REGIEGROEP IBP IN HET MBO
Kennisnet SURF saMBO-ICT

PO RAAD

VO RAAD

Kennisnet SIVON

Handleiding en model Data Protection Impact Assessment (DPIA)

Uitleg over gegevensbeschermingseffectbeoordeling in het po en mbo

Laat ict werken **voor het onderwijs**

Inhoud

1. INLEIDING 3

2. MANAGEMENTSAMENVATTING 5

3. WAT ZEGT DE AVG OVER DE DPIA? 7
   - 3.1. Wat is een DPIA? 7
   - 3.2. Wie voert de DPIA uit? 7
   - 3.3. Welke hulpmiddelen zijn beschikbaar bij de uitvoering van de DPIA? 8
   - 3.4. Wanneer wordt een DPIA uitgevoerd? 8
   - 3.5. Waaruit moet een DPIA bestaan? 9
   - 3.6. Eindresultaat 10
   - 3.7. Proces- of systeemniveau 10
   - 3.8. Evaluatie DPIA 10

4. STAPPENPLAN DPIA 12
   - 4.1. Fasering: gegevensverwerkingsanalyse en DPIA 12
   - 4.2. Gegevensverwerkingsanalyse 12
   - 4.2.1. Onderdelen gegevensverwerkingsanalyse 13
   - 4.3. Risicoanalyse DPIA 13
   - 4.3.1. Onderdelen van de DPIA 13
   - 4.3.2. DPIA-rapportage: uitgebreide en gewogen risicoanalyse 14
   - 4.3.3. Risico's inventariseren 14
   - 4.3.4. Risico's wegen: kans x impact = risico 15
   - 4.3.5. Uitkomst 16
   - 4.3.6. Goedkeuring van de DPIA-rapportage 16
   - 4.4. Herbeoordeling van de DPIA 16

BIJLAGE 1 VRAGENLIJST GEGEVENSVERWERKINGSANALYSE 17

BIJLAGE 2 VRAGENLIJST RISICOANALYSE DPIA 27

Colofon

Versie 0.99 (12 november 2020)

Bronnen Handreiking DPIA in het mbo (Regiegroep ibp mbo, IBPDOC38)
Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA)
Modelaanpak DPIA Zadkine

Geschreven en bewerkt door
saMBO-ICT / SURF / Kennisnet SIVON

Auteurs Leo Bakker (Kennisnet), Martijn Bijleveld (saMBO-ICT), Bram Bogers (Onderwijsgroep Tilburg), Bart Bosma (SURF), Willem Flink (Hoornbeeck College), Dirk Linden (Kennisnet), Job Vos (SIVON), Chris Zintel (Kennisnet)

Met dank aan Onderwijsgroep Tilburg en Zadkine voor het beschikbaar stellen van voorbeelddocumenten

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

1. Inleiding

In 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht geworden. Zoals iedere privacywet gaat deze Europese privacywet over de bescherming van gegevens van personen. Hierbij is het de bedoeling van de wetgever dat de AVG regels en garanties geeft om het vrije verkeer van die persoonsgegevens mogelijk te maken, binnen Europa en daarbuiten. Privacy als kans en mogelijkheid in plaats van als beperking. De verwerking van persoonsgegevens moet ten dienste staan van de mens die zijn eigen of andermans gegevens wil gebruiken.

Technologie heeft zowel de economie als het maatschappelijk leven ingrijpend veranderd. Dat is ook terug te zien in het onderwijs, dat in de afgelopen decennia steeds meer en beter gebruikmaakt van ict. Door snelle technologische ontwikkelingen en globalisering zijn ook nieuwe uitdagingen ontstaan voor de bescherming van persoonsgegevens. In de AVG is daarmee rekening gehouden: de wet heeft wereldwijde gelding en is technologieneutraal.

De AVG zorgt voor een hoog niveau van bescherming van de privacy van burgers door uit te gaan van de aard, omvang en risico's van het gebruik van persoonsgegevens. Organisaties en bedrijven die persoonsgegevens willen gebruiken, zijn verplicht om 'passende en effectieve maatregelen' te nemen en moeten kunnen aantonen dat elk gebruik van persoonsgegevens in overeenstemming met de AVG plaatsvindt. Zij moeten rekening houden met de aard, omvang, context en doeleinden van de verwerking én het risico voor de privacy (rechten en vrijheden) van burgers. Daarbij wegen de waarschijnlijkheid en de ernst van het risico voor de betrokken personen mee. Hierdoor wordt een breed spectrum van het gebruik van persoonsgegevens mogelijk, zonder dat de AVG een waslijst aan regels geeft onder welke omstandigheden het gebruik van persoonsgegevens al dan niet is toegestaan. Zolang een organisatie of bedrijf aantoont dat het gebruik van persoonsgegevens binnen de algemene kaders van de AVG past, dat de privacy van de betrokken personen gegarandeerd is en dat de risico's zijn beoordeeld en beperkt zijn (of dat maatregelen genomen worden om die risico's te beperken), is dat gebruik toegestaan.

De AVG stoelt voor een groot deel op een risico-gebaseerde insteek. In een aantal gevallen schrijft de wet zelfs een risicoweging voor. Daarbij is de organisatie verplicht om te beoordelen wat het effect is van het gebruik van persoonsgegevens op de privacy van de betrokken personen. Dit proces wordt een gegevensbeschermingseffectbeoordeling genoemd, in het Engels een Data Protection Impact Assessment (DPIA).

De DPIA geeft een risicobeoordeling van het gebruik van persoonsgegevens en laat zien of (en zo ja, welke) maatregelen genomen moeten worden om de privacy van de betrokken personen te beschermen. **Deze handleiding beschrijft specifiek voor onderwijsinstellingen in Nederland hoe zij met deze risicobeoordeling moeten omgaan en hoe zij een DPIA moeten uitvoeren.** In deze handleiding is een model-DPIA opgenomen. Hierbij is niet alleen naar de AVG gekeken, maar ook naar de onderwijswetgeving en hoe informatiebeveiliging en privacy (IBP) in het onderwijs geregeld en georganiseerd worden. Om deze handleiding te lezen en toe te passen, wordt enige basiskennis van privacy en de AVG verondersteld. Meer informatie over de AVG is te vinden op de website van de Aanpak IBP (https://kn.nu/IBPonderwijs) en in het Framework IBP in het middelbaar beroepsonderwijs (mbo) (https://www.sambo-ict.nl/framework).

Om te kunnen beoordelen of de onderwijsinstelling een DPIA moet uitvoeren, is informatie nodig over het type en de aard van de te gebruiken persoonsgegevens en de software die ze daarvoor inzet. Het proces om deze informatie te verkrijgen wordt in deze aanpak de **gegevensverwerkingsanalyse** genoemd. Een dergelijke analyse heet in andere publicaties ook weleens pre-DPIA of pre-PIA, maar omdat die term dan net iets anders betekent, wordt deze, om misverstanden te voorkomen, hier bewust niet gebruikt.

De gegevensverwerkingsanalyse maakt op een gestructureerde wijze inzichtelijk welke processen worden onderzocht, welke systemen daarbij betrokken zijn, welke gegevens worden verwerkt en hoe deze gegevens zijn geclassificeerd. Vervolgens wordt op basis van door de toezichthouder geformuleerde criteria beoordeeld of het

nodig is om een DPIA uit te voeren. De gegevensverwerkingsanalyse kan dus als resultaat hebben dat er geen DPIA hoeft te worden uitgevoerd en vormt dan de onderbouwing van die conclusie. Wanneer de uitkomst is dat er wel een DPIA vereist is, wordt de gegevensverwerkingsanalyse onderdeel van de DPIA.

De basis voor de gegevensverwerkingsanalyse zijn de procesbeschrijvingen: welke processen, functies, systemen en gegevens maken deel uit van de te onderzoeken verwerking? Onderwijsinstellingen kunnen daarbij gebruikmaken van een referentiearchitectuur. Voor het primair en voortgezet onderwijs (po/vo) is dat de FORA (Funderend Onderwijs Referentie Architectuur)[1], en voor het middelbaar beroepsonderwijs (mbo) zijn dat de uniforme procesbeschrijvingen van Route21.[2]

Het uiteindelijke doel is dat een onderwijsinstelling met het instrument van de gegevensverwerkingsanalyse en de DPIA op een veilige en verantwoorde wijze gebruik kan maken van de persoonsgegevens van onderwijsdeelnemers en medewerkers, binnen de kaders van de AVG.

[1] https://www.wikixl.nl/wiki/fora/index.php/Hoofdpagina
[2] https://www.sambo-ict.nl/route21/ en https://www.sambo-ict.nl/wp-content/uploads/2020/09/Hoofdprocesmodel-Route21-v1.2.pdf

2. Managementsamenvatting

Onderwijsinstellingen maken steeds beter en meer gebruik van ict. Daardoor neemt het aantal persoonsgegevens[3] dat scholen gebruiken toe. De bescherming van de privacy van onderwijsdeelnemers en medewerkers wordt daarom steeds belangrijker. De besturen van de onderwijsinstellingen zijn volgens de wet verplicht om privacy goed te regelen en te beschermen. Hiervoor moeten zij passende maatregelen nemen.

De Algemene Verordening Gegevensbescherming (AVG) verplicht organisaties zoals onderwijsinstellingen om te onderzoeken welk effect de verwerking[4] van persoonsgegevens heeft op de privacy van onderwijsdeelnemers en medewerkers. Dit onderzoek wordt een gegevensbeschermingseffectbeoordeling genoemd. In Nederland wordt vaak de Engelse benaming gebruikt: Data Protection Impact Assessment of DPIA. Het is een instrument om vooraf de privacyrisico's van gegevensverwerking in kaart te brengen, om daarna maatregelen te kunnen nemen om die risico's te verkleinen. De DPIA geeft inzicht in de risico's die de verwerking van persoonsgegevens binnen de onderwijsinstelling oplevert.

Een DPIA is verplicht als de verwerking van persoonsgegevens − gelet op de aard, omvang, context en doeleinden van die verwerking − een waarschijnlijk hoog risico inhoudt voor de privacy van onderwijsdeelnemers en medewerkers. De onderwijsinstelling beoordeelt dan door middel van zo'n DPIA vooraf het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Dat is bijvoorbeeld aan de orde bij de aanschaf van nieuwe software of de uitvoering van een grote update van bestaande software.

De functionaris voor gegevensbescherming (FG) van de onderwijsinstelling adviseert over de noodzaak van de DPIA en is altijd betrokken bij de beoordeling ervan. De DPIA wordt vaak uitgevoerd door de ict-coördinator, informatiemanager, privacy officer en/of IBP-manager.

De DPIA is verplicht in een aantal in de AVG genoemde gevallen, zoals bij de evaluatie of scoretoekenning, de stelselmatige monitoring of het op grote schaal verwerken van persoonsgegevens van alle betrokken personen. In ieder geval gaat het om verwerkingen die een (hoog) risico kunnen opleveren voor onderwijsdeelnemers of medewerkers. Bijvoorbeeld de aanschaf of update van de administratie van de onderwijsinstelling, het leerlingvolgsysteem of het studentinformatiesysteem (SIS). De Autoriteit Persoonsgegevens heeft een lijst[5] van verwerkingen gepubliceerd in welke gevallen een DPIA verplicht is.

Het DPIA-proces omvat twee stappen:

1. De eerste stap is de **gegevensverwerkingsanalyse**: een systematische beschrijving van welke processen worden onderzocht, welke systemen daarbij betrokken zijn, welke gegevens worden verwerkt en hoe deze gegevens zijn geclassificeerd. Daarbij wordt ook ingegaan op het doel en de grondslag van de verwerking en de eventuele betrokkenheid van andere partijen, zoals leveranciers. Het gaat om een feitelijke rapportage en analyse. Vervolgens wordt op basis van richtlijnen van de toezichthouder bepaald of de organisatie een DPIA moet uitvoeren. Mocht een DPIA niet nodig zijn, dan is dat hiermee een weloverwogen en gemotiveerd besluit.
2. De **DPIA** geeft van het bij 1 uitgewerkte gegevensverwerkende proces een oordeel over de rechtmatigheid, evenredigheid en noodzaak van de gegevensverwerking. Vervolgens worden de risico's en te nemen maatregelen beschreven, inclusief een inschatting van de restrisico's.

De FG van de onderwijsinstelling adviseert over de uitvoering van de DPIA. Het bestuur verleent goedkeuring als de DPIA is uitgevoerd. Als er geen hoge risico's zijn gevonden, of als deze al tijdens het proces gemitigeerd zijn, kan de onderwijsinstelling starten met de betreffende gegevensverwerking. In veel gevallen zijn er echter hoge risico's benoemd, waarvoor maatregelen zijn beschreven. Goedkeuring van de DPIA houdt dan in dat de

[3] Alle gegevens waarmee direct of indirect een natuurlijk persoon (mens) kan worden geïdentificeerd. Het kan bijvoorbeeld gaan om een naam, BSN, geboortedatum, telefoonnummer of IP-adres.
[4] Alles wat er met persoonsgegevens wordt gedaan, wordt in de wet 'verwerken' genoemd. Verwerken is dus onder meer: online en offline persoonsgegevens verzamelen, kopiëren, opslaan, verspreiden, publiceren, delen én uitwisselen. Het maakt dus niet uit wat men doet met persoonsgegevens: alles heet 'verwerken' en valt onder de wettelijke bescherming.
[5] Zie: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667

onderwijsinstelling die mitigerende maatregelen binnen redelijke termijn (afhankelijk van de hoogte van het risico) moet uitvoeren. Het bestuur besluit of er intussen gestart kan worden met de gegevensverwerking.

Het is belangrijk om het proces of de software waarop een DPIA is uitgevoerd, regelmatig opnieuw te beoordelen. Dat moet in ieder geval bij wijzigingen in het verwerkingsproces of de gebruikte technologie. Maar ook als er ogenschijnlijk niets is veranderd, moet eens in de twee tot drie jaar gecontroleerd worden of de uitkomsten van de DPIA nog actueel zijn.

3. Wat zegt de AVG over de DPIA?

De AVG verplicht organisaties zoals onderwijsinstellingen om te onderzoeken wat het effect is van de verwerking van persoonsgegevens op de privacy van onderwijsdeelnemers en medewerkers. Dit onderzoek wordt een gegevensbeschermingseffectbeoordeling genoemd. In Nederland wordt vaak de Engelse benaming gebruikt: Data Protection Impact Assessment of DPIA.

3.1. Wat is een DPIA?

De DPIA is beschreven in artikel 35 van de AVG. Daar staat wat de DPIA is en wanneer deze verplicht is. Artikel 36 van de AVG beschrijft in welke gevallen de onderwijsinstelling verplicht is om, op basis van de uitkomsten van de DPIA, contact op te nemen met de Autoriteit Persoonsgegevens (AP; de privacytoezichthouder in Nederland).

De DPIA geeft inzicht in de risico's die de verwerking van persoonsgegevens binnen de onderwijsinstelling oplevert. De DPIA is dus een analyse van de kans dat een risico of bedreiging werkelijkheid wordt, wat de gevolgen hiervan zijn en welke maatregelen de onderwijsinstelling heeft genomen en nog kan nemen om privacyschending te voorkomen.

Het DPIA-proces omvat twee stappen:

1. Gegevensverwerkingsanalyse
2. Risicoanalyse DPIA

Bij de gegevensverwerkingsanalyse worden alle gegevens over de verwerking verzameld, zoals doel, grondslag, categorieën betrokken personen en persoonsgegevens, betrokken (andere) partijen en leveranciers. Het gaat hier om een feitelijke rapportage en analyse. Vervolgens wordt aan de hand van een globale risico-inschatting, op basis van door de toezichthouder geformuleerde criteria, bepaald of de onderwijsinstelling een DPIA moet uitvoeren. Als dit leidt tot de conclusie dat een DPIA niet nodig is, moet dat goed beargumenteerd worden vastgelegd.

Is een DPIA nodig, dan vormt de reeds uitgevoerde gegevensverwerkingsanalyse het startpunt. Deze analyse levert de volgende informatie op:

- Beschrijving van het verwerkingsproces
- Wie bij het proces betrokken zijn
- Oordeel over de rechtmatigheid, evenredigheid en noodzakelijkheid van het proces

De risicoanalyse DPIA beschrijft:

- Risico's voor de betrokkenen
- Maatregelen die moeten worden genomen
- Inschatting van eventuele restrisico's

3.2. Wie voert de DPIA uit?

De uitvoering van een DPIA valt onder de verantwoordelijkheid van het bestuur van de onderwijsinstelling (schoolbestuur, college van bestuur (cvb)). De DPIA raakt altijd een groot deel van de organisatie.

De volgende functies/rollen zijn betrokken bij de uitvoering van de gegevensverwerkingsanalyse en DPIA:

- Bestuur: het schoolbestuur of cvb is opdrachtgever en verwerkingsverantwoordelijke (AVG). Het is cruciaal om het opdrachtgeverschap voor de DPIA op het hoogste niveau te beleggen, omdat een DPIA geen vrijblijvend enquête-instrument is: de gevonden hoge risico's moeten binnen de kortst mogelijke tijd worden teruggebracht tot een aanvaardbaar niveau.
- Privacy officer/IBP-manager: deze voert de DPIA uit.
- Procesverantwoordelijke(n): dit zijn de medewerkers die betrokken zijn of worden bij de verwerking van persoonsgegevens waarvoor de DPIA uitgevoerd wordt (bijvoorbeeld de applicatiebeheerder,

het hoofd van de administratie). Zij zijn de ervaringsdeskundigen, bezitten inhoudelijke expertise en werken mee aan vervolgmaatregelen.
- IBP-/informatiemanager/projectleider/ict-coördinator: deze coördineert de vervolgmaatregelen.
- FG: de functionaris voor gegevensbescherming adviseert over de noodzaak en de uitvoering van de DPIA en beoordeelt de kwaliteit van de DPIA.

In de praktijk worden er vaak DPIA-workshops georganiseerd. Zeker als de scope van de DPIA nog niet volledig helder is of als niet zeker is of de organisatie daadwerkelijk volgens de beschreven processen werkt, is het verstandig om te kiezen voor een aanpak met DPIA-workshops. Een groep ervaringsdeskundigen − medewerkers die de werkzaamheden uitvoeren – gaat in gesprek over het betreffende proces, de gegevensstromen, de verwerkte gegevens en het doel daarvan. Vervolgens benoemt en classificeert de groep de risico's. Medewerkers die goed in staat zijn om risico's te identificeren, kunnen deze niet altijd ook goed classificeren en vice versa. Het is daarom belangrijk te zorgen voor een groep deskundigen met voldoende diversiteit.

De AVG kent de mogelijkheid om betrokkenen (onderwijsdeelnemers en/of medewerkers) te consulteren bij de uitvoering van de DPIA.

3.3. Welke hulpmiddelen zijn beschikbaar bij de uitvoering van de DPIA?

In de eerste plaats vormt deze gestandaardiseerde aanpak voor de uitvoering van de DPIA een praktisch hulpmiddel om stap voor stap de benodigde informatie te verzamelen. Daarnaast maakt deze aanpak het mogelijk dat instellingen DPIA's met elkaar uitwisselen, zodat niet elke instelling zelf het wiel hoeft uit te vinden. De verwachting is dat voor de meeste onderwijsapplicaties 80 procent van de beschrijvingen en analyses overgenomen kan worden. Onderwijsinstellingen in het po en vo kunnen uitgevoerde DPIA's met elkaar delen via het Netwerk Informatiebeveiliging en Privacy PO/VO.

Meer informatie over door mbo-instellingen uitgevoerde DPIA's komt beschikbaar op de website van saMBO-ICT.

Verder kunnen onderwijsinstellingen voor de beschrijvingen van het te onderzoeken proces, de applicaties en de verwerkte gegevens, inclusief de classificatie hiervan, gebruikmaken van een referentiearchitectuur. Voor het po/vo is dat de FORA[6], voor het mbo biedt Route21[7] (de opvolger van Triple A) gestandaardiseerde beschrijvingen.

In de bijlage van deze handleiding zijn de vragenlijsten gegevensverwerkingsanalyse en risicoanalyse DPIA opgenomen.

3.4. Wanneer wordt een DPIA uitgevoerd?

De beoordeling of een DPIA gewenst is, vindt plaats voordat een nieuwe verwerking van persoonsgegevens gaat starten of wanneer veranderingen binnen of buiten de onderwijsinstelling een grote impact hebben op bestaande gegevensverwerkingen.

De uitvoering van een DPIA is verplicht als een verwerking door de onderwijsinstelling een mogelijk hoog risico inhoudt voor de privacy van de betrokken personen. Dit wordt beoordeeld aan de hand van de aard, omvang, context en doeleinden van de verwerking. De onderwijsinstelling weegt deze gegevens en onderzoekt wat het effect van de beoogde verwerking is op de bescherming van persoonsgegevens. Dit is bijvoorbeeld aan de orde bij de uitwisseling van persoonsgegevens met een nieuwe organisatie of leverancier.

De AVG noemt voorbeelden van verwerkingen die een hoog risico met zich meebrengen, zoals evaluaties of scoretoekenningen, de stelselmatige monitoring en vastlegging van de observaties in een geautomatiseerd systeem of administratie, de verwerking van gegevens op grote schaal, geautomatiseerde besluitvorming of het nemen van beslissingen op basis van profielen (profiling), de grootschalige verwerking van bijzondere

[6] https://www.wikixl.nl/wiki/fora/index.php/Hoofdpagina
[7] https://www.sambo-ict.nl/route21/

categorieën van persoonsgegevens (zoals gezondheidsgegevens), de stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten (bijvoorbeeld cameratoezicht) en het gebruik van nieuwe, nog onbewezen technologieën.

De AP heeft een lijst[8] gemaakt met typen van verwerkingen waarvoor altijd een DPIA vereist is. Het gaat hierbij om de volgende voor het onderwijs relevante verwerkingen:

- Financiële situatie
  Grootschalige verwerkingen en/of de stelselmatige monitoring van financiële gegevens waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden (bijvoorbeeld overzichten van bankoverschrijvingen, de saldi van iemands bankrekeningen of mobiele of pinbetalingen).
- Gezondheidsgegevens
  Grootschalige verwerkingen van gegevens over gezondheid (bijvoorbeeld door instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, arbodiensten, re-integratiebedrijven, (speciaal)onderwijsinstellingen, verzekeraars en onderzoeksinstituten), waaronder ook de grootschalige elektronische uitwisseling van gegevens over gezondheid valt.
- Samenwerkingsverbanden
  De uitwisseling van bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard (bijvoorbeeld over gezondheid, verslaving, armoede, problematische schulden, werkloosheid, sociale problematiek, strafrechtelijke gegevens, betrokkenheid van jeugdzorg of maatschappelijk werk) in of door samenwerkingsverbanden van gemeenten of andere overheden met andere publieke of private partijen, bijvoorbeeld in wijkteams, veiligheidshuizen of informatieknooppunten.
- Cameratoezicht
  Grootschalige en/of stelselmatige monitoring van openbaar toegankelijke ruimten met behulp van (mobiele) camera's en webcams.
- Observatie en beïnvloeding van gedrag
  Grootschalige verwerkingen van persoonsgegevens waarbij op stelselmatige wijze via een geautomatiseerde verwerking het gedrag van natuurlijke personen geobserveerd of beïnvloed wordt, dan wel gegevens daarover worden verzameld en/of vastgelegd.
- Grootschalige verwerkingen en/of stelselmatige monitoring van biometrische gegevens met als doel een natuurlijk persoon te identificeren.

De controle of een DPIA vereist is, is opgenomen in de gegevensverwerkingsanalyse in deze modelaanpak. Vuistregel voor het onderwijs is dat een onderwijsinstelling in ieder geval een DPIA uitvoert bij de aanschaf van een nieuw administratiesysteem, leerlingvolgsysteem of studentinformatiesysteem, bij cameratoezicht of bij een ingrijpende update van deze systemen.

3.5. Waaruit moet een DPIA bestaan?

Volgens de AVG bevat de DPIA ten minste:

1. Een systematische beschrijving van de beoogde verwerkingen en verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die de verwerkingsverantwoordelijke aanvoert.
2. Een beoordeling van de noodzaak en evenredigheid van de verwerkingen in relatie tot de doeleinden.
3. Een beoordeling van de risico's voor de privacy van de betrokken onderwijsdeelnemers en medewerkers als gevolg van de onder 1 benoemde verwerking.
4. De beoogde maatregelen om de privacyrisico's te beperken (waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en aan te tonen dat aan de AVG is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie).

In deze modelaanpak is het DPIA-proces in twee stappen onderverdeeld, namelijk de gegevensverwerkingsanalyse gevolgd door de feitelijke DPIA. Onderdeel 1 van de bovenstaande opsomming is

[8] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf

het onderwerp van de gegevensverwerkingsanalyse, onderdelen 2, 3 en 4 gaan over de beoordeling en weging van de risico's en zijn onderdelen van de uitvoering van de DPIA zelf.

Hoewel de AVG en toezichthouder AP duidelijk zijn over de eisen waaraan de DPIA moet voldoen, is de vorm vrij. Er zijn dan ook diverse modellen van DPIA's in omloop, bijvoorbeeld van de rijksoverheid, SURF of NOREA. Vaak wordt er gebruikgemaakt van vragenlijsten. Zo bevat de DPIA van de rijksoverheid 17 vragen (die bestaan uit meerdere deelvragen). Dat lijkt misschien niet veel, maar om ze goed te kunnen beantwoorden moet de onderwijsinstelling, zoals eerder gezegd, wel in kaart hebben hoe de processen en het applicatielandschap eruitzien en een complete risicoanalyse hebben gedaan. Deze modelaanpak helpt de onderwijsinstellingen bij het doorlopen van alle benodigde stappen.

3.6. Eindresultaat

Over het algemeen geeft de FG advies over de kwaliteit en de bevindingen van de DPIA, waarna het rapport ter ondertekening wordt aangeboden aan het bestuur/cvb. Als het bestuur de DPIA heeft geaccepteerd, moeten ten minste de benoemde maatregelen om de hoge risico's te beperken binnen redelijk termijn worden uitgevoerd. Als dat niet mogelijk is, moet de AP worden geraadpleegd en de betreffende verwerking in de tussentijd worden gestopt.

Het eindproduct is een DPIA-rapportage, die in ieder geval de volgende onderdelen bevat:

- Beschrijving van de verwerking
- Beschrijving van de gegevensstromen
- Beschrijving van de (categorieën) persoonsgegevens
- Beoordeling van de rechtmatigheid (rechtsgrond)
- Beoordeling van het voldoen aan principes (doel/doelbinding, proportionaliteit, dataminimalisatie et cetera)
- Beschrijving van de risico's (inclusief classificatie)
- Beschrijving van de te nemen maatregelen en inschatting van het eventuele restrisico

3.7. Proces- of systeemniveau

Een DPIA is volgens de definitie een analyse en een beoordeling van een gegevensverwerkend proces. Het gaat daarbij niet alleen om de inventarisatie van de categorieën persoonsgegevens en classificatie van die data in een systeem, maar ook om een beoordeling van de rechtmatigheid, het doel, de proportionaliteit enzovoorts. Dit proces wordt vaak ondersteund door meer dan één systeem. Een DPIA op procesniveau dwingt om te bepalen welke systemen, al dan niet gekoppeld, een rol spelen in het gegevensverwerkende proces. De samenhang en afhankelijkheden daartussen kunnen een reden zijn om te kiezen voor een DPIA op procesniveau.

Toch zijn er ook DPIA's op systeemniveau. Zo zal een DPIA voor cameratoezicht vaak gebaseerd zijn op één systeem. Voor de hrm-processen kan worden gedacht aan een DPIA op basis van het hrm-pakket. Daarbij is een risico dat ondersteunende systemen vergeten kunnen worden, zoals de cloudopslag waarvan hrm ook gebruikmaakt, of waar de teamleider de functioneringsgespreksverslagen bewaart of de e-mail waarmee die het verslag naar de medewerker stuurt.

Tot slot ondersteunen sommige systemen zo veel processen dat het ondoenlijk is om ze in één DPIA te beoordelen. Een voorbeeld daarvan is het leerlingadministratiesysteem (LAS) of het SIS; het kan in dat geval verstandig zijn de scope van de DPIA te beperken tot een afgebakend proces, bijvoorbeeld 'instroom' of 'begeleiding'.

3.8. Evaluatie DPIA

De onderwijsinstelling kan de DPIA na een periode evalueren of herhalen, bijvoorbeeld als de software waarvoor ze de DPIA oorspronkelijk uitvoerde een ingrijpende update krijgt.

De FG kan onderzoeken of controleren of de maatregelen die in de DPIA staan ook genomen zijn, of beoordelen of er nieuwe risico's in beeld zijn gekomen nadat de verwerking is gestart.

4. Stappenplan DPIA

4.1. Fasering: gegevensverwerkingsanalyse en DPIA

Een DPIA is een veelomvattend, ingrijpend en niet-vrijblijvend instrument. Daarom is deze aanpak gesplitst in twee stappen:

1. Gegevensverwerkingsanalyse: een uitgebreide beschrijving van de gegevensverwerking om onder andere te beoordelen of een DPIA noodzakelijk is.
2. Risicoanalyse DPIA: de gegevensverwerkingsanalyse aangevuld met een beoordeling van de noodzaak en evenredigheid van de verwerkingen als het gaat om de doeleinden, de weging van de risico's (voor de betrokken personen) en de te nemen maatregelen om de privacyrisico's te beperken.

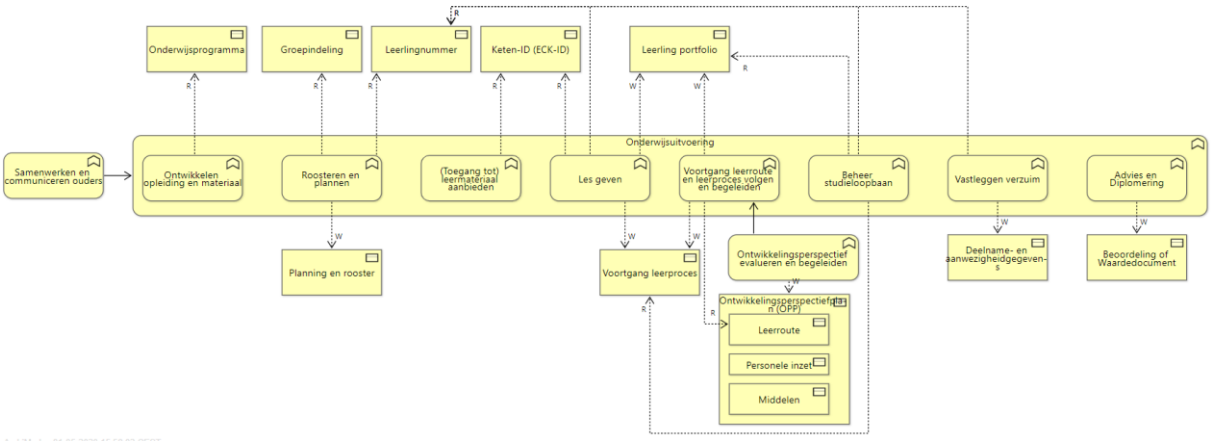
4.2. Gegevensverwerkingsanalyse

Bij de opstelling van de gegevensverwerkingsanalyse zijn personen betrokken die een goed beeld hebben van de processen, systemen en data die in deze systemen worden verwerkt, inclusief de gegevenskoppelingen. Door deze fase goed te doorlopen, kan de onderwijsinstelling de daadwerkelijke DPIA baseren op heldere feiten en omstandigheden en hoeft de privacy officer of FG niet zelf te zoeken naar informatie over de verwerking van persoonsgegevens. Het grootste deel van de informatie die gewogen wordt bij de DPIA, wordt in deze fase opgehaald.

De basis voor deze analyse zijn procesbeschrijvingen. Het is om verschillende redenen belangrijk om daarbij zo veel mogelijk aan te sluiten bij een referentiearchitectuur uit het onderwijs (FORA/Route21):

- De organisatie bespaart op die manier tijd omdat ze het proces niet zelf hoeft uit te tekenen.
- De organisatie voorkomt dat ze afhankelijkheden over het hoofd ziet.
- De DPIA wordt op die manier makkelijker deelbaar met andere instellingen; ze spreken immers dezelfde taal.

De afbeelding hieronder toont een voorbeeld van de bedrijfsfunctie **Onderwijsuitvoering** met alle onderliggende bedrijfsprocessen en de betrokken informatieobjecten, afkomstig uit de FORA.



Zie de bijlage voor meer verwijzingen naar referentiearchitecturen van de FORA.

De gegevensverwerkingsanalyse geeft in acht stappen een goed beeld van het gegevensverwerkende proces (de feitelijke situatie), gevolgd door een beoordeling of er belangrijke risico's voor betrokkenen aanwezig zijn. Op basis van deze informatie wordt een inschatting gemaakt of de uitvoering van een DPIA noodzakelijk is. Mocht een DPIA niet nodig zijn, dan beschikt de onderwijsinstelling met de gegevensverwerkingsanalyse over een onderbouwing van die uitkomst.

De vragenlijst voor de gegevensverwerkingsanalyse is opgenomen als bijlage.

4.2.1. Onderdelen gegevensverwerkingsanalyse

De gegevensverwerkingsanalyse bestaat uit de volgende onderdelen:

1. Een beschrijving van het gegevensverwerkende proces
   a. proces (met proceseigenaren)
   b. applicatielandschap (met applicatie-eigenaren)
   c. koppelingen (met documentatie, dataset)
   d. gegevensstromen
2. Verwerkte persoonsgegevens
   a. categorieën persoonsgegevens
   b. classificatie persoonsgegevens
   c. beoordeling conform dataregister
3. Verwerkingsdoeleinden
4. Betrokken partijen
   a. externe verantwoordelijken
   b. externe verwerkers
   c. ontvangers persoonsgegevens
5. Bewaartermijnen
6. Een beoordeling van de rechtmatigheid
   a. rechtsgrond
   b. doel/doelbinding
   c. noodzakelijkheid
   d. transparantie
7. Een globale beoordeling van de risico's
   a. hoge risico's voor betrokkenen?
   b. wel/geen DPIA?
8. Beveiligingsmaatregelen
   a. toegangsbeveiliging
   b. opslag/beveiliging gegevens
   c. beveiliging gegevenskoppelingen
   d. certificering/waarborging leverancier(s)
   e. procedures beveiligingsincidenten
   f. back-up en restoreprocedures
   g. logging van gebeurtenissen

Hierna volgt de beoordeling of een DPIA noodzakelijk is.

Hoewel de gegevensverwerkingsanalyse tot doel heeft om de feitelijke situatie boven tafel te krijgen, is het mogelijk om in deze fase al risico's te identificeren die in de volgende fase gewogen en beoordeeld worden. Dergelijke input helpt bij het maken van de afweging of, volgend op deze gegevensverwerkingsanalyse, de uitvoering van een DPIA nodig is en welke aandachtspunten daarvoor in elk geval van toepassing zijn.

Als de conclusie van deze gegevensverwerkingsanalyse is dat er geen hoge risico's zijn, stopt het DPIA-proces hier. Met de gegevensverwerkingsanalyse is dan onderbouwd dat er geen DPIA nodig is.

4.3. Risicoanalyse DPIA

Als op basis van de gegevensverwerkingsanalyse blijkt dat een DPIA nodig is, loopt het proces verder zoals hieronder beschreven. De eerste fase van de DPIA − de gegevensverwerkingsanalyse − is al afgerond. Deze vormt de beschrijving van de verwerking en is daarmee een belangrijk onderdeel van de DPIA.

4.3.1. Onderdelen van de DPIA

De DPIA bestaat uit een **uitgebreide risicobeoordeling** en een beschrijving van mitigerende maatregelen:

1. Eventuele aanvullingen en een oordeel over de gegevensverwerkingsanalyse (zie 4.2.1)
2. Beschrijving van de aanpak van de DPIA
3. Vastgestelde risico's
4. Mitigerende maatregelen
5. Risicodashboard
6. Planning voor mitigatie hoge risico's
7. Akkoord FG/cvb

4.3.2. DPIA-rapportage: uitgebreide en gewogen risicoanalyse

Op basis van de verzamelde informatie uit de gegevensverwerkingsanalyse kan de onderwijsinstelling één of meer risicoworkshops organiseren voor medewerkers die betrokken zijn bij de betreffende verwerkingen. Met hen worden de stappen uit de analyse getoetst en gewogen:

- Procesbeschrijvingen
- Applicatielandschap
- Koppelingen
- Gegevensstromen
- Dataregister
- Eventueel reeds gesignaleerde risico's

Hierbij wordt de gevonden informatie gewogen en onderbouwd en wordt verkend wat de risico's zijn.

4.3.3. Risico's inventariseren

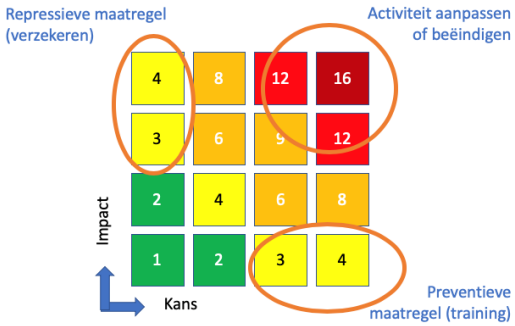
De volgende stap is het bespreken van de bedreigingen vanuit het perspectief van de betrokken medewerkers. Daarbij is de MAPGOOD-methodiek vaak heel behulpzaam. Bij ieder in de MAPGOOD genoemd element spelen bepaalde risico's, bijvoorbeeld:

- Mens
  a. onkunde, slordigheid
  b. niet werken volgens voorschriften
  c. fraude, sabotage
- Apparatuur
  a. verouderd, onjuist functioneren
  b. stroomuitval
- Programmatuur
  a. ontwerp/programmeerfouten
  b. geen actuele updates
- Gegevens
  a. ontoegankelijk
  b. toegankelijk voor onbevoegden
  c. verloren gaan
- Organisatie
  a. onduidelijke taken, bevoegdheden
  b. ontbrekende gedragscodes
- Omgeving
  a. onvoldoende beveiligde ruimtes
  b. natuurgeweld
- Diensten
  a. geen goede leveranciersafspraken
  b. leverancier gaat failliet

Door privacybedreigingen in deze categorieën in te delen wordt meteen voorgesorteerd op de mogelijke maatregelen. Zo vraagt een dreiging in de categorie 'Mens' vaak om maatregelen op het gebied van awareness of training.

4.3.4. Risico's wegen: kans x impact = risico

Naast de identificatie van de dreiging gaat het ook om de classificatie ervan: hoe groot is het risico? Daarbij wordt de kans dat een dreiging optreedt vermenigvuldigd met de impact, ofwel de schade die wordt aangericht. Hierbij wordt uitgegaan van een schaalverdeling van 4; op die manier kan het risico waarden aannemen tussen 1 en 16.



Na weging van de risico's wordt beoordeeld of deze beperkt kunnen worden door bestaande of nieuw te nemen maatregelen. Dit wordt het mitigeren van risico's genoemd. Het risico na toepassing van de mitigerende maatregelen wordt restrisico genoemd.

Een succesvolle risicoworkshop levert een schat aan informatie voor de risicoanalyse op. Deze analyse bevat:

- Beschrijving van de dreigingen
- Categorie (MAPGOOD)
- Classificatie (1 tot 16)
- Voorgenomen maatregelen
- Restrisico (1 tot 16)
- Optioneel: eigenaar

Deze gegevens worden verwerkt in het risicodashboard: een tekstuele of grafische weergave van de gevonden en gewogen risico's en de maatregelen.

Risicoanalyse: Instroom

NR	Categorie	Dreiging	Proces	Omschrijving				Beoogde maatregel	Status	Verantwoordelijk	Rest risico		
8	Programmatuur	Onvoldoende grip op de verwerking rondom de voorlichtings-activiteiten	Voorlichting	Er is onduidelijkheid of aan AVG richtlijnen voldaan wordt (minimalisatie, bewaartermijnen, rechten betrokkenen)	4	2	8	Onderzoeken en eventueel herinrichten/heroriënteren wervingstool 4DMS (CRM)	Wacht op akkoord	Sander van der Vorm	2	2	4
14	Gegevens	Gegevens worden verwerkt zonder dat hier een (acceptabel) doel voor is.	Voorlichting	Het doel voor vastleggen persoonsgegevens van kandidaat-studenten is niet omschreven, niet duidelijk wat er met de gegevens gebeurt en wie binnen Zadkine verantwoordelijk is.	2	3	6	Registratieformulieren, disclaimers en werkproces aanpassen zodat ze aansluiten op de AVG.	Wacht op akkoord	Sander van der Vorm	2	1	2
2	Mens - onopzettelijk	Onrechtmatige verwerking van persoonsgegevens.	Aanmelding	Door onzorgvuldig opslaan van papieren aanmeldingen kunnen deze kwijtraken of door ongeautoriseerde worden ingezien. Daarnaast geeft een papieren aanmelding meer vrijheid/minder sturing, waardoor eenvoudig te veel gegevens verstrekt kunnen worden.	2	2	4	Aanmelding op papier staken en inrichten van het Service Punt als vangnet om (digitaal) te kunnen aanmelden.	Wacht op akkoord	Sander van der Vorm	1	2	2
4	Mens - opzettelijk	Onwenselijk gebruik van gegevens	Aanmelding	Er bestaat de kans dat op basis van het DDD een student wordt afgewezen. Hiermee wordt het recht op een frisse start vergeten.	4	4	16	DDD pas beschikbaar stellen na de plaatsing van een student.	Wacht op akkoord	IVP Manager	1	2	2
5	Mens - opzettelijk	Onwenselijk gebruik van gegevens	Aanmelding	Er is geen eenduidig beeld over de noodzaak van het DDD. Zonder duidelijk doel gaat inzet van het DDD tegen het principe van dataminimalisatie in.	4	4	16	Onderzoeken welke invloed Zadkine hierop heeft en eigen beleid bepalen rondom DDD. Onderzoeken hoeveel studenten zonder DDD worden geplaatst.	Wacht op akkoord	Wim Arendse	1	1	1
9	Programmatuur	Aanmeldgegevens worden niet correct opgeslagen en verwijderd	Aanmelding	Als er een probleem is met de koppeling digitaal aanmelden (Sitecore-Eduarte) dan worden de records in xml-format verstuurd aan individuele beheerders.	2	2	4	Dit vervangen door een afvangmailbox, zodat de berichten centraal verwijderd kunnen worden als ze niet meer nodig zijn. Inzicht krijgen in rechten en gebruik van Sitecore.	Wacht op akkoord	Sander van der Vorm	1	2	2
10	Gegevens	Verwerking van te veel gegevens	Aanmelding	Aanmeldingen worden niet opgeschoond. Ook afgekeurde en teruggetrokken aanmeldingen blijven in EduArte staan. Aanmeldgegevens worden bewaard tot na diplomering, voor analyse doeleinden.	4	3	12	Bepalen van beleid/randvoorwaarden rondom bewaren aanmeldgegevens. Periodiek opschonen van EduArte.	Wacht op akkoord	Daan Verbeek	2	2	4
11	Gegevens	Onrechtmatige verwerking van bijzondere persoonsgegevens	Aanmelding	Het DDD bevat mogelijk onrechtmatig gevoelige en/of bijzondere persoonsgegevens.	4	4	16	DDD onderzoeken en zo nodig partijen instrueren. Evt gebruik DDD heroverwegen.	Wacht op akkoord	Wim Arendse	2	4	8

Waar het mogelijk en relevant is in deze fase van beoordeling kunnen de te nemen maatregelen worden gekoppeld aan een eigenaar. Hiermee wordt gelijk de verantwoordelijkheid voor de uitvoering van de maatregel belegd. Het is alleen noodzakelijk om de hoge risico's aan te pakken, van de overige risico's kan in het dashboard worden aangegeven dat ze blijven bestaan. Overigens is dit een risicoafweging die de FG en het bestuur van de onderwijsinstelling moeten bekrachtigen.

4.3.5. Uitkomst

Nadat de DPIA met de FG is besproken, en eventueel een akkoord voor het risicodashboard is verkregen, worden de bevindingen in een DPIA-rapportage verwerkt. Daar mag de onderwijsinstelling een eigen vorm voor kiezen.

Het is een goed gebruik om de bevindingen voor te leggen aan een vertegenwoordiging van de betrokkenen: de (gemeenschappelijke) medezeggenschapsraad, ondernemingsraad en/of leerlingen- of (centrale) studentenraad. Behalve aan het draagvlak zal dat ook bijdragen aan de kwaliteit van de rapportage.

4.3.6. Goedkeuring van de DPIA-rapportage

Het bestuur van de onderwijsinstelling (schoolbestuur of cvb) verleent op basis van advies van de FG goedkeuring voor de DPIA.

Als er geen hoge risico's zijn gevonden, of als deze al tijdens het proces zijn gemitigeerd, is de DPIA afgerond.

In veel gevallen staan er echter nog hoge risico's open, waarvoor maatregelen zijn beschreven. Goedkeuring van de DPIA houdt dan in dat de onderwijsinstelling de beschreven mitigerende maatregelen binnen redelijke termijn (afhankelijk van de hoogte van het risico) moet uitvoeren. Nadat die maatregelen zijn genomen worden de restrisico's opnieuw ingeschat en besproken met de FG. Daarna kan het betreffende mitigatie(deel)project worden afgesloten.

4.4. Herbeoordeling van de DPIA

In de (toelichting op de) wet staat dat het een goede praktijk is om een DPIA regelmatig opnieuw te beoordelen. Dat moet in ieder geval bij wijzigingen in het verwerkingsproces of de gebruikte technologie. Maar ook als er ogenschijnlijk niets is veranderd moet de organisatie periodiek controleren of de DPIA nog actueel is en of de geadviseerde maatregelen (nog steeds) van kracht en/of geïmplementeerd zijn. Het uitgangspunt is dat DPIA's ten minste eens in de twee tot drie jaar worden herbeoordeeld.

Bijlage 1 Vragenlijst gegevensverwerkingsanalyse

Uitleg

Een DPIA of gegevensbeschermingseffectbeoordeling begint met de **gegevensverwerkingsanalyse**. Dat is een systematische beschrijving van welke processen worden onderzocht, welke systemen daarbij betrokken zijn, welke gegevens worden verwerkt en hoe deze gegevens zijn geclassificeerd. Daarbij wordt ook ingegaan op het doel en de grondslag van de verwerking en de eventuele betrokkenheid van andere partijen, zoals leveranciers. Het gaat hier om een **feitelijke** rapportage en analyse. Vervolgens wordt op basis van richtlijnen van de toezichthouder bepaald of de organisatie een risicoanalyse (DPIA) moet uitvoeren. Mocht een DPIA niet nodig zijn, dan vormt de ingevulde vragenlijst daarvoor een weloverwogen en gemotiveerd besluit.

Invulinstructie

Deze 'Vragenlijst gegevensverwerkingsanalyse' wordt ingevuld door de onderwijsinstelling. Dit gebeurt bij voorkeur door medewerkers die inhoudelijk betrokken zijn bij of kennis hebben van de applicatie die of het proces dat onderzocht wordt (bijvoorbeeld de functioneel applicatiebeheerder). Alle vragen worden **vanuit het perspectief van de eigen onderwijsinstelling** beantwoord. Dus geef antwoorden over je eigen software, organisatie, uitwisseling van gegevens et cetera.

De gegevensverwerkingsanalyse geeft in acht stappen een goed beeld van het gegevensverwerkende proces (of de software). De doorgaans lastige vragen bij een DPIA zijn in deze vragenlijst opgesplitst in kortere, eenvoudige vragen. Hierdoor zijn het er weliswaar meer, maar de vragen zijn gemakkelijker in te vullen door medewerkers die geen of beperkte kennis van privacy hebben.

Opbouw vragenlijst (onderdelen)

De gegevensverwerkingsanalyse bestaat, behalve uit algemene informatie, uit de volgende acht stappen, gevolgd door de beoordeling of een DPIA noodzakelijk is:

1. Beschrijving van het gegevensverwerkende proces
2. Verwerkte persoonsgegevens
3. Verwerkingsdoeleinden
4. Betrokken partijen
5. Bewaartermijnen
6. Beoordeling van de rechtmatigheid
7. Globale beoordeling van de risico's
8. Beveiligingsmaatregelen

Hierna volgt de beoordeling of een DPIA noodzakelijk is.

Deze opbouw kan gebruikt worden om in hoofdlijnen een proces of software te beoordelen en te beschrijven.

VRAGENLIJST

Algemene informatie

In dit onderdeel vul je de algemene informatie in.

1. Naam van de organisatie
2. Naam van de invuller
3. Datum
4. Naam van het (deel)proces
5. Omschrijving van het (deel)proces
6. Versieaanduiding van het geraadpleegde verwerkings-/dataregister

1. Beschrijving van het gegevensverwerkende proces

In dit onderdeel beschrijf je in algemene bewoordingen het proces, de gebruikte systemen, de koppelingen en de gegevensstromen van en binnen de onderwijsinstelling. Het gaat er vooral om een beeld te schetsen van de

scope van de gegevensverwerkingsanalyse en de eventueel hierop volgende DPIA. Maak hiervoor gebruik van een referentiearchitectuur (FORA[9] of Route 21[10]).

7. Procesbeschrijving

Een korte beschrijving van het gegevensverwerkende proces waarop de analyse en DPIA betrekking hebben. Beschrijf op hoofdlijnen waar het proces over gaat: welke bedrijfsfunctie? In de FORA gaat het om een proces binnen het bedrijfsfunctiemodel: binnen de school.

> In de FORA is een beschrijving opgenomen van alle bedrijfsprocessen:
> https://www.wikixl.nl/wiki/fora/index.php/DPIA#Procesbeschrijving

8. Applicatielandschap

Een korte beschrijving van het applicatielandschap van de onderwijsinstelling. Dat is een overzicht van alle applicaties en systemen binnen de (eigen) onderwijsinstelling. Voeg via een link eventuele schema's toe.

> In de FORA is een model-applicatielandschap opgenomen:
> https://www.wikixl.nl/wiki/fora/index.php/DPIA#Applicatielandschap

9. Koppelingen

Een korte beschrijving van de van toepassing zijnde (externe) koppelingen van het onderzochte systeem of proces. Waar is het mee gekoppeld? Of staat het systeem los? Voeg via een link eventuele schema's toe. Benoem de koppelvlakken/sleutelvelden waarop wordt gekoppeld. Bij onderdeel 4 ('Betrokken partijen', vanaf vraag 27) geef je aan met welke partijen koppelingen bestaan, dat hoeft niet hier. Bij deze vraag 9 beschrijf je de koppelingen vanuit technisch en functioneel perspectief.

10. Beschrijving gegevensstromen

Een korte beschrijving van de gegevensstromen op hoofdlijnen volgens de systematiek input-verwerking-output. Als er gegevensstroomdiagrammen zijn, voeg die dan via een link toe.

> In de FORA is een voorbeeld opgenomen van gegevensstromen voor de LAS:
> https://www.wikixl.nl/wiki/fora/index.php/DPIA#Gegevensstromen

2. Verwerkte persoonsgegevens

In dit onderdeel onderzoek je welke categorieën persoonsgegevens worden verwerkt binnen de onderwijsinstelling en controleer je of dit in overeenstemming is met het huidige verwerkingsregister/dataregister.

11. Worden er persoonsgegevens van onderwijsdeelnemers, hun ouders/verzorgers verwerkt?

- Ja
- Nee

12. Categorieën persoonsgegevens onderwijsdeelnemers

Welke categorieën van persoonsgegevens van onderwijsdeelnemers worden verwerkt binnen het proces? Vink aan wat van toepassing is.

- Contactgegevens: naam, e-mail en organisatie-eenheid
- Contactgegevens: geboortedatum en geslacht
- Contactgegevens ouder/verzorger
- Student-/leerlingnummer
- Nationaliteit en geboorteplaats
- Medische gegevens
- Godsdienst

[9] https://www.wikixl.nl/wiki/fora/index.php/DPIA
[10] https://www.sambo-ict.nl/route21/

- Studievoortgang (voortgang examen studietraject, begeleiding en handelingsplan, klas/leerjaar opleiding)
- Onderwijsorganisatie (roosters, boekenlijsten et cetera)
- Financiën (volledige cyclus)
- Beeldmateriaal (pasfoto, camerabeelden enzovoort)
- Docenten, mentoren en mbo-adviseur
- Burgerservicenummer/persoonsgebonden nummer (BSN/PGN)

13. Worden er persoonsgegevens van medewerkers verwerkt?
- Ja
- Nee

14. Categorieën persoonsgegevens medewerkers/relaties
Welke categorieën van persoonsgegevens van medewerkers worden verwerkt binnen het proces? Vink aan wat van toepassing is.
- Contactgegevens: naam, e-mail en organisatie-eenheid
- Contactgegevens volledig
- Personeelsnummer
- Nationaliteit en geboorteplaats
- Medische gegevens (voor zover toegestaan, bijvoorbeeld bij re-integratie)
- Ervaringen (werkervaring en opleidingen)
- R&O-gesprekken (resultaat en ontwikkeling)
- Financiën (volledige cyclus)
- Beeldmateriaal (bijvoorbeeld pasfoto, camerabeelden)
- BSN

15. Worden er persoonsgegevens anders dan van onderwijsdeelnemers of medewerkers verwerkt?
- Ja
- Nee

16. Categorieën persoonsgegevens van overige betrokkenen (relaties, derden, leveranciers et cetera)
Welke categorieën van persoonsgegevens van overige betrokkenen worden verwerkt binnen het proces?

17. Zijn de opgegeven categorieën persoonsgegevens in overeenstemming met het dataregister?
Zijn de categorieën van persoonsgegevens opgenomen en verwerkt binnen in het dataregister of register van verwerkingen?
- Ja
- Nee

18. Licht je antwoord hier toe

19. Is de **vertrouwelijkheid** van een of meer categorieën persoonsgegevens ingeschaald als ‘hoog’?
De categorieën persoonsgegevens worden geclassificeerd volgens de BIV-classificatie, zie hiervoor het dataregister. De beschikbaarheid, integriteit en vertrouwelijkheid kunnen laag, midden of hoog zijn.
- Ja
- Nee

20. Eventuele aanvullende opmerkingen over dit onderdeel 'Verwerkte persoonsgegevens'

3. Verwerkingsdoeleinden

In dit onderdeel specificeer je de verwerkingsdoeleinden. Deze vragen hangen samen met onderdeel 6 (‘Beoordeling van de rechtmatigheid’, vanaf vraag 41).

21. Verwerkingsdoeleinden (onderwijsdeelnemers)
Als je had opgegeven dat er persoonsgegevens van onderwijsdeelnemers worden verwerkt, geef dan hieronder de verwerkingsdoeleinden aan.

- Gegevens voor registratie, aanmelding en inschrijving (informatiedagen, informatieverzoeken over opleidingen, open dagen et cetera)
- Komen tot een onderwijsovereenkomst (OOK – alleen mbo)
- Komen tot een praktijkovereenkomst (POK – alleen mbo)
- Verantwoorden aan DUO, inspectie en accountant (bijlage OOK)
- Voorbereiden voor aanschaf en gebruik van (digitale) leermiddelen en toetsmaterialen
- Didactisch en/of pedagogisch dossier (voortgang, examineren en aanwezigheid registratie)
- Begeleiding in het kader van passend onderwijs (gezondheidsgegevens) en aanvragen/advisering ondersteuning (TLV/LWOO/PRO) en arrangementen
- Toestemming verwerken van de onderwijsdeelnemer (bijvoorbeeld voor het gebruik van beeldmateriaal)
- Anders:

22. Verwerkingsdoeleinden (medewerkers)
Als je had opgegeven dat er persoonsgegevens van medewerkers worden verwerkt, geef dan hieronder de verwerkingsdoeleinden aan.

- Komen tot een arbeidsovereenkomst
- Voldoen aan de wettelijke verplichtingen (belasting, pensioen et cetera)
- Overeenkomsten met externe verwerkers (ADP, QMP, Office 365 et cetera)
- Voorbereiden voor aanschaf en gebruik van (digitale) leermiddelen en toetsmaterialen
- Regelingen op het gebied van secundaire arbeidsvoorwaarden
- Begeleiding van medewerkers (arbodienst, bedrijfsarts, re-integratie, coaching et cetera)
- Toestemming voor verwerken van de medewerker (bijvoorbeeld voor het gebruik van beeldmateriaal)
- Anders:

23. Verwerkingsdoeleinden (overig)
Als je had opgegeven dat er persoonsgegevens van overige betrokkenen worden verwerkt, beschrijf dan hieronder de verwerkingsdoeleinden.

24. Zijn de opgegeven verwerkingsdoeleinden in overeenstemming met het verwerkingsregister/dataregister?

- Ja
- Nee of onbekend

25. Licht je antwoord hier toe

26. Eventuele aanvullende opmerkingen over dit onderdeel 'Verwerkingsdoeleinden'

4. Betrokken partijen

In dit gedeelte geef je aan welke partijen betrokken zijn bij de gegevensverwerking. Het gaat om (mede)verwerkingsverantwoordelijken, verwerkers en derden (verstrekkers en ontvangers van persoonsgegevens). Bij het antwoord op vraag 9 is bijvoorbeeld beschreven dat er koppelingen zijn met het onderzochte systeem of proces. In dit onderdeel benoem je de daarbij betrokken partijen, inclusief hun rol in het gegevensverwerkende proces.

27. Is er naast de eigen organisatie nog een andere partij betrokken in de rol van verwerkingsverantwoordelijke?

- Ja
- Nee

28. Welke verwerkingsverantwoordelijke(n) betreft het?

Schrijf een korte toelichting over de samenwerking en rolverdeling. Het gaat bijvoorbeeld om een samenwerkingsverband, een andere onderwijsinstelling of OCW of DUO.

29. Welke verwerkers zijn betrokken bij de gegevensverwerking?
*Het gaat hierbij om **verwerkers** volgens art. 28/29 van de AVG en om partijen die mogelijk op een andere manier betrokken zijn bij het proces en zo bijvoorbeeld inzage in persoonsgegevens zouden kunnen krijgen. Geef voor elke externe partij de vestigingsplaats en aard van de werkzaamheden aan en − indien bekend − of deze partij die werkzaamheden als verwerker of als andere dienstverlener uitvoert.*

30. Worden er gegevens verwerkt buiten de EER?
Wanneer gegevens buiten de Europese Economische Ruimte worden verwerkt, zijn aanvullende waarborgen vereist.

- Ja
- Nee

31. Welke gegevens worden door welke verwerkers buiten de EER verwerkt?
Benoem hier ook in welk land de gegevens worden verwerkt en − indien bekend − de toegepaste waarborgen, bijvoorbeeld een adequaatheidsbesluit of het gebruik van de 'standard contractual clauses'.

32. Worden er persoonsgegevens **van** of **via** externe partijen **ontvangen**? Dus niet van de medewerker of onderwijsdeelnemer zelf.
Het gaat bijvoorbeeld om persoonsgegevens die worden aangeleverd door de aanleverende school, DUO et cetera.

- Ja
- Nee

33. Van welke externe partijen worden persoonsgegevens ontvangen en met welk doel?

34. Worden er persoonsgegevens **aan** externe partijen **verstrekt**?
Het gaat om partijen die niet genoemd zijn als verwerker (zie boven), maar die een zelfstandige taak en verantwoordelijkheid hebben. Denk daarbij aan DUO (onderwijsdeelnemers) en het UWV (medewerkers).

- Ja
- Nee

35. Aan welke partijen worden deze verwerkte persoonsgegevens verstrekt en met welk doel?

36. Eventuele aanvullende opmerkingen over dit onderdeel 'Betrokken partijen'

5. Bewaartermijnen

Dit gedeelte gaat in op het beleid voor bewaartermijnen en de manier waarop die bewaartermijnen worden bewaakt.

37. Worden de bewaartermijnen gehanteerd volgens het door de instelling vastgestelde beleid?
Deze bewaartermijnen zijn opgenomen in het verwerkingenregister/dataregister. Let ook op 'schaduwsystemen', zoals Excel-exportbestanden.

- Ja
- Nee
- Niet van toepassing
- Onzeker/onbekend

38. Toelichting op de bewaartermijnen

Licht hier toe waarom de bewaartermijnen wel/niet in lijn zijn met het vastgestelde beleid of leg uit waarom je hierover onzeker bent.

39. Op welke manier worden de bewaartermijnen bewaakt?
Wordt dit bijvoorbeeld door het proces/systeem ondersteund ('privacy by design').

40. Eventuele aanvullende opmerkingen over dit onderdeel 'Bewaartermijnen'

6. Beoordeling van de rechtmatigheid

In dit gedeelte geef je een globale inschatting van de grondslag, het doel en de doelbinding en in hoeverre de gegevensverwerking noodzakelijk en transparant is. Hierbij is relevant om de antwoorden 21 tot en met 26 (onderdeel 3 'Verwerkingsdoeleinden') bij het antwoord te betrekken.

41. Grondslag(en) voor de verwerking
Geef aan op welke grondslag(en) de gegevensverwerkingen zijn gebaseerd. Meerdere opties zijn mogelijk. Is dit onbekend, vul dan niets in.

- Wettelijke verplichting
- Taak van algemeen belang
- Uitvoering van een overeenkomst
- Gerechtvaardigd belang
- Toestemming van de betrokkene
- Vitaal belang van de betrokkene

42. Toelichting op de grondslag(en)
Geef een toelichting op de grondslag.

43. Doelbinding
Als persoonsgegevens voor een ander doel worden verwerkt dan ze oorspronkelijk zijn verzameld, beoordeel dan of deze verdere verwerking verenigbaar is met het oorspronkelijke doel.

- De gegevens worden uitsluitend gebruikt voor het doel waarvoor ze oorspronkelijk waren verzameld
- De gegevens worden ook gebruikt voor andere toepassingen dan het oorspronkelijke doel

44. Toelichting doelbinding: voor welke andere/nieuwe/afgeleide doelen worden de persoonsgegevens gebruikt?
Geef hierbij ook aan in hoeverre deze andere/nieuwe/afgeleide vorm van gebruik verenigbaar is met het oorspronkelijke doel.

45. Noodzaak van de verwerking
Is de gegevensverwerking noodzakelijk voor het realiseren van de verwerkingsdoeleinden en kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden bereikt?

- Ja
- Nee
- Onzeker/onbekend

46. Toelichting op bovenstaand antwoord over de noodzaak

47. Evenredigheid van de verwerking
Staan de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden en worden er niet te veel gegevens gevraagd of gebruikt?

- Ja
- Nee

- Onzeker/onbekend

48. Toelichting op bovenstaand antwoord over de evenredigheid

49. Rechten van de betrokkenen
Kunnen de betrokkenen via de onderwijsinstelling hun rechten uitoefenen bij deze verwerking, zoals het recht op inzage, correctie, verwijdering of geïnformeerd worden over de verwerking van hun persoonsgegevens?
- Ja
- Nee

50. Eventuele aanvullende opmerkingen over dit onderdeel 'Rechtmatigheid'

7. Globale beoordeling van de risico's

In de (toelichting op de) AVG zijn een aantal scenario's benoemd die worden aangeduid als risicovol. Vrij vertaald naar de onderwijspraktijk levert dat de onderstaande situaties op. Geef aan of het betreffende scenario op de onderzochte gegevensverwerking van toepassing is.

51. Grootschalige verwerking
Is er, gelet op het aantal betrokkenen en/of de hoeveelheid gegevens, sprake van een grootschalige verwerking? Als de verwerking is gericht op alle onderwijsdeelnemers en/of medewerkers is er al snel sprake van een grootschalige verwerking.
- Ja
- Nee
- Onzeker

52. Toelichting op de grootschalige verwerking

53. Bijzondere persoonsgegevens
Worden er binnen het proces bijzondere en/of gevoelige persoonsgegevens verwerkt? Bijvoorbeeld over de gezondheid (zoals een beperking als dyslexie), godsdienst, vakbondslidmaatschap of de financiële situatie van de betrokkene?
- Ja
- Nee
- Onzeker/onbekend

54. Toelichting op bijzondere persoonsgegevens

55. Toestemming van betrokkenen
Is er sprake van toestemming van de betrokkene als rechtsgrond voor de verwerking (zie ook vraag 41 'Grondslag(en) van de verwerking')
- Ja
- Nee

56. Toelichting op de toestemming van betrokkenen

57. Evaluatie en beoordeling: geautomatiseerde besluitvorming en profilering
Is er sprake van een geautomatiseerde evaluatie en beoordeling van betrokkenen, waaronder profilering? Denk aan vormen van 'learning analytics' of andere vormen van geautomatiseerd meten en/of beoordelen van prestaties. Hieronder vallen ook gevallen waarbij door ict-toepassingen/software beslissingen worden genomen die van invloed zijn op de rechten en verplichtingen van onderwijsdeelnemers en/of medewerkers.
- Ja
- Nee

- Onzeker/onbekend

58. Toelichting op evaluatie en beoordeling

59. Systematische observatie
Is er sprake van observatie van betrokkenen door bijvoorbeeld proctoring software, cameratoezicht of de monitoring van software-/netwerkgebruik?
- Ja
- Nee
- Onzeker/onbekend

60. Toelichting op systematische observatie

61. Koppeling van gegevensbestanden
Worden er persoonsgegevens uit verschillende (interne en externe) bestanden aan elkaar gekoppeld waardoor nieuwe vormen/inzichten van data-analyse mogelijk worden?
- Ja
- Nee
- Onzeker/onbekend

62. Toelichting op de koppeling van gegevensbestanden

63. Nieuwe technologieën
Worden de persoonsgegevens verwerkt met gebruikmaking van een nieuwe, tot nu toe nog onbewezen technologie?
- Ja
- Nee
- Onzeker/onbekend

64. Toelichting op nieuwe technologieën

64a. Is er sprake van een van de volgende grootschalige verwerkingen van persoonsgegevens rondom: de financiële situatie, biometrische persoonsgegevens (vingerafdruk, gezichtsscan), gezondheidsgegevens, samenwerkingsverbanden (samenwerkingen tussen onderwijsinstelling en gemeente/overheden/jeugdzorg), (flexibel) cameratoezicht, de stelselmatige controle van werknemers, profilering of geautomatiseerde besluitvorming?
Het betreft hier de opsomming van verwerkingen van persoonsgegevens waarvoor volgens de Autoriteit Persoonsgegevens altijd een DPIA noodzakelijk is.
- Ja
- Nee
- Onzeker/onbekend/niet van toepassing.

65. Aanvullende risico's
Komen er uit deze inventarisatie aanvullend nog risico's waarmee rekening gehouden moet worden?

8. Beveiligingsmaatregelen
Dit onderdeel gaat in op de beveiligingsmaatregelen op hoofdlijnen.

66. Op welke manier krijgen gebruikers toegang tot het gebruikte systeem en op welke wijze is de toegang beveiligd?
Is de toegang tot het systeem gedefinieerd en opgenomen in een autorisatiematrix; op welke manier wordt identity en access management toegepast?

67. Op welke wijze worden de gegevens opgeslagen en beveiligd?
Draait de applicatie bijvoorbeeld 'on premisse' of is er sprake van een clouddienst bij de leverancier? Zijn de gegevens versleuteld?

68. Als er gegevens worden uitgewisseld via gegevenskoppelingen, beschrijf dan op welke manier de gegevens tijdens de overdracht zijn beveiligd
Denk daarbij aan beveiligde webservices en/of de toepassing van end-to-end-encryptie.

69. Heeft of hebben de leverancier(s) certificeringen en worden (audit)rapportages aangeleverd?
Voor informatiebeveiliging wordt vaak een ISO 27001-certificering gebruikt.

70. Heeft de onderwijsinstelling procedures beschikbaar om (security)incidenten pro- en reactief te melden bij of door de verantwoordelijke leverancier (en vice versa)?

71. Zijn er duidelijke afspraken over de back-up en restore van de data en de beschikking daarover?

72. Worden acties van gebruikers binnen de onderzochte applicatie of programmatuur opgeslagen (logging)?

9. Beoordeling van de noodzaak van een DPIA
Als invuller van de gegevensverwerkingsanalyse kun je als afsluiting een advies, oordeel, opmerking of toelichting geven over/op de vraag of de onderwijsinstelling een DPIA moet uitvoeren. Deze beoordeling is met name gebaseerd op de antwoorden op de vragen 51 tot en met 65.

73. Moet de organisatie naar jouw mening op basis van bovenstaande informatie een DPIA uitvoeren?
- Ja
- Nee
- Onzeker/onbekend

74. Toelichting op de noodzaak van een DPIA
Geef hieronder aan waarom de organisatie wel/geen DPIA moet uitvoeren.

75. Als er een DPIA wordt uitgevoerd, zijn er dan specifieke risico's die meegenomen moeten worden?
Geef hieronder puntsgewijs aan wat de belangrijkste of specifieke risico's zijn die de organisatie bij een DPIA niet mag vergeten.

Hartelijk dank voor het invullen van deze gegevensverwerkingsanalyse. Verstuur deze ter beoordeling naar de FG. Mocht er een DPIA worden uitgevoerd, dan worden de gegevens van deze analyse daarin overgenomen en zo nodig gewijzigd/aangevuld. Vervolgens wordt een uitgebreide risicoanalyse toegevoegd en de bijbehorende maatregelen om de gevonden hoge risico's te mitigeren.

De informatie hierna is in te vullen door de proceseigenaar/schoolbestuur/cvb/FG/privacy officer.

76. Beoordeling
Op basis van de bovenstaande gegevens kan de proceseigenaar en/of FG beoordelen of de organisatie een DPIA moet uitvoeren.

77. Moet er op basis van bovenstaande informatie een DPIA worden uitgevoerd?
- Ja
- Nee

78. Toelichting op de noodzaak van een DPIA

Geef hieronder aan waarom er wel/geen DPIA wordt uitgevoerd

79. Gezien FG
De FG tekent voor gezien.

Bijlage 2 Vragenlijst risicoanalyse DPIA

Uitleg

Bij de **risicoanalyse DPIA** worden de antwoorden die bij de gegevensverwerkingsanalyse zijn ingevuld, beoordeeld. Op basis van de antwoorden is het mogelijk om risico's (beter) in beeld te brengen en in deze tweede fase van de DPIA te wegen. In deze fase wordt een oordeel gegeven over de rechtmatigheid, evenredigheid en noodzaak van de gegevensverwerking. Vervolgens worden de risico's en genomen en te nemen maatregelen beschreven, inclusief een inschatting van de restrisico's. De uitkomst geeft een beeld van de impact die de software of het gegevensverwerkende proces heeft op de rechten en vrijheden van degenen die hierbij betrokken zijn.

Invulinstructie

Deze 'Vragenlijst risicoanalyse DPIA' wordt beantwoord door de onderwijsinstelling. Dit gebeurt bij voorkeur door medewerkers die kennis hebben van informatiebeveiliging en/of privacy en/of betrokken zijn bij het gegevensverwerkende proces of de software waarop de DPIA van toepassing is. Alle vragen in deze risicoanalyse van de DPIA worden **vanuit het perspectief van de eigen onderwijsinstelling** beantwoord. Geef dus antwoord op de eigen software, organisatie, uitwisseling van gegevens, maatregelen et cetera.

VRAGENLIJST

Algemene informatie

In dit onderdeel vul je de algemene informatie in.

1. Naam van de organisatie
2. Naam van de invuller(s)
3. Datum
4. Naam van het (deel)proces
5. Omschrijving van de DPIA

6. Gegevensverwerkingsanalyse

Upload de bijbehorende gegevensverwerkingsanalyse en/of voeg deze hier in.

Uitgebreide risicobeoordeling en mitigerende maatregelen

De gegevensverwerkingsanalyse levert een systematische beschrijving op van de betrokkenen, categorieën persoonsgegevens, betrokken partijen, beoogde verwerkingen en verwerkingsdoeleinden.

Aan de hand van de antwoorden op de vragen in de gegevensverwerkingsanalyse is het mogelijk om een oordeel te vormen over de noodzaak en de evenredigheid van de verwerkingen in relatie tot de doeleinden.

In deze risicoanalyse van de DPIA worden verder de dreigingen en risico's geïdentificeerd en geformuleerd, de risico's geclassificeerd en eventuele mitigerende maatregelen beschreven en/of van een advies voorzien. Op basis hiervan wordt het (beoogde) restrisico bepaald. Het is de verantwoordelijkheid van het bestuur van de onderwijsinstelling en de FG om te beoordelen of dit restrisico acceptabel is en of het mogelijk is om de (beoogde) gegevensverwerking uit te voeren.

Dit DPIA-formulier vormt, samen met de eerder uitgevoerde gegevensverwerkingsanalyse, de DPIA-rapportage.

Vragen en beoordeling DPIA

7. Aanpak en procesbeschrijving DPIA

Beschrijf de aanpak en systematiek van de DPIA (bijvoorbeeld via risicoworkshops), inclusief de betrokken medewerkers en hun rol in het proces.

8. Beoordeling van het proces en totstandkoming van de gegevensverwerkingsanalyse

Geef hier het oordeel over de volledigheid en uitvoering van de gegevensverwerkingsanalyse. Beschrijf zo nodig eventuele voorbehouden of belemmeringen bij de uitvoering van de gegevensverwerkingsanalyse.

9. Zijn er eventuele algemene aanvullingen, voorbehouden of toevoegingen bij de antwoorden in de gegevensverwerkingsanalyse?
Ruimte voor samenvatting van of opmerkingen en toevoegingen over de:

- *beschrijving van het gegevensverwerkende proces*
- *beschrijving van de verwerkte persoonsgegevens*

10. Beschrijving en beoordeling van de rechtmatigheid, noodzaak en evenredigheid van de verwerkingen (in relatie tot de beschreven doeleinden van de gegevensverwerking)
Geef een oordeel (met toelichting):

- *Is de verwerking noodzakelijk?*
- *Is de verwerking proportioneel (zijn alle genoemde persoonsgegevens nodig, worden er niet te veel gegevens gevraagd en staan ze in verhouding tot de verwerkingsdoeleinden)?*
- *Kan het doel van de verwerking bereikt worden met minder of andere persoonsgegevens die minder inbreuk maken op de rechten en vrijheden van de onderwijsdeelnemers en/of medewerkers?*
- *Wordt voldaan aan de vijf vuistregels/principes (doel/doelbinding, grondslag, dataminimalisatie, transparantie, data-integriteit)?*

11. Vastgestelde risico's
Beschrijf hieronder de aanleiding voor de uitgebreide risicoanalyse en de belangrijkste gevonden risico's. Geef per risico een beschrijving van de kans dat het zich voordoet, wat de impact ervan is voor de onderwijsinstelling, welke maatregelen genomen (kunnen) worden om het risico te beperken en wat het restrisico is. Gebruik hierbij de MAPGOOD-opbouw.

Beschrijving van het risico

- Categorie: MAPGOOD
- Kans: de waarschijnlijkheid dat het risico zich voordoet (op een schaal van 1 tot 4)
- Impact: de impact op de onderwijsinstelling als het risico optreedt (op een schaal van 1 tot 4)
- Classificatie: 1 tot 16
- Maatregelen: beschrijf de maatregelen die de kans en impact beperken of verkleinen
- Restrisico: beschrijf het restrisico (kans en impact van de bedreiging ná toepassing van de beschreven maatregelen)
- Beoordeling: oordeel over dit restrisico: is het acceptabel of is er sprake van een hoog risico?
- Eigenaar: (optioneel) beschrijf bij wie de verantwoordelijkheid belegd is voor de uitvoering en controle van de maatregelen

12. Risicodashboard
Zet de uitkomsten van de risicoweging en DPIA in een risicodashboard met alle gevonden risico's, inclusief de categorisering, risicobeoordeling, beoogde maatregelen en beoogde restrisico's. Hiermee krijgt de onderwijsinstelling een schematisch overzicht van de risico's en maatregelen. Deze stap is eventueel te combineren met stap 11 ('Vastgestelde risico's').

13. Mitigerende maatregelen
Geef hieronder een opsomming van de belangrijkste maatregelen om de hoge risico's die uit de vastgestelde risico's (vraag 8) naar voren komen, te mitigeren.

14.Planning van de maatregelen
Beschrijf de planning voor te nemen mitigerende maatregelen en de evaluatie van de genomen maatregelen. De geplande datum is het moment waarop de hoge risico's zijn gemitigeerd.

15. Optioneel: herbeoordeling DPIA

Mogelijk is de uitkomst van de DPIA dat de onderwijsinstelling eerst andere maatregelen moet nemen, of dat ze technologische ontwikkelingen moet afwachten waarmee de restrisico's tot een acceptabel niveau beperkt kunnen blijven. Beschrijf op welk moment of datum een (beperkte) herbeoordeling van de (rest)risico's moet plaatsvinden of heeft plaatsgevonden.

16.Resultaat DPIA

Vat de uitkomsten van de DPIA samen, inclusief de beoordeling van de genomen en te nemen maatregelen. Neem daarbij zo nodig het advies voor het schoolbestuur of college van bestuur (bevoegd gezag) mee over de vraag of het gegevensverwerkende proces of de software waarop de DPIA is uitgevoerd, ook daadwerkelijk uitgevoerd respectievelijk gebruikt kan worden.

17. Akkoord

Geef aan wanneer en door wie deze DPIA-rapportage, het bijbehorende risicodashboard en de te nemen mitigerende maatregelen zijn beoordeeld en goedgekeurd.

Gezien FG
[Naam / datum / handtekening]

Akkoord bestuur (schoolbestuur/CvB)
[Naam / datum / handtekening]