DPIA-CHECKLIST

Deze DPIA-checklist is een handreiking voor organisaties die de DPIA uitvoeren volgens het model van M&I/Partners. Bij het gebruik van dit model wordt een systematische beschrijving van de (meta)verwerking gemaakt en een risicoanalyse uitgevoerd. De uitkomsten van de risicoanalyse worden aangevuld met maatregelen. De implementatie van maatregelen wordt ingepland om de risico's op de bescherming van persoonsgegevens in een gecontroleerd proces te mitigeren.

Deze checklist bestaat uit twee onderdelen:
Voorbereidende vragen om te controleren of alles aanwezig is om de DPIA op te starten.
Vragen voor de verschillende rollen die betrokken zijn bij de DPIA.

Voor ieder van deze onderdelen zijn (controle-)vragen opgesteld die helpen bij de uitvoering van de DPIA. Niet iedere vraag uit dit document hoeft beantwoord te worden. Wanneer een vraag vereist is, geven we dat aan met een asterisk (*).

Indien op deze verwerking al eerder een DPIA verricht is, neem het rapport van de eerdere DPIA dan als basis en richt je op de afwijkingen.

INTERVIEWVRAGEN

Deze vragen geven houvast bij uitvoering van interviews en helpen bij het uitvoeren van documentatieonderzoek. Mogelijk krijg je tijdens deze interviews al zaken te horen die klinken als een risico. Hou deze potentiële risico's tijdens de interviews alvast bij in een 'kladblok', hier kun je later op terugvallen bij de risicoanalyse. Boven de vragen staan kopjes; deze corresponderen met de kopjes in het eindverslag. Zo kun je makkelijk de juiste informatie op de juiste plek zetten.

Voorbereiding

- Wat is de scope van de verwerking waarop de DPIA uitgevoerd gaat worden? *
  - Welke processen/subprocessen vallen hieronder?
  - Welke processen/subprocessen vallen buiten scope?
    - Moet op dit deel alsnog een DPIA uitgevoerd worden? Borg dit bij de procesverantwoordelijke.
- Is een DPIA vereist? Stel dit vast middels het uitvoeren van een preDPIA (zie het document preDPIA). *
- Is er documentatie beschikbaar voor deze verwerking? *
  - Is er beleid?
  - Zijn procesbeschrijvingen, protocollen, procedures, werkinstructies aanwezig?
  - Is er een functioneel / technisch ontwerp van de applicaties die ingezet worden beschikbaar?
  - Is er een verwerkingsregister aanwezig? Indien ja, bevat het verwerkingsregister:
    - Welke persoonsgegevens er worden verwerkt?
    - Welke categorieën van betrokkenen er zijn (inclusief informatieplicht)?
    - Wat de grondslag(en) is/zijn van de verwerking?
    - Een omschrijving van de verantwoordelijkheden?
    - Welke verwerkers er betrokken zijn, en of er overeenkomsten zijn gesloten met deze verwerkers?
    - Wat de bewaartermijnen van de persoonsgegevens zijn?
- Welke medewerkers zijn nodig voor de uitvoering van de DPIA?
  - Wie is verantwoordelijk voor de verwerking? *
    - Wie is er verantwoordelijk voor het vaststellen van de risico's en maatregelen (proceseigenaar)? *
  - Zijn alle vereiste medewerkers beschikbaar? *
    - Wie ga je betrekken in de uitvoering van de DPIA?
    - Wie gaat de DPIA trekken?
- Identificeer alle belangrijke stakeholders en informeer hen dat de DPIA gaat starten, o.a.: *
  - Functionaris Gegevensbescherming
  - CISO
  - Intern verantwoordelijke/proceseigenaar

Naar de interviewvragen

Met de proceseigenaar stem je af vóórdat de DPIA begint. Je legt diegene het verloop van de DPIA uit en blikt vooruit naar het einde van het proces, waarin er risico's en maatregelen geformuleerd zijn. Zorg dat de proceseigenaar ervan op de hoogte is dat er risico's en maatregelen zullen volgen en dat de proceseigenaar hier de verantwoordelijke voor is.

Proces-eigenaar | Vakinhoudelijk medewerker | Applicatie-beheerder | CISO | Juridische zaken | Projectleider | Privacy officer

Beschrijving

- Hoe worden persoonsgegevens verkregen? (handmatig, automatisch, direct van betrokkene, etc.). De wijze van verkrijgen van gegevens bepaalt mede welke rechten wel en niet van toepassing zijn. *

Beoordeling

- Hanteren en naleven van bewaartermijnen:
    - Is er een intern archiverings- / bewaarbeleid aanwezig? (Neem op als bijlage.)
    - Is er getoetst of bewaartermijnen van toepassing zijn op de systemen/applicaties/gegevens? *
    - Kunnen gegevens uit uw systemen/applicaties worden verwijderd? *
- Word ik als betrokkene geïnformeerd over de verwerking? *
    - Staat er een privacyverklaring op de website?
    - Informeren jullie de klant via andere kanalen proactief over de verwerking?
    - Is bij het opstellen van informatiemateriaal rekening gehouden met het kennisniveau van de lezer?
- Kan ik me als betrokkene beroepen op mijn rechten? *
- Hoe word ik als betrokkene geïnformeerd over mijn rechten? *
- Kunnen jullie binnen de termijn van 4 weken redelijkerwijs volledig voldoen aan mijn verzoek?
- Welke middelen hebben jullie aan betrokkenen beschikbaar gesteld om zelfstandig zijn / haar rechten uit te oefenen (denk hierbij aan portaal voor inzage, aanvulling of verwijdering)?
- Is er een loketfunctie ingericht (intern of extern, inclusief incident-/klachtenmanagement)?
- Is voor betrokkenen te vinden waar zij terecht kunnen met vragen, opmerkingen en klachten?
    - Dit geldt ook voor medewerkers: indien hun persoonsgegevens worden verwerkt, zijn zij ook betrokkenen.

Risicoanalyse

- Training / bewustwording medewerker (specifiek: directie en management awareness):
    - Is Informatiebeveiliging & Privacy (IB&P) een onderdeel van het inwerkprogramma voor nieuwe medewerkers?
    - Worden er op verschillende kwaliteitsdomeinen structureel (verplichte?) trainingen gegeven aan medewerkers?
    - Wat zijn de meeste recente (afgelopen jaar) initiatieven op het gebied van IB&P awareness?
- Worden er gegevens van kwetsbare doelgroepen verwerkt? Zijn hier extra maatregelen op getroffen?
    - Worden gegevens van jeugdigen (<16 jaar) verwerkt?
    - Worden gegevens van andere kwetsbare doelgroepen verwerkt? (bijv. sprake van machtsverhouding of mensen met een beperking).
- Wie heeft overzicht over de informatie die gedeeld wordt (al dan niet automatisch)?
- Is het afsluiten van verwerkersovereenkomsten (incl. de voorafgaande beoordeling van noodzaak voor een VWO) onderdeel van het inkoopproces? *
    - Is er een verwerkersovereenkomst afgesloten (indien nodig)? *
    - Is door de organisatie een lijst van algemene eisen opgesteld waaraan leveranciers dienen te voldoen (AIV ICT?)? (Neem op in de bijlage.) *
    - Worden leveranciers periodiek gecontroleerd op het voldoen aan informatiebeveiligingsstandaarden? *
- Procesmatig werken:
    - Zijn er procesbeschrijvingen beschikbaar voor de processen?
    - Wordt er conform deze processen gewerkt? Hoe wordt dit gecontroleerd/gemonitord? *
    - Hoe worden processen verbeterd?

De vakinhoudelijk medewerker of de medewerker primair proces is een medewerker die (een deel van het proces) door en door kent. Vaak heb je voldoende aan één tot drie medewerkers om de verschillende stappen van de verwerking in kaart te brengen. Het kan echter nuttig zijn om meerdere medewerkers omtrent dezelfde deelprocessen te interviewen, om een zo volledig mogelijk beeld te krijgen van de praktijk.

Proces-eigenaar | Vakinhoudelijk medewerker | Applicatie-beheerder | CISO | Juridische zaken | Projectleider | Privacy officer

Beschrijving

- Hoe worden persoonsgegevens verkregen (handmatig, automatisch, direct van betrokkene, etc.)? De wijze van verkrijgen van gegevens bepaalt mede welke rechten wel en niet van toepassing zijn. *

Beoordeling

- Dataminimalisatie (welke gegevens verwerk je, heb je ze allemaal nodig)
    - Noodzakelijkheid: zijn deze gegevens noodzakelijk voor het doel waarvoor deze verwerkt worden? *
    - Proportionaliteit: is de inbreuk op de privacy van betrokkene die wordt gemaakt proportioneel ten opzichte van het doel dat wordt nagestreefd? *
    - Subsidiariteit: zou je het beoogde doel met minder of minder ingrijpende persoonsgegevens kunnen bereiken? *
    - Is voor iedere verwerking van persoonsgegevens beoordeeld of de verwerkte gegevens daadwerkelijk noodzakelijk zijn (kan het ook met minder)? *

Risicoanalyse

- Training / bewustwording medewerker (specifiek: directie en management awareness):
    - Is Informatiebeveiliging & Privacy (IB&P) een onderdeel van het inwerkprogramma voor nieuwe medewerkers?
    - Worden er op verschillende kwaliteitsdomeinen structureel (verplichte?) trainingen gegeven aan medewerkers?
    - Wat zijn de meeste recente (afgelopen jaar) initiatieven op het gebied van IB&P awareness?
- Worden er gegevens van kwetsbare doelgroepen verwerkt? Zijn hier extra maatregelen op getroffen?
    - Worden gegevens van jeugdigen (<16 jaar) verwerkt?
    - Worden gegevens van andere kwetsbare doelgroepen verwerkt? (bijv. sprake van machtsverhouding of mensen met een beperking)?
- Delen van informatie (grootschalig / portalen / veilige mail):
    - Worden gegevens (op grote schaal) gedeeld buiten de organisatie? *
    - Welke periodieke aanleveringen met persoonsgegevens doe je als organisatie?
- Procesmatig werken:
    - Zijn er procesbeschrijvingen beschikbaar voor de processen.
    - Wordt er conform deze processen gewerkt? Hoe wordt dit gecontroleerd/gemonitord? *
    - Hoe worden processen verbeterd?

De applicatiebeheerder voert het functioneel beheer uit van de belangrijkste applicatie(s) die worden gebruikt voor de verwerking waar je de DPIA op doet. Vaak werkt de applicatiebeheerder ook aan de verdere inrichting en ontwikkeling van de applicatie. Soms werkt die zelf mee in het proces, maar vaker doet de applicatiebeheerder enkel het applicatiebeheer en is die niet inhoudelijk bij het proces betrokken.

Risicoanalyse

- Is er een OTAP-omgeving (nodig) en welke gegevens worden gebruikt in ontwikkel-, test- en opleidingsomgevingen van systemen/applicaties waarin persoonsgegevens verwerkt worden?
- Vindt er adequate logging plaats op alle omgevingen? *
- Worden gegevens geautomatiseerd verwijderd? *
- Kan ik me als betrokkene beroepen op mijn rechten? *
- Toegangsbeveiliging en autorisaties:
    - Wie heeft toegang tot de persoonsgegevens (fysiek en digitaal)? *
    - Is er een autorisatiematrix?
    - Hoe is identity access management (IAM) ingericht?
    - Is er sprake van role base access control (RBAC)? *
    - Wordt er gebruik gemaakt van een Active Directory?
    - Heeft iedereen een eigen inlogcode (account/wachtwoord)? *
    - Is er een wachtwoordbeleid?
    - Hoe wordt toegang tot gerepliceerde gegevens geregeld?
    - Hoe is clear screen en clean desk beleid ingericht?
    - Worden pc's (automatisch) vergrendeld?
    - Hoe is de toegang tot de locatie geregeld?
    - Is er sprake van sleutelbeheer?
    - Hoe worden beheeraccounts en/of meestersleutels uitgegeven en beheerd?
    - Welke periodieke aanleveringen met persoonsgegevens doe je als organisatie?
    - Is er een veilige mail / veilige fileshare oplossing geïmplementeerd? *
    - Is er een intern beleid waarin de gedragsregels en kaders voor het gebruik van e-mail worden beschreven m.b.t persoonsgegevens? (Neem dit op in de bijlage.)
    - Wie heeft overzicht over de informatie die gedeeld wordt (al dan niet automatisch)?
- Logging (wat doe je, hoe doe je het, welke gegevens leg je vast en wat doe je hiermee):
    - Log je zowel create, read, update en delete (CRUD) van al je gebruikers binnen de bedrijfsapplicaties en -systemen waar persoonsgegevens verwerkt worden? *
        - Bij een patiënten- of cliëntendossier: voldoet de logging aan de NEN7513?
    - Bij een patiënten- of cliëntendossier: is er een noodknopprocedure aanwezig en wordt het gebruik hiervan gemonitord? *
    - Worden voor medewerkers die beheeractiviteiten verrichten ook werkzaamheden buiten de applicaties gelogd?
    - Zijn alle loggingsactiviteiten met zekerheid terug te leiden naar de juiste gebruikers, welke waarborgen heb je hiervoor ingericht? *
    - Hoe is het controleproces op logging ingericht?
- Beveiliging van apparatuur (pc's, laptops, smartphones):
    - Kan iedereen onbeperkt installaties uitvoeren op laptops en pc's? *
    - Is zakelijke informatie op tablets / smartphones (privé) te benaderen? Wordt er beveiliging afgedwongen op het apparaat waarmee de informatie benaderd wordt (versleuteling)? *
    - Wordt patchmanagement (op operation system- (zoals Windows OS of iOS) en applicatielaag) toegepast en gecontroleerd? *
- Continuïteitsplan t.b.v. informatie (recovery (tests)):
    - Is er een continuïteitsplan t.b.v. informatie aanwezig? *
    - Is er een continuïteitsplan t.b.v. procesdoorgang aanwezig? *
    - Wanneer zijn de laatste recovery tests uitgevoerd voor de bedrijfskritische applicaties waarin persoonsgegevens verwerkt worden? (Neem het rapport op in de bijlage.)
    - Bij SaaS-applicaties:
        - Wie bepaalt de RPO en RTO binnen de organisatie? *

De applicatiebeheerder voert het functioneel beheer uit van de belangrijkste applicatie(s) die worden gebruikt voor de verwerking waar je de DPIA op doet. Vaak werkt de applicatiebeheerder ook aan de verdere inrichting en ontwikkeling van de applicatie. Soms werkt die zelf mee in het proces, maar vaker doet de applicatiebeheerder enkel het applicatiebeheer en is die niet inhoudelijk bij het proces betrokken.

Proces-eigenaar | Vakinhoudelijk medewerker | Applicatie-beheerder | CISO | Juridische zaken | Projectleider | Privacy officer

- Datakwaliteit / -integriteit:
    - Is er gegevensinvoervalidatie uitgevoerd op bedrijfskritische applicaties waarin persoonsgegevens verwerkt worden (bv. 11-proef op BSN-velden)?
    - Is er een afdeling datamanagement/gegevensbeheer aanwezig?
- Technische beveiliging van systemen (intern / extern (OWA / RDP / pen test etc.):
    - Voeren jullie periodiek pen-testen uit, intern en extern?
    - Doen jullie dit zelf of laat u een onafhankelijke derde dit doen?
    - Is thuiswerken voor jullie medewerkers mogelijk? *
        - Welke aanvullende maatregelen zijn getroffen voor het benaderen van informatie buiten het bedrijfsnetwerk en het voorkomen van datalekken (2FA, uitzetten van clipboard, VPN, etc.)? *
- Experimenten en innovaties (Big Data/Blockchain/AI/wordt er geknutseld?):
    - Zijn er plekken binnen de organisatie waar geëxperimenteerd wordt met nieuwe technieken (zoals.: Big Data / Blockchain)?
    - Hebben jullie een research / onderzoeksafdeling?
- Netwerkschijven (beheer):
    - Staan alle persoonsgegevens opgeslagen binnen (beheerde, voorzien van autorisaties) applicaties, of komen er ook persoonsgegevens op de netwerkschijven/lokale SharePoint? *
- Project/programmamanagement:
    - Is er een professionele project/programmamanagement structuur aanwezig binnen de organisatie.
    - Is er aandacht voor changemanagement binnen de organisatie?

De CISO, de Chief Information Security Officer, heeft een algemeen beeld over de informatiebeveiligingsrisico's en –maatregelen binnen de organisatie. Dit kan je tijdens de DPIA helpen doordat bepaalde bestaande maatregelen risico's van de verwerking kunnen beperken. Ook kan de CISO je informeren over de bestaande *risk appetite* van de organisatie. Is er geen CISO? Zoek dan naar een ISO (security officer) of informatiebeveiligingsadviseur.

Proces-eigenaar | Vakinhoudelijk medewerker | Applicatie-beheerder | CISO | Juridische zaken | Projectleider | Privacy officer

Risicoanalyse

- Is er een *risk appetite* vastgesteld?
- Governance IB&P kwaliteitscyclus, controles:
    - Is er een jaarlijkse managementrapportage over IB naar het hoogste bestuursorgaan?
    - Worden er jaarlijks interne audits uitgevoerd? (check laatste audit rapport < 1 jaar oud)
    - Is er een jaarplan IB aanwezig?
    - Is er een interne opdrachtgever / portefeuillehouder op directieniveau voor IB? *
    - Is veilig incident melden (VIM) onderdeel van de bedrijfscultuur? *
    - Hoeveel datalekken hebben jullie geregistreerd (gemeld en ongemeld) in de afgelopen 3 jaar? *
- Beleid.
    - Is er een informatiebeveiligingsbeleid beschikbaar? Is deze vastgesteld en wordt dit beheerd?

De afdeling juridische zaken kan je helpen met het 'beoordelings'-gedeelte van de DPIA, waarin je bepaalt of er sprake is van een wettelijke grondslag. Heb je geen afdeling JZ? Vaak is er een onafhankelijk juridisch adviseur die advies kan geven, of kun je terecht bij de koepelorganisatie.

Beoordeling

- Op welke grondslag(en) is de verwerking gebaseerd? *
    - Indien algemeen belang / wettelijke taak:
        - Welke wet(ten), artikel, lid?
    - Is rekening gehouden met het recht op bezwaar?
- Biedt de grondslag voldoende basis voor alle persoonsgegevens die verwerkt worden? *
    - Kijk hierbij ook naar eventuele koppelingen en verdere verwerking.
- Verstrekking aan derden: *
    - Welke grondslagen zijn van toepassing binnen deze verwerking voor bijvoorbeeld verstrekking van persoonsgegevens aan derden?
    - Zijn alle verstrekkingen aan derden in lijn met het originele doel?
        - Zo nee, beoordeel of de verstrekking rechtmatig is.
- Worden geheimhoudingsbepalingen met de verwerking doorbroken?
    - Zo ja, is daarvoor een voldoende basis?
- Welke wet- en regelgeving is (naast de AVG) van toepassing op deze verwerking?
    - Denk hierbij zowel aan wetgeving gericht op archivering, maar ook wetten die richting geven aan de uitvoering van de verwerking (o.a. WMO, Jeugdwet, Participatiewet, etc.).

DPIA’s worden vaak uitgevoerd op nieuwe verwerkingen. Bij sommige van deze nieuwe verwerkingen is een projectleider betrokken. De projectleider kan je helpen met informatie over contractmanagement. Deze projectleider heeft soms ook de rol van proceseigenaar (stel dan ook de vragen onder ‘proceseigenaar’).

Beschrijving

- Wie heeft overzicht over de informatie die gedeeld wordt (al dan niet automatisch)?

Risicoanalyse

- Leveranciersmanagement / VWO's (maatregelen op leveranciersbeveiliging):
    - Is er een (digitale) centrale plaats waar contracten beheerd worden?
    - Wie beheert de contracten? *

De privacy officer ondersteunt de organisatie met het inrichten van de organisatie conform geldende privacywet- en regelgeving. Vaak is de privacy officer de 'trekker' van de DPIA. Is dat niet het geval, zorg dan dat de privacy officer in elk geval onderstaande vragen beantwoord, zodat je een goed beeld krijgt van de privacyorganisatie.

Risicoanalyse

- Governance IB&P kwaliteitscyclus, controles:
    - Is er een jaarlijkse managementrapportage over privacy naar het hoogste bestuursorgaan?
    - Worden er jaarlijks interne audits uitgevoerd? (check laatste audit rapport < 1 jaar oud)
    - Is er een jaarplan privacy aanwezig?
    - Is er een interne opdrachtgever / portefeuillehouder op directieniveau voor privacy? *
    - Is veilig incident melden (VIM) onderdeel van de bedrijfscultuur? *
    - Hoeveel datalekken hebben jullie geregistreerd (gemeld en ongemeld) in de afgelopen 3 jaar? *
- Beleid (voor alle vragen: vaststelling en beheer).
    - Is er een privacybeleid beschikbaar?
    - Is er een privacybeleid voor medewerkers beschikbaar?