het begin van het project wat de verandering moet realiseren. Zo helpt de DPIA om het privacybelang mee te nemen bij het verdere ontwerp of uitvoering ('Privacy by design' of 'Privacy by default'). Op die manier kan worden voorkomen dat later kostbare aanpassingen nodig zijn om alsnog noodzakelijke beveiligingsmaatregelen door te voeren.

Wanneer omstandigheden of het doel tijdens de looptijd van het project veranderen, moet de DPIA opnieuw uitgevoerd worden.

Door de DPIA bij aanvang van elk project uit te voeren zorgt u ervoor dat de privacy een belangrijke plaats binnen uw organisatie inneemt (tip: neem de DPIA op in het sjabloon voor het projectplan). Het helpt ook bij bewustwording van betrokkenen. Daarom bevelen we aan om de DPIA bij elke verandering uit te voeren, ook wanneer het project klein is en u eigenlijk verwacht dat het geen invloed zal hebben op de privacy. Deze vragenlijst is zo opgesteld dat, wanneer het project weinig tot geen gevolgen heeft, u de vragenlijst ook snel kunt afronden.

Voorbeelden van veranderingen waarbij een DPIA nodig is:

1 ICT projecten, zoals:
   a Aanschaf of ontwikkeling van nieuwe applicaties.
   b Aanschaf van nieuwe hardware, zoals PC's, telefoons, laptops etc.
   c Het wisselen van ICT – leverancier.
2 Organisatieveranderingen, zoals:
   a Aangaan van een samenwerking of fusie met een andere organisatie.
   b Het uitbreiden de organisatiedoelen.
   c Het veranderen van de organisatiestructuur.

De volgende stappen kunnen worden gevolgd voor het uitvoeren van een DPIA bij een verandering:

1 Bepaal wie de DPIA gaat uitvoeren

Het is belangrijk dat de juiste personen (mensen van binnen en/of buiten uw organisatie) input kunnen geven op de DPIA:

a Stel vast welke personen betrokken moeten worden bij het uitvoeren van de DPIA.
b Wijs een verantwoordelijke aan voor het uitvoeren van de DPIA en de rapportage aan de directie en/of bestuur.

2 Formuleer de opdracht voor de DPIA

Formuleer, samen met de persoon die verantwoordelijk is voor de DPIA, een heldere opdracht. In de opdracht moet vermeld worden:

a Welke verandering de aanleiding is van de DPIA.
b Wanneer de DPIA gereed moet zijn.
c Hoe het resultaat van de DPIA vastgelegd wordt en aan wie gerapporteerd wordt.
d Welke methodes gebruikt worden om de DPIA uit te voeren. Methodes kunnen zijn:
   I Interviews met medewerkers en/of belanghebbenden.
   II Inwinnen van advies van interne/externe juristen of ICT-specialisten.
   III Een onderzoek door een externe adviseur.
e Op welke manier de resultaten van DPIA gebruikt worden. Bijvoorbeeld om het project bij te stellen en wie daarover beslist.

3 Stel het DPIA rapport op

Het DPIA rapport moet antwoord geven op de volgende vragen:

a Om welke verwerkingen (applicaties) gaat het? Op welke manier veranderen de doelen en inhoud van de verwerkingen?
b Als het gaat om een nieuwe verwerking (applicatie): zijn de persoonsgegevens in deze verwerking in lijn met het doel van de verwerking? En is het doel van de verwerking in lijn met de legitieme organisatiedoelen?
c Welke risico's voor privacy en/of informatieveiligheid zijn geconstateerd?
d Welke maatregelen zijn genomen/gepland om deze risico's aan te pakken?

U kunt als basis voor het DPIA rapport de vragenlijst uit de bijlage gebruiken.

BIJLAGE: VRAGENLIJST DPIA BIJ EEN VERANDERING

	VRAAG	JA	NEE
1	Leidt de verandering tot een nieuwe verwerking (bijvoorbeeld een nieuwe applicatie) met persoonsgegevens?	Ga door naar vraag 2	Ga door naar vraag 4
2	Is duidelijk vastgelegd dat de nieuwe verwerking in lijn is met legitieme doelen van uw organisatie?		**HET RISICO IS HOGER**
3	Worden in de nieuwe verwerking (applicatie) soorten persoonsgegevens vastgelegd die u tot nu toe nog niet vastlegt?	**HET RISICO IS HOGER**	
4	Leidt de verandering tot wijzigingen in de uitwisseling van persoonsgegevens met andere partijen?	**HET RISICO IS HOGER**	
5	Zijn meer partijen (andere organisaties) actief betrokken bij de verandering?	**HET RISICO IS HOGER**	
6	Hebben/krijgen meer partijen toegang tot de nieuwe of een bestaande verwerking (applicatie)? Bijvoorbeeld ketenpartners die persoonsgegevens ook inzien/veranderen?	**HET RISICO IS HOGER**	
7	Worden op basis van persoonsgegevens beslissingen genomen over betrokkenen?	**HET RISICO IS HOGER**	
8	De privacywetgeving stelt eisen aan verwerkingen (applicaties) op het gebied van: — Logging — Mogelijkheid tot inzage, verwijdering, correctie door betrokkenen — Mogelijkheid persoonsgegevens over te dragen of te vernietigen — Beveiliging van persoonsgegevens dmv encryptie en twee factor authenticatie. Zijn deze beveiligingseisen duidelijk vastgelegd en wordt aan deze eisen voldaan?		**HET RISICO IS HOGER**
9	Is duidelijk bepaald dat de, bij het verandering betrokken, leveranciers voldoende capabel zijn? En is afgesproken dat deze leveranciers een verwerkersovereenkomst willen afsluiten?		**HET RISICO IS HOGER**
10	Omvat de verandering toepassing van nieuwe technieken?	**HET RISICO IS HOGER**	
11	Is duidelijk vastgelegd dat alle persoonsgegevens in de nieuwe verwerking noodzakelijk zijn?		**HET RISICO IS HOGER**
12	Kunnen de persoonsgegevens gebruikt worden om het gedrag, de aanwezigheid of prestaties van mensen in kaart te brengen en/of te beoordelen (ook al is dit niet het doel)?	**HET RISICO IS HOGER**	
13	Betreft het een reorganisatie/organisatieverandering binnen de eigen organisatie?	Ga door naar vraag 14	
14	Leidt de reorganisatie tot veranderingen in de toewijzing van verantwoordelijkheden voor ICT en /of informatiebeveiliging?	**HET RISICO IS HOGER**	
15	Leidt de reorganisatie tot veranderingen in het gebruik van verwerkingen (applicaties) met persoonsgegevens?	**HET RISICO IS HOGER**	
16	Leidt de reorganisatie tot veranderingen in het beheer van verwerkingen (applicaties) met persoonsgegevens?	**HET RISICO IS HOGER**	

17	Betreft het een fusie of een verandering in de samenwerking met een andere organisatie?	Ga door naar vraag 18	Ga door naar vraag 20
18	Hebben deze organisaties een beleid opgesteld met betrekking tot informatiebeveiliging?		**HET RISICO IS HOGER**
19	Hebben deze organisaties een register van verwerkingen opgesteld?		**HET RISICO IS HOGER**
20	Betreft het een verhuizing, of verbouwing?	Ga door naar vraag 21	Ga door naar vraag 22
21	Heeft u in het project een plan gemaakt voor beveiliging van het ICT-netwerk, de hardware op de locaties en voor de beveiliging tijdens de verhuizing/verbouwing?		**HET RISICO IS HOGER**
22	Houdt de verandering in dat u contracten aangaat met nieuwe leveranciers?	**HET RISICO IS HOGER**	Ga door naar het einde van deze vragenlijst
23	Heeft u overzicht van alle eisen die u moet stellen aan deze leveranciers ivm informatiebeveiliging (zoals een verwerkersovereenkomst of geheimhoudingsverklaring)	Ga door naar het einde van deze vragenlijst	**HET RISICO IS HOGER**

Na beantwoorden van alle vragen handelt u als volgt:

1 Voor alle vragen die leiden tot de conclusie dat 'Het risico groter is' denkt u na over maatregelen om het risico weer te verlagen.
2 In alle gevallen: leg een moment vast waarop u opnieuw deze vragenlijst bekijkt.
3 Tot slot maakt u een rapport, zoals beschreven bij punt 3

Let op: de vragenlijst is geschikt om risico's op te sporen die veroorzaakt worden door een verandering (project). Met de vragenlijst ontdekt u geen risico's gerelateerd aan de bestaande situatie.