Inhoudsopgave

1 Beschrijving van het instrument PIA

1.1 Wat is een PIA?

Een PIA (Privacy Impact Assessment), ook wel DPIA (Data protection Impact Assessment) en als tool ook wel PIA-Light genoemd, legt in de eerste plaats de risico's bloot van projecten en processen die te maken hebben met privacy en dragen bij aan het vermijden of verminderen van deze privacy risico's. Op basis van de antwoorden van de PIA wordt op systematische wijze inzichtelijk gemaakt of er een kans is dat de privacy van betrokkene wordt geschaad, hoe hoog deze is en op welke gebieden dit is.

De PIA doet dit door op gestructureerde wijze

- de kenmerken van de voorgenomen verwerking in kaart te brengen;
- de mogelijk (negatieve) gevolgen van het gebruik van persoonsgegevens voor de betrokken personen en organisaties inzichtelijk te maken;
- maatregelen te benoemen die, bij uitvoering, de risico's voor de betrokken personen en organisaties zo veel mogelijk te beperken.

Op basis van de uitkomsten van de PIA kun je gericht acties ondernemen om deze risico's te verminderen. Door het gebruik van de PIA kan bescherming van persoonsgegevens op een gestructureerde manier onderdeel uitmaken van de belangenafweging en besluitvorming over een project.

In deze toelichting en in het spraakgebruik worden de begrippen PIA, DPIA en PIA-Light door elkaar gebruik. Een zuivere benadering is dat de PIA/DPIA het proces is en de PIA-Light deze tool/dit formulier is wat hiervoor wordt gebruikt. In essentie gaat het dus telkens over hetzelfde.

1.2 Wat levert een PIA op

Het belangrijkste doel van een PIA is het voorkomen van kostbare aanpassingen in processen, herontwerp van systemen of stopzetten van een project door vroegtijdig inzicht in de belangrijkste privacyrisico's. Daarnaast kunnen nog de volgende doelen worden onderscheiden:

1. Het verminderen van de gevolgen van toezicht en handhaving
2. Het verbeteren van de kwaliteit van de gegevens
3. Het verbeteren van de dienstverlening
4. Het verbeteren van de besluitvorming
5. Het verhogen van het privacy bewustzijn binnen een organisatie
6. Het verbeteren van de haalbaarheid van een project/verandering
7. Het verstevigen van het vertrouwen van cliënten, patiënten medewerkers en toezichthouders in de wijze waarop persoonsgegevens worden verwerkt en privacy wordt gerespecteerd
8. Het verbeteren van de communicatie over privacy en de bescherming van persoonsgegevens

1.3 Wanneer is een PIA noodzakelijk of verplicht?

Een PIA-light wordt uitgevoerd bij elke wijziging in een proces of een systeem waarbij persoonsgegevens worden verwerkt of een wijziging van de omvang of de detaillering van een bestaande verwerking . Een PIA is in ieder geval verplicht bij:

- Grootschalige verwerking van bijzondere gegevens

- Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die gebaseerd is op geautomatiseerde verwerking (bijvoorbeeld profiling) en daarop gebaseerde beslissingen die die personen raken
- Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

Maar ook gekoppelde databases met informatie over kwetsbare groepen personen kan bijvoorbeeld aanleiding zijn voor het doen van een PIA.

1.4 Wanneer wordt een PIA uitgevoerd

Een PIA kan het beste in een zeer vroeg stadium van een project uitgevoerd worden. Immers, als je de PIA in een vroeg stadium uitvoert, helpt de PIA je om het privacybelang mee te nemen bij het verdere ontwerp van het project. Het is vroeg in het traject (bijvoorbeeld de ontwerpfase) vaak nog makkelijk om wijzigingen door te voeren en bijvoorbeeld aan je leverancier specifieke features te vragen, die later wellicht lastig in te bouwen zijn. Op deze manier geef je relatief eenvoudig invulling aan de wettelijk vereiste principes van privacy by design en default. Ook aanpassingen of wijzigingen van bestaande systemen of projecten rechtvaardigen een PIA. Op die manier kun je voorkomen dat latere kostbare aanpassingen nodig zijn om alsnog de noodzakelijke beheersmaatregelen met betrekking tot privacy te implementeren. Ook wanneer de omstandigheden van een project tijdens de looptijd veranderen, is het raadzaam de PIA te herhalen en/of te evalueren bij de afsluiting van een project

1.5 Hoeveel tijd kost het om een PIA uit te voeren

Er zijn verschillende factoren van invloed op de tijd die het kost om een PIA uit te voeren de belangrijkste zijn:

- Het aantal belanghebbende bij het project en de mate waarin deze vragen of twijfels hebben over de consequenties voor privacy
- De impact en het belang van het project op de organisatie en de samenleving
- De (technische en organisatorische) complexiteit van de verwerking

Tijdsinvestering kan variëren van ’n uurtje voor een bekende verwerking of een verwerking waarvoor al eerder een PIA is gedaan, tot een aantal uren, verdeeld over meerdere sessies.

1.6 Succesfactoren

Hierna zijn een aantal factoren opgenomen die bij kunnen dragen aan een succesvolle uitvoering van de PIA:

- PIA is een integraal onderdeel van de risicomanagementstrategie en/of PIA heeft een plek in de projectmethodiek, de PIA is geïntegreerd in processen (de PIA is geen ad hoc/toevallige activiteit en geen add-on).
- PIA wordt zo vroeg mogelijk in het project opgestart en uitgevoerd (in plaats van ‘als mosterd na de maaltijd’).
- Tijdens de PIA worden de relevante interne en externe belanghebbenden betrokken (in plaats van alleen de PIA teamleden).
- PIA’s zijn toekomstgericht om er zo aan bij te dragen dat privacy risico’s worden geïdentificeerd voordat systemen in gebruik worden genomen en programma’s worden geïmplementeerd.

- De PIA wordt gedurende het project (in ieder geval als de privacy impact dan wel privacy risico's wijzigen) geactualiseerd (het PIA rapport is dus een dynamisch document in plaats van een statisch document).
- PIA wordt bij voorkeur uitgevoerd door een team waarin verschillende expertises en vaardigheden aanwezig zijn (in plaats van door één persoon).
- PIA's zijn voorts meer effectief:
    - Als deze onderdeel uitmaken van een systeem van motivering, sancties en toetsing.
    - Als deze deel uitmaken van de project aanpak/methodiek of het kwaliteitsbewakingsproces.
    - Als de individuen die de PIA uitvoeren beschikken over kennis van het project/programma, dan wel toegang hebben tot privacy relevante expertise (privacywetgeving, informatiebeveiliging, records management en andere functionele expertise waar relevant).
    - Als ook externen die door het initiatief worden geraakt worden betrokken (gehoord, geconsulteerd).
    - Als er een (formeel dan wel informeel) proces is van externe/onafhankelijke toetsing.

1.7 Faalfactoren

Negatief geformuleerd zijn de succesfactoren tevens de faalfactoren. Hier komen drie specifieke aandachtspunten bij, namelijk:

- PIA wordt gezien als een doel op zich. PIA 's zijn alleen zinvol als deze worden beschouwd als een middel dat de potentie heeft om een voorstel/initiatief te veranderen als dat nodig is om privacy risico's te vermijden of verminderen. Als deze worden uitgevoerd als een voorgeschreven oefening met het doel om te voldoen aan een interne verplichting of een bureaucratische eis, dan worden deze beschouwd als een manier om te legitimeren in plaats van een risicoanalyse en gaat de toegevoegde waarde verloren.
- PIA wordt gezien als het noodzakelijk middel om privacy compliance tot stand te brengen. Het uitvoeren van een PIA is weliswaar een goede manier om de privacy risico's in kaart te brengen, privacy compliance komt echter pas tot stand als de aanbevelingen uit een PIA worden opgevolgd en er een volledige implementatie heeft plaatsgevonden van de noodzakelijke maatregelen om voortdurend aan de privacywet- en regelgeving te voldoen.
- Te veel fixatie op de uitkomst. Het uitvoeren van een goede PIA is geen 'rechttoe rechtaan' proces. Het proces waarin het rapport tot stand komt is minstens zo belangrijk als het resultaat ervan. Als het proces te snel of onzorgvuldig wordt uitgevoerd, bestaat het gevaar dat relevante privacy risico's en daarmee samenhangende oplossingsrichtingen niet goed worden doordacht.

2 Bijlage: begrippen

Betrokkene	Degene op wie een persoonsgegeven betrekking heeft
Verwerker	Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen
Compliance	Voldoen aan wet en regelgeving
Compliance check	Beoordeling of voldaan wordt aan wet en regelgeving
OECD data protection Principles	1. Limitering van het verzamelen van gegevens 2. Gegevenskwaliteit 3. Doelbinding 4. Limitering van het gebruik van gegevens 5. Beveiliging van gegevens 6. Transparantie 7. Rechten van betrokkenen 8. Verantwoording
Persoonsgegevens	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon
Privacy Dimensies	1. Lichamelijke privacy Grondwet artikel 11: Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op onaantastbaarheid van zijn lichaam 2. Ruimtelijke privacy Grondwet artikel 12: • Het binnentreden in een woning tegen de wil van de bewoner is alleen geoorloofd in gevallen bij of krachtens de wet bepaald, door hen die daartoe bij of krachtens de wet zijn aangewezen • Voor het binnentreden overeenkomstig voorgaande lid zijn voorafgaande legitimatie en mededeling van het doel van binnentreden vereist, behoudens bij wet gestelde uitzondering • Aan de bewoners wordt een schriftelijk verslag van het binnentreden verstrekt. 3. Relationele privacy Grondwet artikel 13 • Het briefgeheim is onschendbaar, behalve in de gevallen bij de wet bepaald, op last van de rechter • Het telefoon en telegraafgeheim is onschendbaar, behalve in de gevallen bij de wet bepaald door of met machtiging van hen die daartoe bij de wet zijn aangewezen 4. Informationele privacy Grondwet artikel 10 • Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer

	• De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens • De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens
Privacyrisico:	Het risico dat gepaard gaat met een bedreiging. Het privacy risico is de kans van optreden van een bedreiging dat de privacy van een betrokkene wordt geschonden maal de impact die de bedreiging heeft op de betrokkene en de organisatie.
Verwerken	Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm ter beschikkingstelling, samenbrengen met elkaar in verband brengen, alsmede het afschermen uitwisselen of vernietigen van gegevens
Verantwoordelijke	De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt

3 Bijlage: Modeldocument PIA-light

Voor verwerking (vul in) is deze PIA-light uitgevoerd op dag maand jaar (vul in).
De benoemde maatregelen worden waar mogelijk tijdens het project in uitvoering genomen. Daarnaast is het zeer belangrijk dat deze PIA periodiek (PDCA) tijdens het gebruik van de verwerking wordt geactualiseerd (tijdens de jaarlijkse leveranciersbeoordeling en indien nodig vaker).

Elke verwerking en/of voorgenomen verwerking van persoonsgegevens dient volledig te voldoen aan het gestelde in de AVG. Deze beschrijving/risico-inventarisatie (PIA) sluit ook aan bij de opzet van het register van verwerkingen en dient op grond van de Verordening ten minste het volgende te bevatten:

- een systematische beschrijving van de beoogde verwerkingen, de verwerkingsdoeleinden en de grondslag(en) waarop de verwerking plaatsvindt/vinden;
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
- de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan de Verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

Uiteraard hoeft niet alles in een keer en kan met onderstaande handreiking in meerdere stappen tot het gewenste resultaat gekomen worden: (stap 1) beschrijven verwerkingen, (stap 2) benoemen risico's per verwerking en (stap 3) beschrijven maatregelen.

Nr.	Onderdeel/item	Toelichting	STAP 1: Beschrijving van de verwerking	STAP 2: Risico, kans, impact	STAP 3: Maatregelen
			Beschrijf de gevraagde kenmerken van de voorliggende of voorgenomen verwerking. Geef de verwerking waar nodig ook een voor de hand liggende naam (vaak applicatienaam)	*Wat is onvolledig, wat kan misgaan, wat kan beschikbaarheid, continuïteit, kwaliteit, juistheid, volledigheid, vertrouwelijkheid van de verwerking beïnvloeden etc. etc.*	*Wat kun je doen om de risico's te beperken (stoppen met verwerking, verzekeren of uitbesteden zijn ook opties!)*
1.	**Formuleer het doel van de verwerking: waarom wil je dit gaan verzamelen, verwerken en wat wil je ermee bereiken.**	*Niet alleen relevant om vooraf eens goed na te denken en te beoordelen wat je wilt bereiken, maar ook om te toetsen of een eventuele uitbreiding van bestaande functionaliteit nog onder het oorspronkelijke doel valt. Daarnaast is het doel van de verwerking ook de toets verderop voor proportionaliteit (hoeveelheid gegevens en*			

		passend bij het doel) en subsidiariteit (kan het ook anders?), passende beveiliging etc.			
2.	**Wordt de verwerking van persoonsgegevens voor een samenhangend doel verwerkt? Zijn er verbanden met andere verwerkingen? Is er sprake van uitbreiding of hergebruik van een bestaande verwerking voor iets anders?**	*Doelbinding is dat persoonsgegevens niet verder worden verwerkt dan voor het doel waarvoor zij zijn verkregen. Een verdere of uitgebreide verwerking is alleen toegestaan indien deze verenigbaar is met het oorspronkelijk doel waarvoor de persoonsgegevens zijn verkregen. Slechts in uitzonderingsgevallen kan van het principe van een verenigbare verdere verwerking van persoonsgegevens worden afgeweken. Fraudebestrijding en/of afhandeling van stafbare feiten valt onder deze uitzondering.*			
3.	**Toets de grondslag: is er een wettelijke basis die je het recht geeft om persoonsgegevens te verwerken/verzamelen?**	*Verwerken mag alleen op één van de 6 grondslagen die in de AVG zijn genoemd. Een van deze bepalingen geeft je het recht om deze gegevens te verwerken[1]. Toestemming als grondslag moet je proberen te vermijden en alleen maar gebruiken als het echt niet onder een van de andere te passen is, toestemming kan immers altijd ingetrokken worden en dan heb je een uitdaging.*			
4.	**Welke persoonsgegevens worden er verwerkt/zijn er voornemens verwerkt te worden? Let hierbij ook op of er bijzondere persoonsgegevens[2], strafrechtelijke gegevens en/of gevoelige persoonsgegevens (financiële data of locatiegegevens) verwerkt worden of gaan worden?**	*Aan de hand van het doel van de verwerking wordt de toets op subsidiariteit en proportionaliteit gedaan: wat heb je echt aan persoonsgegevens nodig? Voor deze afweging moeten alle relevante factoren worden meegenomen: niet alleen hoeveelheid gegevens, maar ook wijze van verkrijging, verwerking, kans of fouten en datakwaliteit, risico's voor misbruik en mogelijkheden voor controle etc. Voor de verwerking van bijzondere persoonsgegevens geldt een strenger regime. Het uitgangspunt is dat het niet is toegestaan deze bijzondere gegevens te verwerken, tenzij dit door de wet (AVG-UAVG) wordt toegestaan.*			

[1] De 6 (rechts)grondslagen zijn niet cumulatief, er is ook geen hiërarchische volgorde. Slechts 1 hoeft van toepassing te zijn.

a. De betrokkene heeft toestemming gegeven voor de verwerking voor een of meerdere doeleinden
b. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene tot sluiting van de overeenkomst te komen.
c. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke ligt (bv. wettelijke plicht werkgevers om kopie/scan ID-bewijs van personeel op te nemen in loonadministratie in navolging van de Wet op de loonbelasting).
d. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen.
e. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.
f. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, m.n. wanneer de betrokkene een kind is.
Als de verwerking voldoet aan een van de grondslagen b t/m f genoemde doelen, dan is toestemming van de betrokkene niet nodig. Bij twijfel, heroverweging verwerking.

[2] De AVG ziet deze persoonsgegevens als bijzondere persoonsgegevens:

- Persoonsgegevens waaruit ras of etnische afkomst blijkt;

5.	**Met wie worden deze persoonsgegevens uitgewisseld?**	*Veel van de gegevens die een organisatie verwerkt worden ergens in een zorgketen gedeeld of moeten op grond van wettelijke plichten uitgewisseld of gedeeld worden. De uitwisseling met deze partijen heeft niet alleen een technische component die beschreven/beoordeeld moet worden (welk middel, welk formaat, welke beveiliging, welke encryptie etc.) maar zeker zo belangrijk een "proportionaliteit" component (heb je alles wel nodig wat je vraagt of waartoe je bevoegdheid hebt om te vragen, bijvoorbeeld gemeentes onder WMO of Jeugdwet). Op zijn minst moeten partijen in kaart zijn met wie uitgewisseld wordt/gaat worden.*			
6.	**Op welke wijze zijn de persoonsgegevens beveiligd en waar is dat terug te vinden?**	*De verantwoordelijke moet zorgen voor passende technische en organisatorische beveiligingsmaatregelen om hiermee de persoonsgegevens te beschermen tegen verlies of enige andere vorm van onrechtmatige verwerking. De te nemen beveiligingsmaatregelen dienen in principe op basis van een risicoanalyse vooraf tot stand te komen: (D)PIA. Dit ziet minimaal op autorisaties, rechten, geheimhoudingsplichten en vertrouwelijkheidsafspraken, technische beveiliging (binnen de organisatie en tijdens uitwisseling met derden) bij import/export, maatregelen om juistheid van gegevens te borgen/controleren etc. Deze maatregelen moeten beschreven, helder en controleerbaar zijn. Goede gewoonte is (onderdelen van) de beveiliging periodiek door bijvoorbeeld auditoren of accountants mee te laten testen/beoordelen.*			
7.	**Is, waar nodig, een verwerkersovereenkomst afgesloten.**	*Een verwerker is een partij die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. Indien er een verwerker voor de verwerking van persoonsgegevens is ingeschakeld, dienen afspraken hierover te worden vastgelegd in een verwerkersovereenkomst. Deze afspraken zijn beschikbaar in een model-verwerkersovereenkomst.*			
8.	**Wat is de bewaartermijn voor de verwerking van persoonsgegevens?**	*Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk is voor het doel waarvoor ze worden verwerkt. In een aantal gevallen zijn er duidelijke wettelijke bewaartermijnen. Wanneer die er niet zijn, gaat het om een valide*			

- Persoonsgegevens waaruit politieke opvattingen blijken;
- Persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken;
- Persoonsgegevens waaruit het lidmaatschap van een vakvereniging blijkt;
- Gegevens over gezondheid;
- Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid;
- Genetische gegevens;
- Biometrische gegevens met het oog op de unieke identificatie van een persoon.

		beargumentering waarom een bepaalde bewaartermijn - gelet op het doel van de verwerking - noodzakelijk is en/of onder welke omstandigheden hiervan afgeweken kan worden (bijvoorbeeld bij incidenten en/of lopende rechtszaken).			
9.	**Hoe wordt voldaan aan de informatieplichten over de verwerking voor verantwoordelijke en de rechten van betrokkene?**	*Het is verplicht om betrokkenen te informeren over wie, wat, waar, waarom etc. en de mogelijkheden voor inzage, correctie, wijziging en bezwaar helder aan te geven. Per verwerking dus voorbereiden op berichtgeving naar betrokkenen, maar ook voorbereiden op het ontvangen van reacties van betrokkenen.* *Benoem dus per verwerking bijvoorbeeld een inhoudelijk aanspreekpunt (voor aanpassingen, opvragen, inzage, kwaliteit) en een technisch aanspreekpunt. De beschrijving die met dit overzicht van een verwerking wordt gemaakt is de informatie-set die je aan een betrokkenen moet kunnen verschaffen volgens de AVG.*			
10.	**Valt de hierboven beschreven verwerking of het voornemen mogelijk onder bijzondere bevoegdheden van de OR of van de cliëntenraad?**	*Het is geen een eis vanuit AVG maar wel best-practice dat ook interne afstemming/toestemming bij een aantal verwerkingen meerwaarde heeft. Systemen/verwerkingen/verzamelingen dienen, alvorens tot start wordt overgegaan, vooraf aan de OR en/of cliëntenraad te worden aangeboden (ter instemming, advies, informatie of gewoon informele informatie en betrokkenheid).*			