Kennisnet

Handreiking DPIA PO / VO

Data Protection Impact Assessment V1.0

Laat ict werken **voor het onderwijs**

Inhoud

Colofon

Versie 1.0 (13 juli 2018)

Auteurs Roza van Cappellen, Elly Dingemanse, Axel Eissens

Met dank aan Leon van Lare (SOML), Annemarie Jonker (Kennisnet)

LET OP!
Deze versie van de Handreiking DPIA heeft nog een voorlopige status.
De werkgroepen IBP van de PO en de VO raad, kunnen nog wijzigingen in het document aanbrengen.
Wanneer je zelf onvolkomenheden aan het document constateert of je hebt een vraag over de inhoud, neem dan contact op met de supportdesk van Kennisnet *https://support.kennisnet.org/Core/Default/Index*

Waar in deze publicatie geschreven wordt in de mannelijke vorm, kan mede de vrouwelijk vorm gelezen worden.

1. Samenvatting

Een DPIA is een Data Protection Impact Assessment.

Deze handreiking beschrijft waarom je een DPIA uitvoert, wanneer dat nodig is en wanneer niet. Met een kleurenschema kun je een inschatting maken of een DPIA voor jouw organisatie nodig is of niet. De uitkomst daarvan kan meteen een handig hulpmiddel zijn als je inderdaad een DPIA moet uitvoeren.

Met een DPIA schat je de privacyrisico's in voordat je:

- een nieuwe verwerking van persoonsgegevens start, of
- een bestaande verwerking van persoonsgegevens aanpast.

Een DPIA maak je niet alleen. Dat doe je met een groep medewerkers (intern of extern) die bij de verwerking betrokken zijn.

Vanuit een bestaande situatie ga je kijken naar welke gevolgen deze verwerking heeft voor de betrokkenen.

In 4 stappen doorloop je het hele DPIA. Aan de hand van je projectplan of plan van aanpak kijk je naar:

1. **de kenmerken van de verwerking**;
   het doel van de verwerking, wie betrokken zijn en wat de verwerkingen betekenen voor de betrokkenen
2. **de rechtmatigheid**;
   de grondslag voor de verwerking en aan welke wet- en regelgeving je moet voldoen
3. **de risico's** die kunnen optreden bij de verwerking;
   zijn er mogelijk negatieve gevolgen voor de betrokkenen, is het waarschijnlijk dat die optreden en wat is de impact daarvan?
4. **de maatregelen die je moet nemen** om die risico's zoveel mogelijk te beperken;
   dekken die maatregelen de negatieven gevolgen af?
   - Zo ja, dan ga je met je DPIA verslag naar de FG, functionaris voor gegevensbescherming, om te bespreken hoe de FG er tegenaan kijkt. Zijn FG en bestuur akkoord, dan kun je aan de slag met je plan van aanpak. Daarmee is je DPIA afgerond
   - Zo nee, dan begin je weer opnieuw, want het is niet acceptabel dat de rechten van de betrokkenen geschonden worden

Wanneer de verwerking is goedgekeurd kun je aan de slag met de verwerking. De verwerking moet ook worden genoteerd in het register van verwerkingen of het dataregister.

Deze handreiking bevat in de bijlagen twee templates voor het uitvoeren van een DPIA. Beide zijn gebaseerd op het stappenplan van de Rijksoverheid. De tweede template geeft de relaties met het dataregister weer.

2. Inleiding

DPIA is de afkorting voor Data Protection Impact Assessment, in het Nederlands een gegevensbeschermings-effectbeoordeling. Onder de Wet bescherming persoonsgegevens (Wbp) werd dit een Privacy Impact Assessment genoemd (PIA). PIA en DPIA worden regelmatig door elkaar gebruikt. In dit document wordt de afkorting DPIA gebruikt.

Verwerkingen van persoonsgegevens moeten beoordeeld worden vóórdat ermee wordt begonnen of vóórdat deze worden aangepast door bijvoorbeeld:

- nieuwe technische ontwikkelingen;
- nieuwe applicaties;
- nieuwe voorgenomen verwerkingen van persoonsgegevens.

Je legt met een DPIA vast wat de consequenties en risico's zijn van de verwerking voor de privacy van de betrokkenen. Op basis van de uitkomsten van het DPIA bepaal je of er (extra) maatregelen nodig zijn om de privacy van de betrokkenen (beter) te beschermen.

Het schoolbestuur moet ervoor zorgen dat een DPIA wordt uitgevoerd wanneer dat nodig is. Een DPIA is verplicht wanneer een project (wijziging in of nieuw administratiesysteem bijvoorbeeld) hoge risico's voor de privacy van de betrokkenen oplevert.

Een DPIA heeft de vorm van een toetsmodel of vragenlijst met feitelijke, technische en juridische eisen en vragen over de voorgenomen verwerkingen van persoonsgegevens. De uitkomst van een DPIA is niet vrijblijvend, maar richtinggevend en corrigerend. Het resultaat is een overzicht van de privacy risico's. Op basis van deze risico's moet je maatregelen nemen om de privacy voldoende te beschermen.

Artikel 35 lid 1 van de AVG beschrijft wanneer een DPIA nodig is:

> "*Wanneer een soort verwerking (in het bijzonder een verwerking waarbij **nieuwe technologieën** worden gebruikt, gelet op de **aard, de omvang, de context en de doeleinden** daarvan) waarschijnlijk een **hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen** voert de verwerkingsverantwoordelijke **vóór de verwerking** een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks **vergelijkbare verwerkingen** bestrijken die vergelijkbare hoge risico's inhouden".*

De belangrijkste aandachtspunten van een DPIA zijn:

- Speciale aandacht voor **nieuwe technologieën**; dat kan een nieuwe digitale omgeving zijn, maar ook een nieuwe applicatie, een grote aanpassing van de (ICT)omgeving of applicatie of een nieuwe/gewijzigde manier waarop persoonsgegevens worden uitgewisseld.
- De **aard, de omvang, context en de doeleinden** waarvoor de verwerking met nieuwe technologieën plaatsvindt; met welk doel worden welke typen persoonsgegevens verwerkt en in welke omvang?
- De inschatting dat de verwerking een **hoog privacy risico** met zich meebrengt; schat in hoe groot het risico is bij de verwerking van een bepaald type persoonsgegeven uitgaande van de nieuwe voorgenomen technologieën of informatiesystemen die gebruikt gaan worden.
- Het DPIA moet uitgevoerd worden **vóór de daadwerkelijke** voorgenomen nieuwe verwerking plaatsvindt; je voert het onderzoek uit voordat het betreffende implementatie project start of wijzigt.
- De beoordeling kan gelden voor een **reeks vergelijkbare verwerkingen** met vergelijkbare hoge risico's; wanneer er al een DPIA is uitgevoerd voor een bestaande vergelijkbare verwerking, mag je daaraan refereren en hoef je geen nieuwe DPIA uit te voeren.

1. Waarom een DPIA

Een DPIA verzamelt informatie over de verwerking, privacyrisico's en maatregelen.

Het verzamelen van informatie, het nadenken over risico's, het beantwoorden van vragen helpt medewerkers en leidinggevenden bij de besluitvorming en het afleggen van verantwoording hierover. Bescherming van persoonsgegevens wordt op deze manier een onderdeel van belangenafwegingen, besluitvorming over voorgenomen beleid, regelgeving en (ict-)projecten binnen het onderwijs.

Een DPIA draagt op deze manier bij aan:

- een betere besluitvorming en inschatting van de haalbaarheid van het project,
- een betere kwaliteit van gegevens,
- een groter privacybewustzijn binnen de school, en
- meer vertrouwen bij de betrokkenen in de manier waarop je hun persoonsgegevens verwerkt en maatregelen die je daarvoor treft.

Een DPIA helpt ook bij het aansturen van leveranciers. Je kunt de lijst van risico's en de maatregelen om die risico's te verkleinen gebruiken om een gerichte opdracht geven aan de degene die een product of dienst verder ontwikkelt. Zo kun je voorkomen dat er in een later stadium kostbare aanpassingen nodig zijn, omdat de verwerkingen niet voldoen aan de privacywetgeving.

Wanneer je een DPIA hebt uitgevoerd en de verwerking na goedkeuring start, moet je deze nieuwe verwerking vastleggen in je register van verwerkingen en blijven monitoren. De nieuwe verwerking wordt binnen het gegevensbeschermingsproces opgenomen in de PDCA-cyclus (Plan, Do, Check, Act). Een DPIA en deze monitoring kunnen onderdeel zijn van kwaliteitssystemen die al op school worden ingezet. Je kunt het bijvoorbeeld opnemen als onderwerp in de RI&E of in de stappen die je zet ten behoeve van de accountantscontrole.

2. Wanneer een DPIA

Het schoolbestuur moet een DPIA uitvoeren als de organisatie:

- systematisch en uitgebreid persoonlijke aspecten evalueert, gebaseerd op geautomatiseerde verwerking (waaronder profiling) waarop besluiten worden gebaseerd die gevolgen kunnen hebben voor mensen;
- op grote schaal bijzondere persoonsgegevens verwerkt of wanneer er strafrechtelijke gegevens worden verwerkt ;
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

De AP heeft een lijst van soorten verwerkingen opgesteld waarvoor het uitvoeren van een DPIA verplicht is. De lijst is niet uitputtend. Het kan zijn dat de verwerking niet op deze lijst staat[1]. In dat geval moet de school zelf beoordelen of de verwerking een hoog privacyrisico oplevert voor de betrokkenen.

Bij die beoordeling kun je gebruik maken van de 9 criteria die de Europese privacytoezichthouders hebben opgesteld. Als vuistregel geldt dat een DPIA moet worden uitgevoerd als de verwerking aan twee of meer van de onderstaande criteria voldoet:

- **Beoordeling van mensen op basis van persoonsgegevens**
  Denk daarbij aan het maken van prognoses, met name op basis van kenmerken als gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsing.
- **Geautomatiseerde beslissingen**
  Denk hierbij aan beslissingen die voor de betrokkene wezenlijke gevolgen kunnen hebben, zoals discriminatie of uitsluiting. De beslissingen worden door de technologie automatisch gemaakt, niet door mensen.
- **Stelselmatig en grootschalige monitoring**
  Denk hierbij bijvoorbeeld aan monitoring in openbaar toegankelijke ruimten met camera's. Maar ook het volgen van leerlingen en vastleggen van de observaties valt in deze categorie: het leerlingadministratiesysteem en leerlingvolgsysteem vallen onder deze definitie.
- **Gevoelige informatie**
  Hierbij gaat het om bijzondere categorieën van persoonsgegevens. Deze staan omschreven in artikel 9 van de AVG en hebben te maken met bijvoorbeeld politieke voorkeuren, strafrechtelijke gegevens, gezondheid, financiële gegevens.
- **Grootschalige verwerkingen**
  Dit kan te maken hebben met de hoeveelheid mensen van wie je persoonsgegevens verwerkt of de hoeveelheid gegevens of de verscheidenheid daarvan, de tijdsduur ervan of de reikwijdte. Denk dus of het gaat om verwerkingen van alle leerlingen of medewerkers in een systeem.
- **Gekoppelde databases**
  Denk hierbij aan gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn. Ze kunnen een verschillende wettelijk grondslag of verschillend doel of zelfs een verschillende verwerkingsverantwoordelijke hebben.

1 **Let op:** *De verwerking moet altijd voldoen aan de AVG. Als de voorgenomen verwerking op deze lijst staat, moet nog steeds worden nagegaan of er voor deze verwerking een geldige grondslag is. Is er geen geldige grondslag, dan mogen de persoonsgegevens niet verwerkt worden ongeacht de uitkomsten van een eventuele DPIA.*

- **Gegevens van kwetsbare personen**
  Denk hierbij aan de ongelijkheid tussen de betrokkene en de verwerkingsverantwoordelijke. Betrokkene kan bijvoorbeeld niet in vrijheid toestemming verlenen of de verwerking weigeren, zoals sommige patiënten of kinderen. Bedenk hierbij dat de Autoriteit Persoonsgegevens leerlingen benoemd tot een kwetsbare groep betrokkenen waarvan doorgaans veel gevoelige gegevens worden vastgesteld.
- **Gebruik van nieuwe technologieën**
  De reden daarvoor is dat er mogelijk op een nieuwe manier gegevens verzameld worden met mogelijk grote privacyrisico's. Met een DPIA kan de verantwoordelijke de risico's beter begrijpen en verhelpen.
- **Blokkering van een recht, dienst of contract**
  Denk hierbij aan een verwerking die als gevolg kan hebben dat de betrokkene een recht niet kan uitoefenen, een dienst niet kan gebruiken of een contract niet kan afsluiten. Zoals bijvoorbeeld een bank die persoonsgegevens verwerkt om te bepalen of zij een lening aan iemand wil verstrekken.

De verwerking moet altijd voldoen aan de AVG. Als de voorgenomen verwerking op de lijst voor de verplichte DPIA staat, moet nog steeds worden nagegaan of er voor deze verwerking een geldige grondslag is. Is er geen geldige grondslag, dan mogen de persoonsgegevens niet verwerkt worden ongeacht de uitkomsten van een eventuele DPIA.

3. Wanneer geen DPIA

Je hoeft geen DPIA uit te voeren wanneer:

- de verwerking waarschijnlijk geen hoog privacyrisico oplevert;
- de verwerking sterk lijkt op een andere gegevensverwerking waarvoor je al een DPIA hebt uitgevoerd (die DPIA mag je dan hergebruiken). Let wel: wanneer de verwerking, het risico of de context verandert, kan die verplichting er weer wel zijn.
- je persoonsgegevens verwerkt op basis van een andere wet en als je in het kader van die wet al een DPIA hebt uitgevoerd;
- de verwerking op een lijst staat van verwerkingen waarvoor een DPIA niet verplicht is. De AVG geeft de privacy toezichthouder de mogelijkheid om zo'n lijst op te stellen, maar dit is niet verplicht. De AP heeft tot nu toe geen gebruik gemaakt van de mogelijkheid een dergelijke lijst op te stellen.

4. Wie voert een DPIA uit

De verwerkingsverantwoordelijke moet zorgen dat een DPIA uitgevoerd wordt. Voor een school is dat de bestuurder, het bevoegd gezag. De bestuurder hoeft een DPIA niet zelf uit te voeren, maar is er wel verantwoordelijk voor dat het daadwerkelijk gebeurt.

Een best practice bij een DPIA is om verschillende medewerkers en eventueel externen te betrekken om een juiste beeldvorming te krijgen. Denk hierbij aan:

- **Andere partijen die belangen hebben bij de verwerking**
  Denk hierbij aan de IT-afdeling, juridische adviseurs, informatiemanager, applicatiebeheerder.
- **De verwerker van de gegevens**
  Als de verwerking van de persoonsgegevens is uitbesteed, dan moet de verwerker de school ondersteunen en informatie verstrekken bij de uitvoering van een DPIA. Dat geldt uiteraard alleen voor dat gedeelte dat is uitbesteed. Het is goed om daarbij een onderscheid te maken tussen de inhoud en de uitvoering. De verwerkingsverantwoordelijke blijft verantwoordelijk voor de inhoud, de verwerker kan bijvoorbeeld verantwoordelijk zijn voor de manier waarop de gegevens opgeslagen worden.
- **De betrokkenen**
  In sommige gevallen kun je de betrokkenen om hun mening vragen, wijk je daarna af van de mening van de betrokkenen dan moet je dat goed onderbouwen.
- **Een functionaris voor gegevensbescherming (FG)**
  Voor een DPIA moet je de FG om advies vragen. In de verslaglegging moet dat advies staan en wat je ermee gedaan hebt. De FG moet de uitvoering van het DPIA in de gaten houden. Het is dan ook verstandig de FG in een vroeg stadium hierbij te betrekken.

5. Hulpmiddel bij het DPIA voorbereiden

De tabel hieronder is een hulpmiddel bij het inschatten of je een DPIA moet uitvoeren.

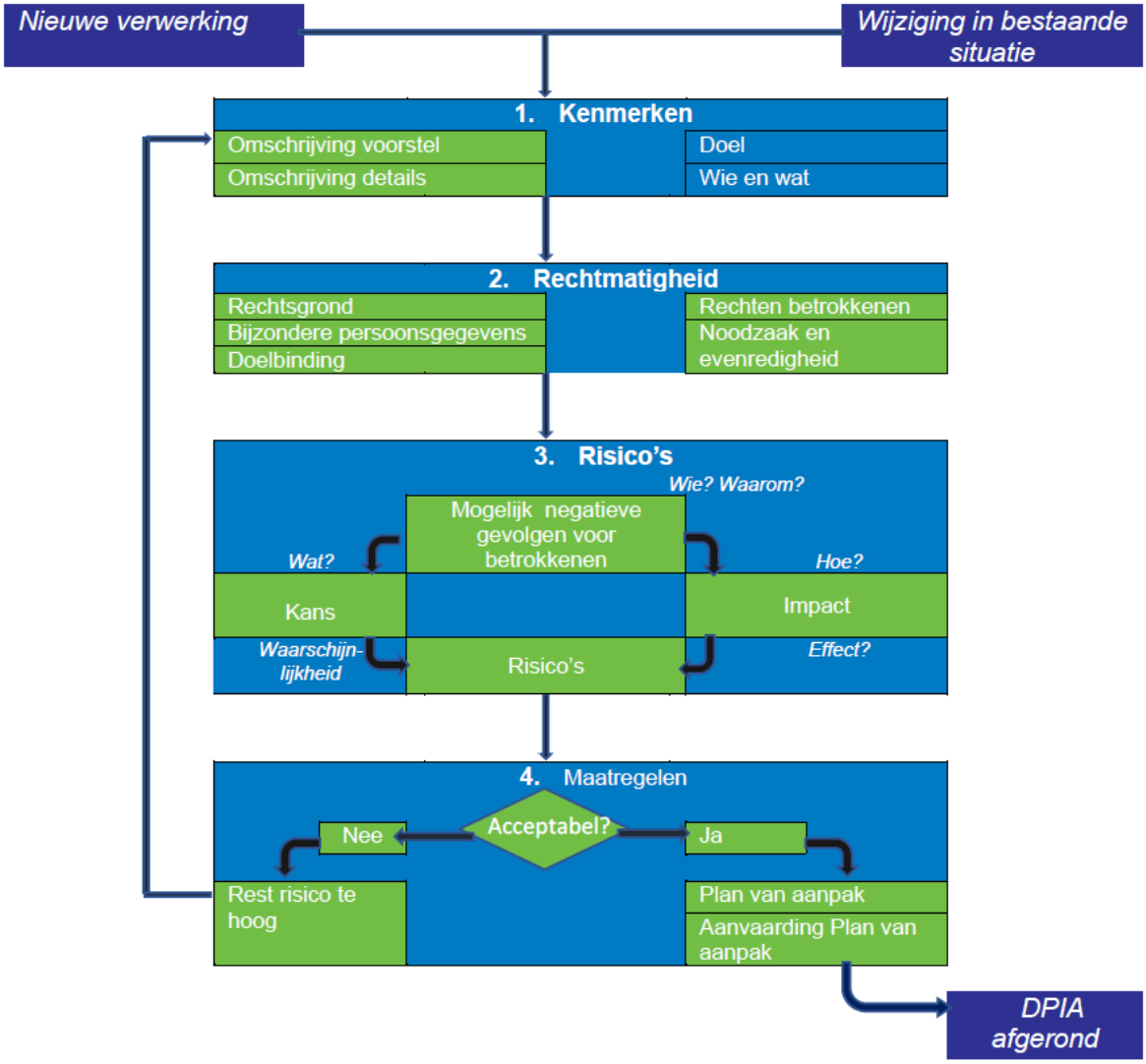
Zet een vinkje in kolom van het best passende antwoord ja of nee. Wanneer er veel vinkjes staan in de oranje vakken, moet je waarschijnlijk een DPIA uitvoeren. Het geeft gelijk een indruk van welke onderdelen extra aandacht nodig hebben.

	Vraag	**Ja**	**Nee**
1.	Is er sprake van een nieuwe verwerking of een nieuwe manier van de verwerking van persoonsgegevens (bijvoorbeeld een nieuwe applicatie of nieuwe techniek)?	Ga naar 3	
2.	Is de verwerking al opgenomen in een verwerkings- of dataregister?	Ga naar 8	
3.	Zijn de te verwerken persoonsgegevens, het systeem of de applicatie waarmee de verwerking plaatsvindt geclassificeerd (hebben ze een BIV waarde)?		
4.	Past de nieuwe verwerking bij de verwerkingsdoeleinden van de school?		
5.	Is er een grondslag voor de nieuwe verwerking?		
6.	Kun je aantonen dat je alleen de meest noodzakelijke gegevens vastlegt?		
7.	Kun je aantonen dat je de gegevens op geen enkele andere manier kunt verkrijgen?		
8.	Worden er andere persoonsgegevens vastgelegd dan tot nu toe?		
9.	Worden er gevoelige persoonsgegevens over betrokkenen verwerkt?		
10.	Wordt er informatie verwerkt over kwetsbare personen?		
11.	Worden er met andere partijen dan tot nu toe persoonsgegevens uitgewisseld?		
12.	Krijgen er meer of andere partijen toegang tot verwerkingen van persoonsgegevens?		
13.	Worden er geautomatiseerd beslissingen genomen over betrokkenen op basis van persoonsgegevens?		
14.	Is het mogelijk om op basis van de persoonsgegevens gedrag, prestaties of aanwezigheid van betrokkenen in kaart te brengen of te beoordelen?		
15.	Geeft de verwerking de mogelijkheid tot inzage door de betrokkenen?		
16.	Geeft de verwerking de mogelijkheid tot correctie voor de betrokkenen?		
17.	Geeft de verwerking de mogelijkheid tot het wissen van persoonsgegevens (vergetelheid) voor de betrokkenen?		
18.	Geeft de verwerking de mogelijkheid tot overbrenging van de gegevens naar een ander systeem (dataportabiliteit)?		
19.	Is duidelijk wat de bewaartermijn van de gegevens is?		
20.	Vindt logging en monitoring plaats op de verwerking?		
21.	Is geregeld hoe om te gaan met een datalek?		
22.	Wordt de beveiliging van de persoonsgegevens duidelijk vastgelegd en voldoet deze aan de eisen van de huidige stand van de techniek (bijvoorbeeld 2 factor authenticatie)?		
23.	Als de verwerking bij een andere partij plaatsvindt, is deze aangesloten bij het privacyconvenant?		
24.	Voldoet de andere partij aan de beveiligingseisen die in het privacyconvenant en de verwerkersovereenkomst zijn vastgelegd?		

6. Hoe voer ik een DPIA uit

Een DPIA voer je op hoofdlijnen uit als volgt:

- Bepaal het onderwerp van het DPIA;
- Bepaal wie het DPIA gaat uitvoeren: dat kan één persoon of team zijn. Een team heeft de voorkeur, omdat diverse deelnemers aan het DPIA vanuit hun eigen invalshoek naar de verwerking kunnen kijken.
- Betrek de FG in een vroeg stadium bij het proces;
- Gebruik ter voorbereiding de tabel uit het vorige hoofdstuk;
- Voer het DPIA uit aan de hand van het volgende schema. De vier stappen worden in het volgende hoofdstuk gedetailleerd beschreven.



- Leg alle bevindingen vast in een verslag;
- Vermeld in het verslag wat het advies van de FG is en wat je ermee gedaan hebt.

Als de uitkomst van een DPIA is dat de verwerking een **hoog** risico oplevert en dat je geen risico beperkende maatregelen **kunt** nemen, dan moet je vooraf aan een eventuele verwerking een raapleging aanvragen bij de AP[2]. Deze situatie zal niet snel voorkomen in het onderwijs.

Wanneer je klaar bent met het DPIA en je met de verwerking van persoonsgegevens bent begonnen, moet je bepalen of wat je bedacht hebt ook daadwerkelijk gebeurt. Hiervoor voer je een (onafhankelijke) toets uit op de verwerking aan de hand van het DPIA.

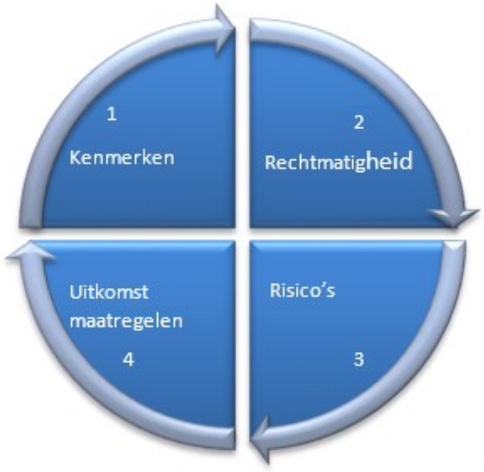
2 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/data-protection-impact-assessment-dpia#publications

6.1. Model voor het uitvoeren van een DPIA

De Rijksoverheid heeft een model gemaakt voor het uitvoeren van een DPIA. Dat model bestaat uit vier stappen waarmee je 17 vragen beantwoordt.

Het maken van een DPIA is een dynamisch proces. Het is mogelijk dat nadat je een stap hebt uitgevoerd, een maatregel invloed heeft op de inschatting van risico's in een eerdere stap. Neem de vrijheid om dan naar die stap terug te gaan en de nodige aanpassingen te maken. Zie het uitvoeren van een DPIA als een dynamisch proces.

1. **Beschrijf de kenmerken van de gegevensverwerkingen:** een beschrijving van de voorgenomen verwerkingen en de verwerkingsdoeleinden;
2. **Beoordeel de rechtmatigheid van de gegevensverwerkingen:** een juridische beoordeling van de feiten zoals de rechtsgrond, de noodzaak, evenredigheid en verenigbaarheid van de voorgenomen verwerkingen in relatie tot de verwerkingsdoeleinden;
3. **Beschrijf en beoordeel de risico's voor de betrokkenen:** een beoordeling van de gevolgen en risico's van de voorgenomen verwerkingen voor de rechten en vrijheden van de betrokkenen;
4. **Beschrijf de voorgenomen maatregelen:** de voorgenomen maatregelen om deze gevolgen en risico's van de voorgenomen verwerkingen aan te pakken.



6.2. Stappen bij het uitvoeren van het DPIA

Bij elke stap van de DPIA beantwoord je een aantal vragen. Het detail van de antwoorden kan meer of minder gedetailleerd zijn afhankelijk van de aard en omvang van de verwerking of aanpassing. Alle antwoorden leg je vast in een verslag. Bijlage 1 bevat een template voor zo'n verslag.

Stap 1: beschrijf de kenmerken van de gegevensverwerkingen

het DPIA is bedoeld en waarom het wordt uitgevoerd. Geef hierbij ook de naam van de organemers aan. Beschrijf op een gestructureerde manier de voorgenomen gegevensverwerkingen, einden, betrokken partijen en dergelijke.

	Onderwerp	Vraag
1.	Voorstel	Beschrijf op hoofdlijnen het voorstel waar het DPIA op toeziet en de context waarbinnen deze plaatsvindt
2.	Persoonsgegevens	Geef per type betrokkene aan welke persoonsgegevens van hen verwerkt worden. Som alle categorieën van persoonsgegevens op die worden verwerkt. Deel deze in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificatienummer
3.	Gegevensverwerkingen	Geef alle voorgenomen gegevensverwerkingen weer
4.	Verwerkingsdoeleinden	Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen
5.	Betrokken partijen	Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens
6.	Belangen bij de gegevensverwerkingen	Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen
7.	Verwerkingslocaties	Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden

8.	Technieken en methoden van de gegevensverwerkingen	Beschrijf op welke wijze en met welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi) geautomatiseerde besluitvorming, profilering of big dataverwerkingen en, zo ja, beschrijf deze specifiek
9.	Juridisch en beleidsmatig kader	Benoem de wet en regelgeving (met uitzondering van de AVG) en het beleid wat relevant is voor de voorgenomen gegevensverwerkingen.
10.	Bewaartermijnen	Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden

Stap 2: beoordeel de rechtmatigheid van de gegevensverwerkingen

Beoordeel de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkenen.

	Onderwerp	Vraag
11.	Rechtsgrond	Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd
12.	Bijzondere persoonsgegevens	Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dit is toegestaan
13.	Doelbinding	Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld
14.	Noodzaak en evenredigheid	Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit. ▪ Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden? ▪ Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt? Benoem hierbij de overwogen alternatieven
15.	Rechten van betrokkenen	Geef aan hoe invulling wordt gegeven aan de rechten van de betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzondering dat is toegestaan

Stap 3: beschrijf en beoordeel de risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen.

	Onderwerp	Vraag
16.	Risico's	Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Ga in ieder geval in op: a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen; 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

Stap 4: beschrijf de voorgenomen maatregelen

Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevensverwerkingen voor de vrijheden en rechten van de betrokkenen aan te pakken.

	Onderwerp	Vraag
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 en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is

6.3. Melding aan de AP

Als de uitkomst van een DPIA is dat de verwerking een **hoog risico** oplevert en dat er geen risico beperkende maatregelen genomen **kunnen** worden, dan moet je vooraf aan een eventuele verwerking een raadpleging aanvragen bij de AP. Deze situatie zal in het onderwijs niet snel voorkomen.

6.4. DPIA en de relatie met het dataregister

Alle verwerkingen van persoonsgegevens die een school uitvoert, moeten worden vastgelegd in een register van verwerkingen. Op basis van dat register kan het bevoegd gezag verantwoording afleggen over de verwerkingen.

De AVG geeft in artikel 30 aan wat een register van verwerkingen minimaal moet bevatten.

Kennisnet heeft voor het onderwijs een verwerkingsregister verrijkt met extra informatie, zoals autorisatiegegevens en een BIV-classificatie op het niveau van de persoonsgegevens. Dit noemen we een **dataregister**. Dit register kan een waardevolle aanvulling zijn bij het uitvoeren van een DPIA. **Bijlage 2** laat bij de beschrijving van de 17 vragen van het DPIA zien waar eventuele gegevens of aanvullende informatie uit het dataregister gehaald kan worden.

Bijlage 1 Template verslag DPIA

Toelichting op het gebruik van dit template

- Je kunt de tabellen hieronder gebruiken voor het vastleggen van de antwoorden op de vragen van het DPIA. De volgorde van de vragen komt overeen met de eerder beschreven stappen. Het geheel vormt het verslag van het DPIA.
- Bij elke stap is in het zwart de toelichting op de stap gegeven. Je kunt zelf besluiten of je die laat staan.
- Om het invullen makkelijker te maken is de lijst gedeeltelijk ingevuld en voorzien van suggesties voor antwoorden.
- Omdat een DPIA alles te maken heeft met risicoanalyse, kun je als naslag goed gebruik maken van de methode die we in de Aanpak IBP beschreven hebben. In het dataregister kun je meer specifieke informatie vinden over reeds ingevulde BIV-waarden, rechten van betrokkenen e.d.
- Verwijder deze toelichting.

DPIA verslag

(hier kun je bijvoorbeeld een logo of naam van de school neerzetten, je kunt dit blok ook verwijderen)

Stap 1 Beschrijf de kenmerken van de gegevensverwerkingen

Toelichting: Geef aan waarvoor het DPIA is bedoeld en waarom het wordt uitgevoerd. Geef hierbij ook de naam van de organisatie en de deelnemers aan. Beschrijf op een gestructureerde manier de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden, betrokken partijen en dergelijke.

Onderwerp van dit DPIA

DPIA voor	Omschrijf op hoofdlijnen waarvoor het DPIA bedoeld is en de context waarbinnen het DPIA wordt uitgevoerd.

Deelnemers DPIA d.d. **<datum>**

Naam	Organisatie	Functie

Te verwerken persoonsgegevens (per categorie betrokkene invullen)

Betrokkenen	Medewerker / tijdelijke medewerker / leerling / ouder / gast
Soort persoonsgegeven	**Gewoon** Niet van toepassing of gegevens zoals bijvoorbeeld: Naam / e-mailadres / opleiding / geboortedatum / geboorteplaats / geslacht / leerlingnummer / personeelsnummer / nationaliteit / gegevens ouders – voogd / examinering / studietraject / begeleiding / aanwezigheid / klas / leerjaar / opleiding / onderwijsorganisatie (rooster, boekenlijst etc.) /werkervaring / financiën / functie / kredietwaardigheid / persoonlijke voorkeuren / loonschaal / verslag functioneringsgesprek / (wan)-gedrag / / kenteken / bankrekeningnummer Maar ook: IP-adres / MAC-adres / KvK nummer / gebruikersnaam / wachtwoord / inloggegevens / communicatiegegevens / locatiegegevens ….
	Bijzonder Niet van toepassing of gegevens Zoals bijvoorbeeld: Medisch dossier / Ras of etnische afkomst / politieke opvattingen / religieuze of le-

	vensbeschouwelijke overtuiging / lidmaatschap vakbond / genetische gegevens / biometrische gegevens / gezondheidsgegevens / seksueel gedrag of seksuele gerichtheid / ….					
	Strafrechtelijk Niet van toepassing of gegevens zoals bijvoorbeeld: Proces-verbaal / strafblad / ….					
	Identificatienummer Niet van toepassing of gegevens zoals bijvoorbeeld: BSN / PGN / ECK-ID …					
BIV-Classificatie	**Beschikbaarheid**		**Integriteit**		**Vertrouwelijkheid**	
Specifieke beveiligings-maatregelen nodig	J / N, namelijk Vb 2 factor authenticatie, token, 4 ogen, …					

Schematische weergave van de verwerking

De verwerking betreft het: Ontvangen / leveren / doorzenden / vastleggen / raadplegen /…. Gebruik ter illustratie hiervoor bijvoorbeeld een workflow, een schema, een tekening of een beschrijving

Technieken en methoden van de gegevensverwerkingen

Bijvoorbeeld ▪ (semi) geautomatiseerde besluitvorming ▪ Profilering ▪ Big data verwerkingen

Betrokken partijen (verwijder overbodig verwerkers)

Extern	Verwerkingsverantwoordelijk	Leerling: DUO / Leerplicht / Schoolinspectie / SWV / Accountant / GGD / CJP / Stage bedrijf / Vervolgonderwijs / Medewerker: Belastingdienst / ABP / UWV / Bank / ARBO / ….
	Verwerker	Leerling: LAS / ELO / Toets / Rooster / CRM / Studiebegeleiding / Zorg en overdracht / Regionale samenwerking / Bibliotheek e.d. / Cloud als Office 365 etc. / Uitgeverijen en distributeurs / … Medewerker: HR / LAS –LVS / MIS / Financiën / ELO / Uitgeverijen en distributeurs/ Cloud als Office 365 etc. / ….
Intern	Interne applicatie	IDM / Netwerk software / Registratie incidenten / Medisch dossier / …..
	Persoon / Groep	Gehele organisatie Leerling adm. / Docent / Mentor / Decaan / IB-er / PR / Financiën / Personeelsadministratie / Applicatie beheer Speciale groep: Netwerk beheer / IT-beheer / Administrators

Gegevens externe verwerkingsverantwoordelijke / verwerker (maak een keuze en per organisatie invullen)

1.	Rol	Verwerkingsverantwoordelijk / verwerker
	Naam	
	Adres	
	Woonplaats	
	Contactpersoon	
	Hoofdvestiging	Nederland / Europa / VS / Buiten Europa geen VS
	Valt onder	AVG / GDPR / Privacy Shield / …
	Verwerking vindt plaats in	Land benomen
	Aangesloten bij Privacy Convenant	J / N
	ISO 27001	J / N
	Overige IBP certificering	….

Doeleinden voor de gegevensverwerking

Zie voor de specifieke bewaartermijnen de Handreiking bewaartermijnen, bijlage met overzicht relevante wet- en regelgeving.

Leerlingen

Verwerkingsdoeleinden	Grondslag (behoort bij stap 2)	Bewaar-termijn
Organiseren of het geven van onderwijs (w.o. onderwijs-overeenkomst)	Wettelijk en overeenkomst	
Berekenen, vastleggen en innen van 'gelden'	Overeenkomst, gerechtvaardigd belang	
Verantwoorden aan DUO, onderwijsinspectie en accountant	Wettelijke verplichting en overeenkomst	
Verstrekken van (digitale) leermiddelen	Wettelijk en overeenkomst	
Begeleiding leerling (pedagogisch dossier) en studieadvies	Overeenkomst, gerechtvaardigd belang	
Onderzoek	Overeenkomst, gerechtvaardigd belang	
Uitvoering of toepassing van een andere wet of taak van algemeen belang	Wettelijk, overeenkomst, publiek rechtelijke taak	
Overig		

Medewerkers (vast of tijdelijk)

Verwerkingsdoeleinden	Grondslag (behoort bij stap 2)	Bewaar-termijn
Komen tot een aanstelling (overeenkomst)	Wettelijke verplichting en overeenkomst	
Voldoen aan wettelijke verplichtingen (belasting, pensioen e.d.)	Wettelijke verplichting	
Organiseren en uitvoeren van de arbeidsovereenkomst (HR, MIS, Financiën etc.)	Overeenkomst, gerechtvaardigd belang	
Regelingen op gebied van secundaire arbeidsvoorwaarden	Overeenkomst	
Berekenen, vastleggen, betalen van salarissen en innen vorderingen	Wettelijke verplichting en Overeenkomst	
Uitvoering of toepassing van een andere wet of taak van algemeen belang	Wettelijke verplichting, Overeenkomst, Publiek rechtelijke taak	
Overig		

Relaties

	Verwerkingsdoeleinden	Grondslag (behoort bij stap 2)	Classificatie B	I	V	Bewaar-termijn
Ouders	OOK (Mede) ondertekenen	Overeenkomst en gerechtvaardigd belang	M	H	M	opt out
Sollicitanten	Toetsen aspirant medewerker	Toestemming	M	H	H	2 jaar of opt out
Alumni	Delen nieuws en aanbod	Gerechtvaardigd belang	M	M	M	Opt out
Belangstellenden	Informeren opleidingsaanbod	Toestemming	M	L	M	2 jaar of opt out
Overig						

Juridisch- en beleidsmatig kader

Benoem de wet en regelgeving (met uitzondering van de AVG) en het beleid dat relevant is voor de voorgenomen gegevensverwerkingen. Zie voor de specifieke bewaartermijnen de Handreiking bewaartermijnen, bijlage met overzicht relevante wet- en regelgeving.

Specifieke wetgeving	Doeleinde	Gegevens	Bewaar-termijn
Voorbeeld Besluit bekostiging WPO	In- Uitschrijving, verzuim	Gegevens in leerlingadministratie	5 jaar

Stap 2 Beoordeel de rechtmatigheid van de gegevensverwerkingen

Beoordeel de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkenen.

Rechtsgrond waarop de verwerking is gebaseerd

Zie hiervoor het schema stap 1 bij "verwerkingsdoeleinden per categorie betrokkene"

Bijzondere persoonsgegevens (alleen invullen als daarvan sprake is)

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Beoordeel bij verwerking van een wettelijk identificatienummer of dit is toegestaan.

Worden er bijzondere of strafrechtelijke persoonsgegevens verwerkt of een wettelijk identificatienummer?	J / N
Categorie bijzonder persoonsgegeven	**Beoordeling**
Bijzonder (Zie opsomming onder stap 1)	
Strafrechtelijk (Zie opsomming onder stap 1.)	
Identificatienummer (Zie opsomming onder stap 1)	

Wijziging van verwerkingsdoel

Indien de persoonsgegevens voor een ander doel worden verwerkt dan waarvoor ze oorspronkelijk verzameld zijn, beoordeel dan of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld

Is er sprake van wijziging van het doel van het verzamelen van persoonsgegevens?	J / N
Persoonsgegeven	Toelichting gewijzigd doel en toelichting nieuwe doelbinding en grondslag
Persoonsgegeven (zie opsomming onder stap 1)	(zie hiervoor stap 1 voor een overzicht per categorie betrokkene)

Beoordeling noodzaak en evenredigheid

Proportionaliteit	Staat de inbreuk op de privacy van betrokkenen in verhouding tot de noodzaak tot verwerking van het gegeven	J / N
	Licht toe	
Subsidiariteit	Kan het verwerkingsdoel niet op een andere minder belastende manier worden verwezenlijkt	J / N
	Licht toe	

Borging van rechten van de betrokkenen

Geef aan hoe invulling wordt gegeven aan de rechten van de betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzondering dat is toegestaan.

Recht op/van	J/N	Toelichting
Inzage		
Correctie		
Wissing (vergetelheid)		
Beperking van de verwerking		
Kennisgeving inzake rectificatie, wissing of beperking		
Dataportabiliteit (overdraagbaarheid)		
Bezwaar		

Stap 3 Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen.

Gecombineerd met

Stap 4 Beschrijving voorgenomen maatregelen

Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevensverwerkingen voor vrijheden en rechten van betrokkenen aan te pakken.

Mogelijke risico's (per risico omschrijven en voorzien van een nummer/identificatie in je eigen administratie)

Risico omschrijving		Nummer <1> omschrijving				
Risico eigenaar/verantwoordelijke						
Negatieve gevolgen rechten en vrijheden van betrokkenen						
Oorsprong van deze gevolgen						
Omschrijf de kans (waarschijnlijk)						
Omschrijf de impact (ernst)						
Kans (waarschijnlijkheid)	waarde	Impact	waarde	Risicowaarde = kans x impact		waarde
Mogelijke maatregelen						
Technisch						
Autorisaties						
Organisatorisch						
Restrisico		Nummer <1A> omschrijving				
Kans (waarschijnlijkheid)	waarde	Impact	waarde	Risicowaarde = kans x impact		waarde
Restrisico aanvaarden?		J / N	Akkoord risico eigenaar		d.d.	<datum>
Restrisico aanvaarden?		J / N	Akkoord bevoegd gezag		d.d.	<datum>

Bijlage 2 Template verslag DPIA in relatie met het dataregister

Artikel 30 van de AVG geeft aan wat een register van verwerkingen *minimaal* moet bevatten. Voor de duidelijkheid zijn de afzonderlijke onderdelen in het overzicht met een kleur aangegeven.
Het dataregister bevat alle onderdelen die een register van de verwerkingsactiviteiten moet bevatten. Daarnaast is het aangevuld met o.a. het onderdeel autorisatie en een BIV-classificatie op het niveau van de persoonsgegevens. Hiermee is het dataregister een waardevol document bij het uitvoeren van een DPIA.
Huidige verwerkingen, gebruikte categorieën persoonsgegevens, verwerkingsdoeleinden et cetera kunnen van pas komen bij het doen van een DPIA.

	Onderdelen artikel 30 AVG
A	Contactgegevens van de instelling
B	Beschrijving van de categorieën: Leerlingen/studenten, medewerkers, etc.
C	Verwerkingsdoeleinden
D	Beschrijving van categorieën van persoonsgegevens
E	Brondocumenten.
F	Categorieën van ontvangers aan wie de persoonsgegevens zijn of worden verstrekt (intern / extern).
G	Gegevens van verwerkers (s)
H	Of er sprake is van doorgifte van de persoonsgegevens buiten de EU.
I	Van toepassing zijnde bewaar- en vernietigtermijnen van de persoonsgegevens.
J	Algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Deze bijlage is dan ook geschikt voor degene die al een start hebben gemaakt met het dataregister. De opbouw is hetzelfde als bijlage 1 en laat bij de 17 punten van het model DPIA zien waar gegevens of aanvullende informatie uit het dataregister gehaald kan worden. De kleuren en letteraanduidingen komen 1 op 1 overeen.

LET OP: De keuze tussen het gebruiken van de template uit bijlage 1 of bijlage 2 is aan de onderwijsinstelling.

Toelichting op het gebruik van bijlage 2

- Je kunt de tabellen hieronder gebruiken voor het vastleggen van de uitkomsten van de vragen van het DPIA. De volgorde van de vragen komt overeen met de eerder beschreven vier stappen.
- Het geheel vormt het verslag van het DPIA. Je geeft erin aan dat het DPIA is uitgevoerd, hoe en waarom dat gedaan is en wat het resultaat is.
- *De schuingedrukte tekst is een algemene aanvulling of voorbeeld. Verwijder na afloop deze tekst.*
- Gebruik losse tabellen voor het vastleggen van de uitkomsten van de vragen van het DPIA.
- De gekleurde vlakken en letters komen overeen met de kleuren en letters uit het dataregister, hiermee kun je eerder vastgelegde informatie gebruiken als ondersteuning bij het beantwoorden van de vragen.
- Verwijder overbodige informatie en vul gevraagde informatie in of aan.
- Verwijder deze toelichting en plaats eventueel een logo boven stap 1.

Een DPIA heeft alles te maken met risicoanalyse. Als naslag voor een risicoanalyse kan gebruik gemaakt worden van de methode die in de Aanpak IBP beschreven is.

LOGO

Stap 1: Beschrijf de kenmerken van de gegevensverwerkingen

Toelichting: Geef aan waarvoor het DPIA is bedoeld en waarom het wordt uitgevoerd. Geef hierbij ook de naam van de organisatie en de deelnemers aan. Beschrijf op een gestructureerde manier de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden, betrokken partijen en dergelijke.

1 Voorstel *Omschrijf waarvoor het DPIA is bedoeld en waarom het DPIA wordt uitgevoerd. Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkings-doeleinden en de belangen bij de gegevensverwerkingen. Geef aan wie de verwerkingsverantwoordelijke, de eventuele verwerker en de 'hoofdgebruiker'/functioneel beheer-der is.*	
DPIA voor	

1 Deelnemers DPIA d.d. <datum> *Geef aan wie er bij het DPIA betrokken zijn geweest*		
Naam	**Organisatie**	**Functie**

2 Persoonsgegevens

Geef per categorie betrokkene aan welke persoonsgegevens van hen verwerkt worden. Som alle categorieën van persoonsgegevens op die worden verwerkt. Deel persoonsgegevens in naar de typen: gewoon (G), bijzonder (B), strafrechtelijk (S) en wettelijk identificatienummer (I). Geef de uitkomst van de BIV-classificatie aan en de eventuele aanvullende beveiligingsmaatregelen.
Vul de bewaartermijnen in vanuit 10

(zie dataregister D, en I)

Categorieën per-soonsgegevens	Betrokkenen (zie dataregister)	G/B/S/I *	Bewaartermijn (zie 10)	B I V (L-M-H)	Specifieke beveiligingsmaatregelen op basis van de BIV Ja / Nee	G/B/S/I * G= gewoon B= bijzonder S= strafrechtelijk I= identificatie nr.

3 Gegevensverwerkingen

Geef in een workflow aan hoe de persoonsgegevens worden verwerkt. (Benoem daarbij eventueel de verwerkingen zoals ontvangen, leveren, doorzenden, vastleggen et cetera en eventueel de daarbij gebruikte technieken.)

4 Verwerkingsdoeleinden *Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen. Geef om het overzichtelijk te maken ook de resultaten van vraag 11 en 13 aan. (Geef ook de categorie van betrokkenen aan en de categorieën van persoonsgegevens).*						(zie dataregister C en D)
Categorieën persoonsgegevens	**Betrokkenen (zie dataregister)**	**Verwerkingsdoeleinden**	**Grondslag (11)** W / O / GB / T / P**	**Verwerking *** O / L / D / V / R**	**Verwerking voor ander doel (13)**	**Opmerkingen / aanvullingen**

** Grondslagen voor de verwerking (11):	*** Verwerking heeft in ieder geval betrekking op:
W = Wettelijk	O = Ontvangen
O = Overeenkomst	L = Leveren
GB = Gerechtvaardigd belang	D = Doorzenden
T = Toestemming	V = Vastleggen/ opslaan
P = Publiekrechtelijke taak	R = Raadplegen

5. Betrokken partijen *Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.(Dit kan ook de eigen organisatie zijn) .*					(zie dataregister F, G, en X)
Gegevensverwerking	**Verwerkingsverantwoordelijken**	**Verwerkers**	**Wie hebben toegang**	**Interne applicatie**	**Interne rollen / gebruikers**

6. Belangen bij de gegevensverwerkingen

Beschrijf alle belangen die de verwerkingsverantwoordelijke en andere partijen hebben bij de voorgenomen gegevensverwerkingen. Het is voldoende om aan te geven wat op hoofdlijnen de belangen zijn om persoonsgegevens te delen.

7. Verwerkingslocaties

(zie dataregister F, G, en H)

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden. Geef informatie over hoofdvestiging, website. Aanvullende informatie over aansluiting bij Privacy Shield, Convenant en eventuele certificeringen kunnen van toegevoegde waarde zijn bij onderbouwing van de besluitvorming.

VV	V	Naam	Website	Hoofdvestiging	AVG / Privacy Shield	Convenant J / N	ISO 27001 J / N	Overige certificering	Datum

8. Technieken en methoden van de gegevensverwerking

Beschrijf op welke wijze en met welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi) geautomatiseerde besluitvorming, profilering of big dataverwerkingen en, zo ja, beschrijf deze specifiek

Gebruikte technische middelen en methoden		Beschrijving

Wordt er gebruik gemaakt van:	Ja / Nee	Indien ja, beschrijf deze dan specifiek
(semi) geautomatiseerde besluitvorming		
profilering		
Big-data verwerkingen		

9. Juridisch en beleidsmatig kader *Benoem de wet en regelgeving (met uitzondering van de AVG) en het beleid wat relevant is voor de voorgenomen gegevensverwerkingen.*	*Denk aan de AWR (Algemene Wet inzake Rijksbelastingen), BW (Burgerlijk Wetboek) in het kader van de jaarrekening, Archiefwet, WHW (Wet op het Hoger onderwijs en Wetenschappelijk onderzoek), WEB (Wet Educatie en Beroepsonderwijs), etc. Maar denk ook aan intern vastgelegde afspraken in het IBP-beleid.*

10. Bewaartermijnen *Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.* ***Bewaartermijnen conform handreiking bewaartermijnen zie 2***	**(zie dataregister I)**

Stap 2: Beoordeel de rechtmatigheid van de gegevensverwerkingen

Toelichting: Beoordeel de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkenen.

11. Rechtsgrond *Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd*		**(zie dataregister)**
Verwerkingsdoeleinden	**Grondslagen**	
Zie punt 4 bij stap 1 ***Zie dataregisters van betrokkenen voor vastgestelde verwerkingsdoeleinden***	**Zie punt 4 bij stap 1** ***Zie dataregisters van betrokkenen voor bijbehorende grondslagen***	

12. Bijzondere persoonsgegevens *Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel dan of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dit is toegestaan.* *Alleen invullen indien daarvan sprake is.*		**(zie dataregister D)**
Categorie bijzondere persoonsgegevens	**Beoordeling**	**Opmerkingen/aanvullingen**
Strafrechtelijk		
Identificatienummer		

13. Doelbinding *Indien de persoonsgegevens voor een ander doel worden verwerkt dan waarvoor ze oorspronkelijk verzameld zijn, beoordeel dan of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.*	**(zie dataregister C)**
Persoonsgegeven	**Toelichting gewijzigd doel en toelichting nieuwe doelbinding en grondslag**

14. Beoordeling noodzaak en evenredigheid *Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor en in verhouding staan met de te behalen doelen. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.*		
Proportionaliteit	***Staat de inbreuk op de privacy van betrokkenen in verhouding tot de noodzaak tot verwerking van het gegeven?***	**J / N**
	Toelichting:	
Subsidiariteit	***Kan het verwerkingsdoel niet op een andere minder belastende manier worden verwezenlijkt?***	**J / N**
	Toelichting:	

15. Rechten van betrokkenen *Geef aan hoe invulling wordt gegeven aan de rechten van de betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzondering dat is toegestaan*		
Recht op/van	**J / N**	**Toelichting**
Recht op inzage		
Recht op correctie		
Recht op wissen (vergetelheid)		
Recht op beperking van de verwerking		
Recht op kennisgeving inzake rectificatie, wissen of beperking		
Recht op dataportabiliteit (overdraagbaarheid)		
Recht van bezwaar		

Beschrijf en beoordeel de risico's voor de betrokkenen

ijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de ext en doelen van de voorgenomen gegevensverwerkingen.

16. Mogelijke risico's (per risico omschrijven) *Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen.*						
Risico omschrijving		Nummer <1> omschrijving				
Risico eigenaar/verwerkingsverantwoordelijke						
Negatieve gevolgen rechten en vrijheden van betrokkenen						
Oorsprong van deze gevolgen						
Omschrijf de kans (waarschijnlijk)						
Omschrijf de impact (ernst)						
Kans (waarschijnlijkheid)	waarde	Impact	waarde	Risicowaarde = kans x impact	waarde	
Mogelijke maatregelen						
Technisch						
Autorisaties						
Organisatorisch						
Restrisico		Nummer <1A> omschrijving				
Kans (waarschijnlijkheid)	waarde	Impact	waarde	Risicowaarde = kans x impact	waarde	
Restrisico aanvaarden?		J / N	Akkoord risico eigenaar	d.d.	<datum>	
Restrisico aanvaarden?		J / N	Akkoord bevoegd gezag	d.d.	<datum>	

Stap 4: Beschrijf de voorgenomen maatregelen

Toelichting: Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevensverwerkingen voor de vrijheden en rechten van de betrokkenen aan te pakken.

17. Maatregelen beschrijven *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 en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is* *Autorisatie is toegevoegd op basis van functies en rollen. Vastgelegd is welke persoonsgegevens in interne specifieke documenten en applicaties worden vastgelegd en een BIV-classificatie is gemaakt op het niveau van de categorieën van persoonsgegevens. Deze BIV-classificatie is leidend voor de technische maatregelen die genomen moeten worden.* *Voorbeeld: als de vertrouwelijkheid 'hoog' wordt geclassificeerd zijn aanvullende beveiligingsmaatregelen nodig (bijvoorbeeld bij bijzondere persoonsgegevens).*			**(zie dataregister J, X en BIV)**
Technische en organisatorische maatregelen	**Autorisatie**	**BIV – classificatie L – M - H**	**Opmerkingen / aanvullingen**