Samen aanjagen van vernieuwing

Uitvoeren van een DPIA: hoe doe je dat?

Handreiking

Auteur(s): ICTRecht
Versie: 1.0
Datum: 7 januari 2025

Inhoudsopgave

Het uitvoeren van een DPIA: hoe doe je dat?

Deze handreiking voor het uitvoeren van een DPIA is voor het laatst aangepast op 07 januari 2025 en is opgesteld door ICTRecht in opdracht van MBO Digitaal. Deze handreiking DPIA is toepasbaar voor alle bij SURF aangesloten (onderwijs-)instellingen.

1 Inleiding

Ga je als instelling met een nieuw ICT-systeem werken of op een nieuwe manier werken met persoonsgegevens, zoals de gegevens van medewerkers of studenten? Dan ben je in sommige gevallen verplicht om een Data Protection Impact Assessment (DPIA) uit te (laten) voeren. Een DPIA is alleen verplicht als er een verwerking gaat plaatsvinden die mogelijk een hoog risico met zich meebrengt. Hiervoor zijn criteria opgesteld in de Algemene verordening gegevensbescherming (AVG) en aanvullend door de Autoriteit Persoonsgegevens en EU-privacy toezichthouders.

In dit document tref je handvatten en hulpvragen aan voor het uitvoeren van een DPIA volgens het 'DPIA-model van het Rijk[1]'. Daartoe wordt per onderdeel uit het Rijksmodel een aantal aandachtspunten en hulpvragen weergegeven. In de bijlagen zijn een pre-DPIA checklist en een DPIA-vragenlijst opgenomen die je kunt gebruiken als je een DPIA uit gaat voeren.

[1] https://www.kcbr.nl/sites/default/files/2023-09/Model%20DPIA%20Rijksdienst%20v3.0.pdf

2 Handreiking uitvoeren DPIA

In dit hoofdstuk zijn de handvatten en hulpvragen beschreven die kunnen helpen bij het uitvoeren van een DPIA.

2.1 Voorstel schrijven

'Beschrijf het voorstel waar de DPIA op toeziet op hoofdlijnen en benoem hoe het voorstel tot stand is gekomen en wat de beweegredenen zijn achter de totstandkoming van het voorstel.'

Om het bovenstaande uit te werken kan je de volgende hulpvragen en aandachtspunten gebruiken:

Het voorstel op hoofdlijnen

- Binnen welk project, welk proces of binnen welke applicatie zullen de verwerkingen van persoonsgegevens plaatsvinden?
- Wat zijn de belangrijkste kenmerken van het project, het proces of de applicatie? Denk hierbij aan de kernfunctionaliteiten van een applicatie, de datastroom/stroomschema op hoofdlijnen en de verschillende fasen voor een proces, of de onderdelen van een project waarbij persoonsgegevens gebruikt zullen worden.
- Indien een projectplan of een vergelijkbaar document aanwezig is, vat dan de belangrijkste onderdelen van dit document samen.
- Welke andere organisaties zijn betrokken bij het voorstel?

De wijze waarop het voorstel tot stand is gekomen

- Beschrijf de concrete aanleiding voor het voorstel. Heeft er bijvoorbeeld een beleidswijziging plaatsgevonden, is er nieuwe wetgeving waaraan voldaan moet worden, zijn er nieuwe efficiency-doelstellingen en/of zijn er klachten geweest waaraan tegemoet wordt gekomen?

De beweegredenen achter het voorstel

- Welke doelen dient het project, het proces of de applicatie? De beweegredenen kunnen sterk samenhangen met de aanleiding die hierboven wordt genoemd en met de verwerkingsdoeleinden en doelbinding zoals die in onderdelen 5 en 13 nader worden gespecificeerd.
- Zijn er andere organisaties bij betrokken die samen met de instelling de doelen hebben vastgesteld?
- De beweegredenen in dit onderdeel kunnen meer in zijn algemeenheid worden beschreven. In onderdelen 5 en 13 (model DPIA Rijksdienst) dienen de specifieke doeleinden per verwerking uiteen te worden gezet.

2.2 Persoonsgegevens

'Beschrijf alle persoonsgegevens die worden verwerkt. Classificeer deze persoonsgegevens naar: gewoon, gevoelig, bijzonder, strafrechtelijk en wettelijk identificatienummer. Geef per categorie persoonsgegevens aan welke persoonsgegevens worden verzameld en geef aan wat de bron is van deze persoonsgegevens.'

Hulpvragen en aandachtspunten:

Classificatie persoonsgegevens

- Voor de classificatie van persoonsgegevens kunnen eventuele verwerkersovereenkomsten worden geraadpleegd. Mogelijk is in een projectplan of bijbehorende documentatie al in kaart gebracht of, en zo ja welke, persoonsgegevens worden verwerkt.

Bron van persoonsgegevens

- Wat is de bron van de persoonsgegevens? Komen deze bijvoorbeeld van betrokkenen zelf (studenten, medewerkers, onderzoekers, contactpersonen), worden deze uit interne of openbare databases of applicaties gehaald, zoals het SIS? Werden de persoonsgegevens al eerder door uw instelling verwerkt, en zo ja, uit welke systemen worden de persoonsgegevens dan gehaald?

2.3 Gegevensverwerkingen

'Geef alle gegevensverwerkingen weer en geef aan welke categorieën persoonsgegevens worden verwerkt per gegevensverwerking. Desgewenst kan een stroomschema van de gegevensverwerkingen worden toegevoegd.'

Hulpvragen en aandachtspunten:

Algemeen

- Zijn of worden alle gegevensverwerkingen opgenomen in het verwerkingsregister, en voldoet dit register aan de wettelijke eisen?
- Let op de mate waarin de weergegeven gegevensverwerkingen moeten worden opgesplitst, of dat ze worden gecombineerd in overkoepelende gegevensverwerkingen. Splits bijvoorbeeld de verwerkingen op per verwerkingsdoel, en eventueel per grondslag eventueel weer. Als bijvoorbeeld binnen één verwerking verschillende persoonsgegevens worden verwerkt op een andere grondslag, kan voor het overzicht de verwerking worden opgesplitst (gelet op onderdeel 11 'Rechtsgrond' - model DPIA Rijksdienst).
- Let erop dat dezelfde persoonsgegevens in meerdere verwerkingen kunnen voorkomen.

2.4 Technieken en methoden van de gegevensverwerkingen

'Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem, bijvoorbeeld, of sprake is van bijvoorbeeld (semi-) geautomatiseerde besluitvorming, profilering, een cloudoplossing of big dataverwerkingen en, zo ja, beschrijf waaruit dat bestaat.'

Hulpvragen en aandachtspunten:

Algemeen

- Zijn er andere organisaties die de middelen van de verwerkingen samen met uw instelling hebben vastgesteld?

Geautomatiseerde besluitvorming

- Wat voor type besluiten worden (semi)geautomatiseerd genomen?

- Op welke wijze treffen deze besluiten de betrokkenen? Zijn er bijvoorbeeld rechtsgevolgen aan de besluiten verbonden?
- Welke betrokkenen worden getroffen door (semi)geautomatiseerde besluiten? Worden individuele betrokkenen geraakt, of (bepaalde) groepen van betrokkenen?

Juistheid van gegevens

- Let op! Het beginsel van juistheid van persoonsgegevens komt niet expliciet in het Rijksmodel aan bod. Toch kunnen er risico's bestaan in de naleving van dit beginsel, bijvoorbeeld als gegevens worden gecombineerd. Vanwege de samenhang met technieken en methoden van de gegevensverwerkingen worden relevante handvatten bij dit onderdeel gedeeld, maar het staat de uitvoerder van de DPIA vrij dit onderdeel ook mee te wegen bij de beoordeling van de rechtmatigheid van de gegevensverwerking.
- Worden persoonsgegevens gekoppeld, verrijkt of vergeleken uit verschillende bronnen?
- Wordt de kwaliteit van persoonsgegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig?
- Op welke wijze wordt de juistheid van persoonsgegevens gewaarborgd met de verschillende verwerkingen? Met welke frequentie worden persoonsgegevens bijvoorbeeld geüpdatet en op welke wijze wordt data gevalideerd bij invoering?
- Kunnen onjuiste persoonsgegevens worden gecontroleerd, gecorrigeerd, en onvolledige persoonsgegevens worden aangevuld?
- Wat zijn (mogelijke) gevolgen bij de verwerking van onjuiste persoonsgegevens?

2.5 Verwerkingsdoeleinden

'Beschrijf de doeleinden van alle gegevensverwerkingen. Voeg aanvullende informatie toe in het tekstveld.'

Hulpvragen en aandachtspunten:

Algemeen

- Let op de mate waarin de weergegeven gegevensverwerkingen moeten worden opgesplitst, of dat ze worden gecombineerd in overkoepelende gegevensverwerkingen. Splits bijvoorbeeld de verwerkingen op per verwerkingsdoel, en eventueel weer verder per oorspronkelijk verwerkingsdoel. Het kan zijn dat enkele gegevens binnen één verwerking al eerder voor een ander doel werden gebruikt, maar andere gegevens voor het eerst worden verwerkt.
- Zijn de genoemde verwerkingsdoeleinden ergens vastgelegd en formeel vastgesteld?
- Zijn er andere organisaties die samen met uw instelling de doelen van de verwerkingen hebben vastgesteld?

2.6 Betrokken partijen

'Benoem alle partijen die betrokken zijn en deel deze in per gegevensverwerking. Deel deze partijen in onder de rollen: verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker, sub-verwerker, verstrekker, ontvanger, betrokkene(n) en derde. Wanneer bekend, benoem ook welke functionarissen/afdelingen binnen deze partijen toegang krijgen tot welke categorieën persoonsgegevens. Voeg aanvullende informatie toe in het tekstveld.'

Hulpvragen en aandachtspunten:

Algemeen

- Welke (rechts)verhouding bestaat tussen uw instelling en de andere partij? Welke diensten worden van de betrokken partijen afgenomen (indien van toepassing)?
- Heeft de andere partij meer dan één rol, bijvoorbeeld omdat die partij persoonsgegevens verder verwerkt voor eigen doeleinden (indien van toepassing)?
- Let op! In het Rijksmodel komen gesloten overeenkomsten met derden (zoals verwerkersovereenkomsten en data uitwisselingsovereenkomsten) niet expliciet aan bod, net als certificeringen van deze partijen (indien en voor zover van toepassing). Uw instelling dient voor de volledigheid deze informatie nog in de DPIA op te nemen, waarvoor dit onderdeel geschikt is.

2.7 Belangen bij de gegevensverwerkingen

'Beschrijf alle belangen die de betrokken partijen hebben bij de gegevensverwerkingen. Vraag betrokkenen of hun vertegenwoordigers ook naar hun mening over de verwerking indien relevant. Licht deze mening toe onder het belang van de betrokkenen.'

Hulpvragen en aandachtspunten:

Algemeen

- De belangen van partijen kunnen verweven zijn met de doeleinden van de verwerkingen. Welke partijen verwerken persoonsgegevens, en met welke doelen doen zij dit? Verwerken partijen persoonsgegevens verder voor eigen doeleinden?
- In hoeverre zijn verdere verwerkingen van persoonsgegevens van partijen en de daaraan verbonden doeleinden voorzienbaar voor betrokkenen?

2.8 Verwerkingslocaties

'Benoem in welke landen de gegevensverwerkingen plaatsvinden. Beschrijf het doorgiftemechanisme dat van toepassing is wanneer verwerkingslocaties buiten de Europese Economische Ruimte bevinden en noem of en welke aanvullende maatregelen van toepassing zijn. Voeg aanvullende informatie toe in het tekstveld.'

Hulpvragen en aandachtspunten:

Algemeen

- Welke van de partijen genoemd in onderdeel 7 (belangen bij de gegevensverwerkingen - model DPIA Rijksdienst) verwerken persoonsgegevens?
- Op welke locaties verwerken deze partijen persoonsgegevens, en welke locaties vallen buiten de Europese Economische Ruimte (EER)?
- Ten aanzien van verwerkingen op locaties buiten de EER: welke waarborgen zijn getroffen voor de doorgifte? Denk aan een adequaatheidsbesluit of de Standard Contractual Clauses (SCC's).
- Welke aanvullende maatregelen zijn getroffen? Worden bijvoorbeeld persoonsgegevens geanonimiseerd of gepseudonimiseerd?

2.9 Juridisch en beleidsmatig kader

'Benoem alle wet- en regelgeving en beleid met mogelijke gevolgen voor de gegevensverwerkingen. De AVG en de Richtlijn [Richtlijn (EU) 2016/680, deze is niet relevant voor onderwijsinstellingen] hoeven niet genoemd te worden. Voeg aanvullende informatie toe in het tekstveld.'

Hulpvragen en aandachtspunten:

Algemeen

- Let erop dat ook beleid wordt meegenomen in het kader. Ten aanzien van bewaartermijnen is bijvoorbeeld het Documentair structuurplan (DSP) van belang.
- Welke gevolgen kan de wet- en regelgeving hebben op de gegevensverwerkingen?

2.10 Bewaartermijnen

'Bepaal de bewaartermijnen van de persoonsgegevens aan de hand van de gegevensverwerkingen en de verwerkingsdoeleinden. Motiveer waarom deze bewaartermijnen niet langer zijn dan strikt noodzakelijk ten opzichte van de verwerkingsdoeleinden. Beschrijf wie toeziet op de bewaartermijn en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn. Voeg aanvullende informatie toe in het tekstveld.'

Hulpvragen en aandachtspunten:

Algemeen

- Ten aanzien van bewaartermijnen is bijvoorbeeld het Documentair structuurplan (DSP) van belang. Let erop dat niet alle bewaartermijnen hieruit 1-op-1 worden overgenomen, maar dat de verwerkingsverantwoordelijke zelf een motivering geeft per bewaartermijn, voor zover deze niet wettelijk is voorgeschreven.
- Worden persoonsgegevens op meerdere plaatsen bewaard en is voor iedere plaats een bewaartermijn vastgesteld?
- Is er een procedure voor de verwijdering, retourzending of vernietiging van persoonsgegevens, en hoe ziet deze procedure uit? Worden bewaartermijnen geautomatiseerd gehandhaafd, of gebeurt dit handmatig?
- Worden persoonsgegevens na afloop van de bewaartermijn op zodanige wijze verwijderd of vernietigd dat deze niet meer te benaderen en te gebruiken zijn?

2.11 Rechtsgrond

'Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd. Elke rechtsgrond moet aan bepaalde voorwaarden voldoen. Voeg in de toelichting op de rechtsgrond toe hoe aan deze voorwaarden wordt voldaan. En voeg aanvullende informatie toe in het tekstveld.'

De rechtsgronden zijn:

- Toestemming
    - Voor toestemming is nodig dat deze op ondubbelzinnige wijze vrij wordt gegeven voor een specifieke verwerking.
    - Licht toe hoe hieraan wordt voldaan.
- Noodzakelijk voor de uitvoering van de overeenkomst

    - Hier moet sprake zijn van een overeenkomst met de betrokkene, geef aan van wat voor overeenkomst sprake is.
- Noodzakelijk om te voldoen aan een wettelijke verplichting
    - Geef aan welke EU- of Nederlandse wetsbepalingen van toepassing zijn.
- Noodzakelijk om de vitale belangen van de betrokkene of een ander te beschermen
    - Hiervan kan sprake zijn wanneer iemands leven of gezondheid in gevaar is en die persoon niet in staat is om toestemming te geven.
- Noodzakelijk voor de vervulling van een taak van algemeen belang
    - Geef aan welke EU- of Nederlandse wetsbepalingen van toepassing zijn.
- Noodzakelijk voor de behartiging van een gerechtvaardigd belang
    - Deze grondslag is niet van toepassing op gegevensverwerkingen die worden uitgevoerd in het kader van de publieke taak van een overheidsorgaan.
    - Voor deze grondslag is een belangenafweging nodig, voeg deze toe aan de toelichting op de rechtsgrond.

Hulpvragen en aandachtspunten:

<u>Algemeen</u>

- Zijn er verdere verwerkingen van persoonsgegevens, en zijn de doeleinden voor die verdere verwerkingen verenigbaar met de oorspronkelijke doeleinden van de verwerking? Zo ja, dan kan voor de grondslag van de verenigbare verwerking worden teruggevallen op de grondslag van de oorspronkelijke verwerking. Zo niet, dan dient een nieuwe grondslag voor de verwerking te worden aangewezen.
- Is voorafgaand aan de verwerkingen aan elk verwerkingsdoel een rechtsgrond verbonden?

2.12 Bijzondere persoonsgegevens

'Het verwerken van bijzondere of strafrechtelijke persoonsgegevens is in principe verboden. Verwerking is pas mogelijk wanneer een uitzonderingsgrond van toepassing is. Beoordeel of een van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een nationaal identificatienummer, beoordeel of dit is toegestaan. Voeg aanvullende informatie toe in het tekstveld.'

Hulpvragen en aandachtspunten:

<u>Algemeen</u>

- Worden er bijzondere persoonsgegevens verwerkt, en zo ja, is er een uitzondering op het verbod tot verwerking van bijzondere persoonsgegevens op van toepassing? Denk aan de uitzondering die voor verwerkingen die noodzakelijk zijn met het oog op de speciale begeleiding van leerlingen of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand (artikel 9 lid 2 sub g AVG jo. artikel 30 lid 2 sub a UAVG).

2.13 Doelbinding

'Als de persoonsgegevens voor een ander doeleinde worden verwerkt dan het doeleinde waarvoor de persoonsgegevens oorspronkelijk zijn verzameld, beoordeel of deze (nieuwe) verdere verwerking toelaatbaar is op grond van Unie- of lidstaatrechtelijk recht, dan wel

verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. Voeg in het tekstveld de verenigbaarheidstoets en aanvullende informatie toe.'

Hulpvragen en aandachtspunten:

Algemeen

- Worden er persoonsgegevens verwerkt die eerder voor een ander doeleinde werden verwerkt? Zo ja, is het doeleinde van de nieuwe verwerking verenigbaar met het oorspronkelijke doeleinde?
- Om te beoordelen of een verwerkingsdoel verenigbaar is met het oorspronkelijke verwerkingsdoel, moet op de volgende punten worden gelet:
    - het verband tussen het oorspronkelijke doel en het nieuwe/toekomstige doel;
    - de context waarin de gegevens zijn verzameld (wat is de relatie tussen uw onderneming/organisatie en de persoon?);
    - de soort en aard van de gegevens (betreft het gevoelige gegevens?);
    - de mogelijke gevolgen van de voorgenomen verdere verwerking (welke zijn de gevolgen de betrokkene?);
    - het bestaan van passende waarborgen (zoals versleuteling of pseudonimisering).
- Indien de beoogde verwerking verenigbaar is met de oorspronkelijke verwerking hoeft geen nieuwe verwerkingsgrondslag te worden aangewezen, maar kan worden teruggevallen op de grondslag van de oorspronkelijke verwerking. Indien de beoogde verwerking niet verenigbaar is, dient een nieuwe grondslag te worden gezocht.
- Hoe wordt gewaarborgd dat persoonsgegevens enkel voor het vastgestelde doel worden verwerkt, en de vastgestelde doeleinden niet zomaar uitdijen?

2.14 Noodzaak en evenredigheid

'Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk en evenredig zijn voor het verwezenlijken van de verwerkingsdoeleinden.
Ga hierbij in ieder geval in op:

a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt?'

Hulpvragen en aandachtspunten:

Algemeen

- Let erop dat de noodzakelijkheidsvraag sterk raakt aan het beginsel van dataminimalisatie. In de toelichting bij proportionaliteit dient er dan ook aandacht te worden besteed aan de vraag of er persoonsgegevens worden verwerkt die strikt noodzakelijk zijn, of dat ze enkel 'nice to have' zijn.
- Hoe is toegang tot persoonsgegevens gewaarborgd (autorisaties)? Kunnen personen enkel bij gegevens die strikt noodzakelijk zijn voor de uitoefening van hun werkzaamheden?
- Op welke andere wijzen wordt de privacy-inbreuk voor betrokkenen beperkt?

2.15 Rechten van betrokkenen

'Beschrijf de procedure waarmee invulling wordt gegeven aan de rechten van de betrokkenen. Als de rechten van de betrokkene worden beperkt, beschrijf op grond van welke wettelijke uitzondering dat is toegestaan.'

Hulpvragen en aandachtspunten:

Algemeen

- Is er beleid, een protocol of een werkinstructie voor de omgang met rechten van betrokkenen, en wordt deze documentatie nageleefd?
- Is de aanwezige documentatie ook van toepassing op de door het voorstel beoogde verwerkingen, en zijn er nog aanpassingen nodig in deze documentatie?
- Leidt het voorstel ertoe dat één of meer rechten van betrokkenen lastiger kunnen worden uitgeoefend?
- Kunnen betrokkenen hun rechten ook uitoefenen ten aanzien van de door het voorstel beoogde verwerkingen?
- Worden de beoogde verwerkingen in de privacyverklaring opgenomen, voldoet deze privacyverklaring aan de wettelijke eisen en is deze makkelijk vindbaar voor betrokkenen?
- Indien cookies of vergelijkbare technologieën worden gebruikt: wordt over dit gebruik dan voldoende informatie gegeven in de cookieverklaring en cookiebanner, zijn de cookies juist ingesteld en wordt op de juiste wijze toestemming gevraagd in de cookiebanner?

2.16 Risico's voor betrokkenen

'Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, zoals het verbod op discriminatie;
b. de oorsprong van deze gevolgen;
c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.'

Hulpvragen en aandachtspunten:

Algemeen

- Ga per onderwerp (1 t/m 15 - model DPIA Rijksdienst) na of er risico's bestaan voor betrokkenen. Let er daarbij op dat in het Rijksmodel niet alle relevante thema's expliciet worden benoemd, zoals juistheid van persoonsgegevens en al dan niet gesloten (verwerkers)overeenkomsten.
- Let erop dat er ook risico's kunnen zijn voor uw instelling, zonder dat dit direct een risico voor betrokkenen hoeft op te leveren. Uw instelling dient te overwegen of zij deze risico's hier ook uiteen wil zetten. Zo kan bijvoorbeeld een probleem bestaan in de verantwoordingsplicht, terwijl de relevante informatie wel beschikbaar is binnen de organisatie, zoals een nog bij te werken verwerkingsregister.

2.17 Maatregelen

'Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt. Voeg aanvullende informatie in het tekstveld onder de tabellen toe.

Beschrijf ook de resterende risico's die nog aanwezig zijn na de uitvoering en/of implementatie van de geïdentificeerde maatregelen. Geef per resterend risico aan wat het niveau is van dit risico.

Geef tot slot een conclusie over de restrisico's. Zijn deze acceptabel? En is er een voorafgaande raadpleging bij de Autoriteit Persoonsgegevens nodig?'

Hulpvragen en aandachtspunten:

<u>Algemeen</u>

- Let erop dat de te treffen maatregelen maatwerk zijn: er is geen algemeen overzicht van maatregelen die getroffen kunnen worden dat altijd volstaat. Maatregelen moeten passend zijn, waarvoor gelet kan worden op:
    - de organisatie,
    - de gegevensverwerkingen,
    - de gesignaleerde risico's.
- Bij de te treffen maatregelen moet rekening gehouden worden met:
    - de stand van de techniek,
    - de kosten om persoonsgegevens goed te beveiligen,
    - de aard, de omvang, de context en het doel van de verwerkingen.
- Worden de getroffen maatregelen periodiek getoetst op effectiviteit door middel van een plan-do-check-act cyclus?
- Worden er technische maatregelen getroffen, zoals:
    - software up-to-date houden,
    - beheer van technische kwetsbaarheden,
    - versleuteling van gegevens (encryptie),
    - het maken van back-ups.
- Worden er organisatorische maatregelen getroffen, zoals:
    - het beperken van autorisaties voor omgang met persoonsgegevens,
    - privacy en security awareness (bewustzijn) verhogen binnen de organisatie,
    - het opstellen van een plan-do-check-act cyclus,
    - werkinstructies en protocollen opstellen met betrekking tot privacy en security, bijvoorbeeld over de afhandeling van datalekken.
- Worden er juridische maatregelen getroffen, zoals:
    - het sluiten van (verwerkers)overeenkomsten met betrokken partijen,
    - het overeenkomen van geheimhoudingsbedingen met personen die met gevoelige persoonsgegevens omgaan.

Bijlage 1 Pre-DPIA Checklist

Waarom is een DPIA nodig voor deze verwerking?		
Een DPIA is alleen verplicht als er een verwerking gaat plaatsvinden die mogelijk een hoog risico met zich meebrengt. Hiervoor zijn criteria opgesteld in de Algemene verordening gegevensbescherming (AVG) en aanvullend door de Autoriteit Persoonsgegevens en EU-privacy toezichthouders. De AVG geeft aan dat in ieder geval een DPIA moet worden uitgevoerd als bij de (voorgenomen) verwerking sprake is van een van de onderstaande 4 punten. **Als de verwerking aan één van deze criteria voldoet, dan is het uitvoeren van een DPIA verplicht**. Meer uitleg over elk punt kun je vinden via de volgende link: - **https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia#wanneer-een-dpia** **Geef hieronder aan of sprake is van een of meerdere criteria.**		
1.	De organisatie beoordeelt systematisch en uitgebreid persoonlijke aspecten van mensen. Dit doet de organisatie op basis van geautomatiseerde verwerking van persoonsgegevens, waaronder profiling. Hierop baseert de organisatie besluiten die gevolgen hebben voor mensen.	☐
2.	De organisatie verwerkt op grote schaal bijzondere persoonsgegevens.	☐
3.	De organisatie verwerkt strafrechtelijke gegevens	☐
4.	De organisatie volgt mensen op grote schaal en systematisch in een publiek toegankelijk gebied.	☐
De AP heeft een lijst opgesteld van soorten verwerkingen waarvoor het uitvoeren van een DPIA verplicht is. Die lijst is opgenomen in de 17 punten hieronder. **Als de verwerking aan één van deze criteria voldoet, dan is het uitvoeren van een DPIA verplicht**. Meer uitleg over elk punt kun je vinden via de volgende twee links: - https://wetten.overheid.nl/BWBR0042812/2019-11-27 - https://www.autoriteitpersoonsgegevens.nl/documenten/lijst-verplichte-dpia **Geef hieronder aan of sprake is van een of meerdere criteria.**		
1.	Heimelijk onderzoek	☐
2.	Zwarte lijsten	☐
3.	Fraudebestrijding	☐
4.	Creditscores	☐
5.	Financiële situatie	☐
6.	Genetische persoonsgegevens	☐
7.	Gezondheidsgegevens	☐
8.	Samenwerkingsverbanden	☐
9.	Cameratoezicht	☐
10.	Flexibel cameratoezicht	☐
11.	Controle werknemers	☐

12.	Locatiegegevens	☐
13.	Communicatiegegevens	☐
14.	Internet of things	☐
15.	Profilering	☐
16.	Observatie en beïnvloeden van gedrag	☐
17.	Biometrische gegevens	☐
Naast de richtlijnen van de AP, hebben EU-privacy toezichthouders opgesteld. Die lijst is opgenomen in de 9 punten hieronder. **Als de verwerking aan twee of meer criteria voldoet, dan is het uitvoeren van een DPIA verplicht**. Meer uitleg over elk punt kun je vinden via de volgende link: - https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia#wanneer-een-dpia **Geef hieronder aan of sprake is van een of meerdere criteria.**		
1.	Beoordelen van mensen op basis van persoonskenmerken	☐
2.	Geautomatiseerde besluiten	☐
3.	Stelselmatige en grootschalige monitoring	☐
4.	Gevoelige gegevens	☐
5.	Grootschalige gegevensverwerkingen	☐
6.	Gekoppelde databases	☐
7.	Gegevens over kwetsbare personen	☐
8.	Gebruik van nieuwe technologieën	☐
9.	Blokkering van een recht, dienst of contract	☐
Als de DPIA op basis van een andere reden wordt uitgevoerd, bijvoorbeeld vrijwillig, dan kan dat hieronder omschreven worden.		
1.	Vrijwillig	☐
2.	Op basis van een andere reden dan tot nog toe vermeld, namelijk [vul onderstaande tekst vak in]:	☐

Bijlage 2 DPIA-vragenlijst

Vragenlijst intakegesprek	
1.	Beschrijf de werkzaamheden die je binnen jouw organisatie uitvoert.
2.	Welke persoonsgegevens worden hierbij verwerkt? *Let erop dat de juridische termen 'persoonsgegevens' en 'verwerkt' in het dagelijks taalgebruik anders kunnen worden geïnterpreteerd.
3.	Van wie zijn deze persoonsgegevens die worden verwerkt?
4.	Verwerk je ook bijzondere persoonsgegevens? * Bijvoorbeeld: medische gegevens, ras, politieke gezindheid, lidmaatschap van een vakbond, godsdienst)
5.	Waarom en met welk doel verwerk je deze persoonsgegevens?
6.	Weet je waar en/of in welke systemen/software deze persoonsgegevens worden opgeslagen? Zo ja, welke systemen/software zijn dat?
7.	Hoe lang worden deze persoonsgegevens bewaard?
8.	Zijn met betrekking tot deze persoonsgegevens bewaartermijnen afgesproken?
9.	Wat is het beleid met betrekking tot het verwijderen van de persoonsgegevens? Bijvoorbeeld: automatische verwijdering.
10.	Met welke interne en/of externe derde(n) worden persoonsgegevens gedeeld? Bijvoorbeeld: (IT-)leveranciers/marketingdienstverleners etc.
11.	In welke landen worden persoonsgegevens gedeeld of opgeslagen?
12.	Op welke manier worden persoonsgegevens beveiligd? Bijvoorbeeld: SSL op de website/encryptie/autorisatiebeleid/audits/logging etc.
13.	Is het mogelijk om thuis te werken, en zo ja, zijn hier regels aan verbonden?
14.	Kun je met eigen apparatuur toegang krijgen tot gegevens van jouw organisatie? En zo ja, zijn hier regels aan verbonden?
15.	Op welke manier worden (reguliere) overeenkomsten met derden gesloten?
16.	Wie is volgens jou verantwoordelijk voor het sluiten van (reguliere) overeenkomsten met derden?
17.	Zijn er, voor zover bekend, eigen (reguliere) standaardovereenkomsten?
18.	Wordt met deze partijen ook een verwerkersovereenkomst gesloten?
19.	Wordt binnen jouw organisatie/afdeling één of meer van de volgende stukken gehanteerd: a. Intern privacy beleid b. Calamiteitenplan voor datalekken c. Personeelshandboek d. ICT-protocol e. BYOD-beleid f. Privacyverklaring g. Verwerkingsregister
20.	Wat versta jij onder een datalek?
21.	Weet jij wat je moet doen bij een datalek?
22.	Heeft jouw organisatieregels opgesteld met betrekking tot hoe je moet handelen bij een datalek?
23.	Zijn er wel een (juridische) incidenten op privacy vlak geweest binnen jouw afdeling en zo ja, hoe zijn deze afgehandeld?

24.	Ben jij / Is in jouw team, in geval het verzoek wordt gedaan, in staat om een betrokkene volledig ‘te vergeten’/alle gegevens te wissen?
25.	Wie is jouw aanspreekpunt voor privacy gerelateerde vragen?
26.	Zijn er nog dingen die je kwijt wilt ten aanzien van privacy zaken binnen jouw afdeling?
27.	Voorzie je verder nog privacy technische of juridische risico’s binnen jouw organisatie/afdeling?