|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
| **DPIA Template**  Checklist |  |  |
|  |  |  |
| Sparrenheuvel 32, 3708 JE Zeist | (030) 2 270 500 | [info@mxi.nl](mailto:offertebureau@mxi.nl) | [www.mxi.nl](http://www.mxi.nl) | |  |  |
|  |  | Versie 1 / 1 januari 2019 |
|  |  |  |

Doel van het document

De checklist DPIA is een handreiking voor organisaties die de DPIA uitvoeren volgens het model van M&I/Partners. Volgens ons model wordt een systematische beschrijving van de (meta)verwerking gemaakt en wordt 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 volgt de stappen uit onze DPIA aanpak:

1. Voorbereiding
2. Beschrijving
3. Beoordeling
4. Risico-analyse

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 gouden asterisk (\*).

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

De hoofdstuknummers in dit document corresponderen met de hoofdstukken van het format voor de DPIA-rapportage van M&I/Partners.

1. 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? Doe hiervoor de een PreDPIA (2 PreDPIA.docx)?\*
* 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?
* Is er eerder al een DPIA uitgevoerd welke vergelijkbaar is met dit proces of waar dit proces onder valt?
* Welke medewerkers zijn nodig voor de uitvoering van de DPIA?
  + Wie is verantwoordelijk voor de verwerking? \*
  + 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

5. Beschrijving

Onderstaande 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.

Deze stap, ‘Beschrijving’ werk je uit in het document ‘7 DPIA Template Eindrapportage’ – hoofdstuk 5. Hier is met kopjes en voorbeeldtekstblokken reeds aangegeven welke informatie hier verwacht wordt.

## 5.1. Globale beschrijving

* Wat is het doel van de verwerking (SMART)?
* Is het doel van deze verwerking formeel vastgelegd (bijv. in het verwerkingsregister of in een convenant)? \*
* Wat zijn de subdoelen van de verwerking (SMART)? Subdoelen zijn onderliggend aan het hoofddoel.\*

## 5.2. Categorieën persoonsgegevens

* Welke categorieën persoonsgegevens verwerk je binnen deze verwerking? (o.b.v. je verwerkingsregister indien aanwezig, anders uitvragen d.m.v. interviews) \*
  + Beschrijf expliciet welke bijzondere gegevens verwerkt worden, zoals strafrechtelijke- of gezondheidsgegevens (artikel 9.1 AVG)
  + Benoem expliciet als burgerservicenummer wordt verwerkt.
  + Benoem expliciet of er gegevens worden verwerkt in het kader van de Wet Politiegegevens (WPG).

5.3. Uitvoering

* Wat doe je bij deze verwerking (in max 1 alinea)? \*
  + Wat is de scope van de DPIA (wat zijn de grenzen van de verwerking die je beoordeelt)? (Zie document ‘7 DPIA Template Eindrapportage’, vul eventueel aan).
  + Aanpassing van scope (bijv. wel of geen meta-verwerking) kan gedurende het opstellen van de beschrijving nog.
  + Kun je een beknopte procesbeschrijving maken (hoog over) voor deze verwerking.
* Wat is de context waarbinnen deze verwerking plaatsvindt?
* Welke verwerkingen vallen onder de verwerking die we binnen deze DPIA beoordelen? (o.b.v. je verwerkingsregister indien aanwezig.) \*
* Welke systemen worden ingezet bij de uitvoering van deze verwerking? \*
* Vindt er verwerking plaats buiten de systemen? (bijv. lokale fileshares of op papier) \*
* Op welke wijze worden gegevens verwerkt (handmatig, automatisch, zijn er koppelingen, etc.)? \*
* Welke partij is verwerkingsverantwoordelijke? \*
* Wie is intern verantwoordelijke voor de verwerking (bijv. proceseigenaar of afdelingsmanager)?
* Van hoeveel betrokkenen worden persoonsgegevens gewerkt (1, 1-10, 100-1.000, 1.000-10.000, 10.000+)?
* Wat zijn de gevolgen voor de betrokkene van deze verwerking?
  + Hierbij zowel gevolgen voor de privacy, als andere gevolgen (bijv. het ontvangen van een bepaalde voorziening).

5.4. Betrokken partijen bij de verwerking

* Beschrijf voor ieder systeem waarin persoonsgegevens verwerkt worden binnen deze verwerking\*:
  + Wat is de naam van het systeem/de applicatie?
  + Wie is de leverancier?
  + Heeft de leverancier een DPIA gedaan (zo ja, vraag verslag)?
  + Is er een verwerkersovereenkomst aanwezig? \*
    - Is deze op een standaard verwerkersovereenkomst gebaseerd?
    - Welke afwijkingen zijn aanwezig ten opzichte van de standaard verwerkersovereenkomst?
    - Tot wanneer is deze verwerkersovereenkomst geldig (vaak gelijk met contract)?
      * Check op bijzondere afspraken die ook hierna doorlopen.
  + Zijn er bijzonderheden uit andere overeenkomsten of SLA’s met verwerker die relevant zijn voor de verwerking van persoonsgegevens.?
* Zijn er naast leveranciers van systemen/applicaties nog andere leveranciers betrokken bij de verwerking (incl. subverwerkers (waar relevant)?
  + Stel voor ieder van deze leveranciers dezelfde vragen als hierboven.

5.5. Ontvangers van persoonsgegevens

* Indien relevant: hoe ziet de keten / samenwerking rondom de verwerking er uit?
* Welke interne ontvangers van persoonsgegevens zijn te onderscheiden (hanteer niveaus als: functie, rol, titel, specialisme)? \*
* Welke externe ontvangers van persoonsgegevens zijn betrokken bij de verwerking? (nb. niet verwerkers of gezamenlijk verwerkingsverantwoordelijke, enkel zelfstandig verwerkingsverantwoordelijke) \*

5.6. Systematische beschrijving

Zie voor een uitgebreidere beschrijving van het maken van een systematische beschrijving het document ‘5 DPIA gegevensstroomanalyse’.

* Stel voor ieder van de sub-doelen/sub-processen de vraag: welke gegevensstromen vinden plaats om te zorgen dat het doel bereikt wordt? \*
* Stel voor ieder van de gegevensstromen de vragen:
  + Welke persoonsgegevens worden als input aangeleverd voor de verwerkingsactiviteit? \*
  + Waar komt de input vandaan? (systemen, mensen en eventuele fysieke gegevensdragers) \*
  + Hoe wordt de input aangeleverd? (mondeling, standaard formulier, open tekstveld, e-mail, etc.) \*
  + Welke output levert de verwerking op? \*
  + Waar komt deze output terecht / waar wordt de output opgeslagen? (systemen, mensen en eventuele fysieke gegevensdragers) \*
  + Wijkt de input af van het verwerkingsregister? Beoordeel of de input of het verwerkingsregister aangepast moet worden. Idem voor output. \*
  + Komt het totaal aan persoonsgegevens dat is beschreven bij input en output overeen met het totale overzicht van persoonsgegevens?

6. Beoordeling

Nb.: Afwijkingen in dit deel van de checklist komen vaak terug als risico’s

6.1. Rechtsgrond per doel van de verwerking

* Op welke grondslag(en) is de verwerking gebaseerd? \*
  + Indien toestemming:
    - Voldoet deze aan de eisen die aan toestemming gesteld worden?
    - Is hierbij rekening gehouden met mogelijke machtsverhoudingen (bijv. werknemer-werkgever)?
    - Is rekening gehouden met de consequenties van het intrekken van toestemming?
  + Indien wettelijke verplichting:
    - Welke wet, artikel, lid? Nb. de verwerking moet noodzakelijk zijn om te voldoen aan de wettelijke verplichting.
  + Indien algemeen belang / wettelijke taak:
    - Welke wet, artikel, lid?
    - Is rekening gehouden met het recht op bezwaar?
  + Indien overeenkomst met betrokkene:
    - Welke overeenkomst, welke versie van de overeenkomst, etc?
  + Indien gerechtvaardigd belang:
    - Hoe zijn belangen afgewogen? Is dit vastgelegd? (N.b. voor overheden, zoals gemeenten, mag deze grondslag **alleen** gebruikt worden voor eigen bedrijfsvoeringstaken).
    - Beschrijf / verwijs naar belangenafweging.
    - Is rekening gehouden met bezwaar.
  + **Uitzonderlijk geval**: Indien vitaal belang:
    - Beschrijf de situatie.
* Biedt de grondslag voldoende basis voor alle persoonsgegevens die verwerkt worden? \*
  + Kijk hierbij ook naar eventuele koppelingen en verdere verwerking.
* Als er geen grondslag aanwezig is voor het verwerken van de gegevens:
  + **Staak de DPIA.**
  + Stem af met Juridische zaken/ Procesverantwoordelijke / FG over vervolgstappen.
* Zorg altijd voor een objectieve toets of de grondslag voldoende is.
* 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?
* 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. \*
* 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.).

6.2. Dataminimalisatie en bewaartermijnen

* Dataminimalisatie (welke gegevens verwerk je, heb je ze allemaal nodig)?
  + Noodzakelijkheid: zijn deze gegevens noodzakelijk voor het doel waarvoor deze verwerkt worden?\*
    - Wie hebben er toegang tot de gegevens? Is dit noodzakelijk voor de uitvoer van hun taken? \*
  + 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)? \*
  + Is er een OTAP-omgeving (nodig) en welke gegevens worden gebruikt in ontwikkel-, test- en opleidingsomgevingen van systemen/applicaties waarin persoonsgegevens verwerkt worden?
    - Indien persoonsgegevens: Vindt er adequate (zie boven) logging plaats op alle omgevingen?\*
* Hanteren en naleven van bewaartermijnen:
  + Is er een intern archiverings- / bewaarbeleid aanwezig? (bijlage uploaden)
  + Is er een getoetst of bewaartermijnen van toepassing zijn op de huidige systemen/applicaties/gegevens? \*
  + Kunnen gegevens uit uw systemen/applicaties worden verwijderd? \*
* Worden gegevens geautomatiseerd verwijderd?

6.3. Waarborgen voor rechten van betrokkenen

* Word ik als betrokkene geïnformeerd over de verwerking? \*
  + Staat er een privacyverklaring op de website?
  + Informeert u 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 betrokkene.

7.1 Checklist (risico)analyse

* 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?
* Toegangsbeveiliging en autorisaties:
  + Wie heeft toegang tot de persoonsgegevens (fysiek en digitaal)? \*
  + Is er een autorisatiematrix? \*
    - Hoe is identity access management 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?
* Worden er gegevens van kwetsbare doelgroepen verwerkt? \* Zijn hier extra maatregelen op getroffen?
  + Worden gegevens van jeugdigen <16 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?
  + 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? (bijlage uploaden)
  + Wie heeft overzicht over de informatie die gedeeld wordt (al dan niet automatisch)?
* Leveranciersmanagement / VWO's (maatregelen op leveranciersbeveiliging)
  + Is er een (digitale) centrale plaats waar contracten beheerd worden?
  + Wie beheert de contracten? \*
  + 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?)? (bijlage uploaden) \*
  + Worden leveranciers periodiek gecontroleerd op het voldoen aan informatiebeveiligingsstandaarden? \*
* 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 van al je gebruikers binnen de bedrijfsapplicaties en -systemen waar persoonsgegevens verwerkt worden? \*
  + 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? \*
* Governance IB&P kwaliteitscyclus, controles:
  + Is er een jaarlijkse managementrapportage over IB&P naar het hoogste bestuursorgaan?
  + Worden er jaarlijks interne audits uitgevoerd? (check laatste audit rapport < 1 jaar oud)
  + Is er een jaarplan IB&P aanwezig?
  + Is er een interne opdrachtgever / portefeuillehouder op directieniveau voor IB&P? \*
  + Is veilig incident melden (VIM) onderdeel van de bedrijfscultuur? \*
  + Hoeveel datalekken hebben jullie geregistreerd (gemeld en ongemeld) in de afgelopen 3 jaar? \*
* 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 (bijv.: pincode / vingerafdruk / versleuteling)? \*.
  + Wordt patchmanagement (op windows- en applicatielaag) toegepast en gecontroleerd? \*
* Continuïteitsplan tbv 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? (rapport uploaden)
    - Specifiek aandachtspunt voor SaaS-applicaties.
  + Wie bepaalt de RPO en RTO binnen de organisatie? \*
* 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.).
  + Voert u periodiek pen-testen uit, intern en extern?
    - Doet u dit zelf of laat u een onafhankelijke derde dit doen?
  + Is thuiswerken voor uw 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)?
  + Heeft u 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 uw organisatie?
* Beleid (voor alle vragen: vaststelling en beheer):
  + Is er een privacybeleid beschikbaar?
  + Is er een privacybeleid voor medewerkers beschikbaar?
  + Is er een informatiebeveiligingsbeleid beschikbaar?
* Procesmatig werken:
  + Zijn er procesbeschrijvingen beschikbaar voor de processen?
  + Wordt er conform deze processen gewerkt? Hoe wordt dit gecontroleerd/gemonitord? \*
  + Hoe worden processen verbeterd?