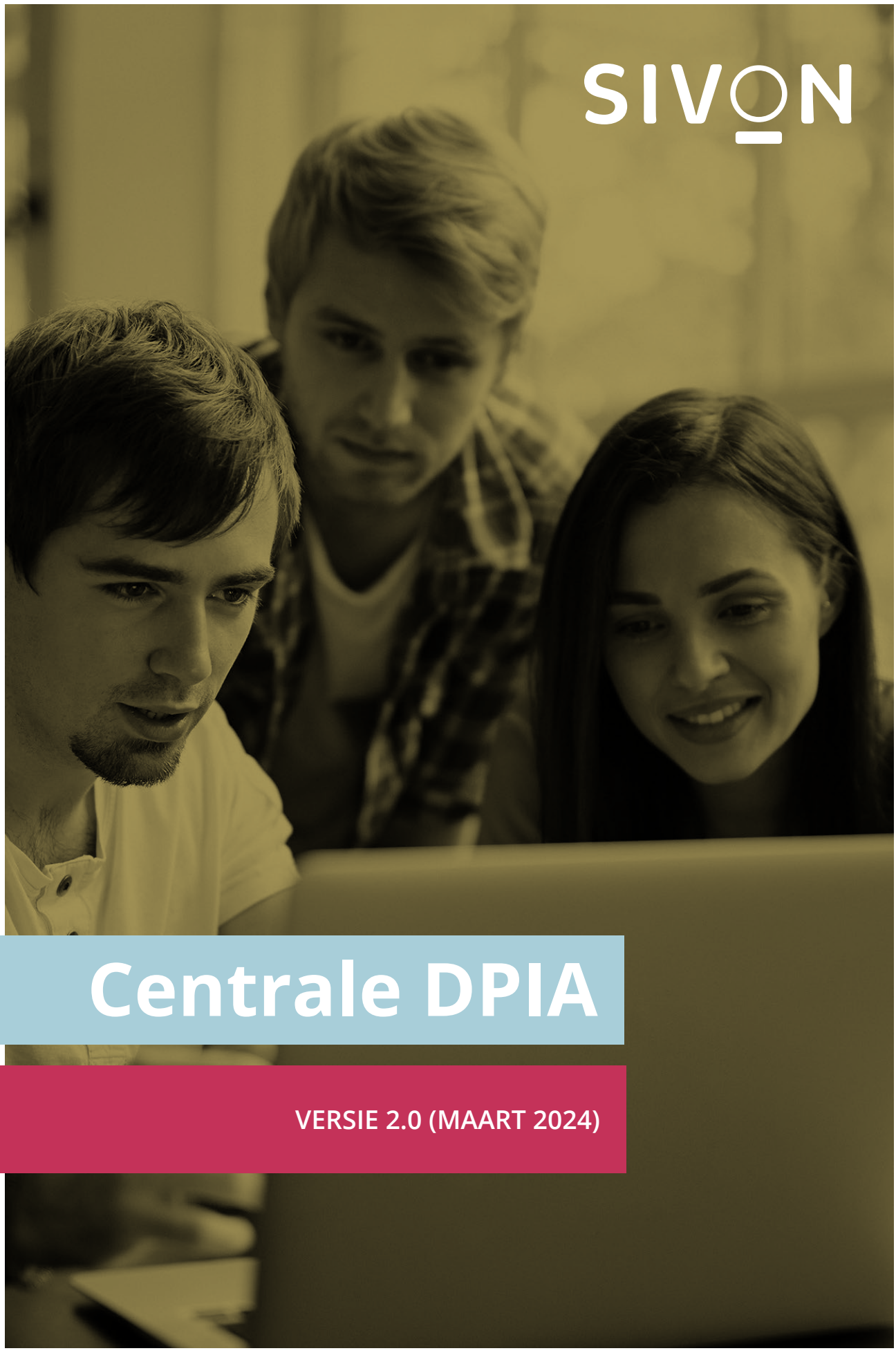


Centrale DPIA

VERSIE 2.0 (MAART 2024)

Colofon

DPIA uitgevoerd door:	Coöperatie Samen Innoveren/Inkopen/Ict voor Onderwijs Nederland U.A. (SIVON) www.sivon.nl info@sivon.nl
Betrokkenen bij uitvoering DPIA:	....
Met dank aan:	[namen en schoolbesturen] [namen leverancier]
Auteurs model DPIA	Hans-Peter Ligthart (portfoliomanager IBP SIVON) Job Vos (jurist en adviseur IBP SIVON) Ferdy IJsselmuiden (DPIA-projectmanager)

Versie beheer

Datum	Versie	Wijziging
Maart 2022	0.0	Concept (HL)
Mei 2022	1.0	Basisversie (JV)
Februari 2023	1.1	Wijzigen risico-tabel (FI)
Juni 2023	1.2	Algemene verbeteringen, opnemen proces toetsen verwerkers-overeenkomst, diverse technische vragen ondergebracht in bijlagen
Februari 2024	1.3	Aanpassingen en actualisatie (nieuw Rijksmodel 3.0)
Maart 2024	2.0	Nieuwe publieke versie

Inhoudsopgave

1. Leeswijzer 6

2. Samenvatting 7

3. Uitleg en achtergrond DPIA 8

1. Informatiebeveiliging en privacy (IBP) 8
2. Privacyconvenant en toetsing verwerkersovereenkomsten 8
3. DPIA 9
4. Verplichte uitvoering DPIA 9
5. Centrale en lokale DPIA 9
6. Methodiek DPIA 10
7. Funderend onderwijs referentie architectuur (FORA) 11

4. Motivering DPIA [applicatie] 12

1. Verplichting uitvoeren DPIA 12
2. Scope van deze DPIA 12
3. Buiten scope 12

5. Deel A: Gegevensverwerkingsanalyse 13

1. Beschrijving van het gegevensverwerkende proces 13
2. Persoonsgegevens 13
3. Gegevensverwerkingen 16
4. Verwerkingsdoeleinden 18
5. Betrokken partijen 20
6. Belangen bij de gegevensverwerking 20

7. Verwerkingslocaties 20

8. Data Transfer Impact Assessment (DTIA) 21

9. Technieken en methoden van gegevensverwerking 21

10. Juridisch en beleidsmatig kader 22

11. Bewaartermijnen 22

6. Deel B: Beoordeling rechtmatigheid gegevensverwerkingen 24

12. Rechtsgrond 24

13. Bijzondere persoonsgegevens 26

14. Doelbinding 26

15. Kinderrechten-afweging (Best Interests Assessment Children) 26

16 a. Noodzakelijkheid 28

16 b. Proportionaliteit en subsidiariteit 28

17. Rechten van de betrokkenen 28

18. Beoordeling verwerkersovereenkomst 29

7. Deel C: Beschrijving en beoordeling risico's voor de betrokkenen 31

19. Risico's 32

8. Deel D: Beschrijving voorgenomen maatregelen 34

20. Maatregelen 35

9. Deel E: MODEL lokale DPIA 37

A. Uitvoering lokale DPIA 37

B. Overwegingen over centrale DPIA 37

C. Organisatiespecifieke- en algemene applicatierisico's 37

D. Overwegingen implementatie en lokale DPIA: aanvullende risico's en maatregelen 40

E. Verklaring en advies functionaris voor gegevensbescherming (fg) 41

F. Visie betrokkenen 41

G. Conclusie 42

H. Risico-mitigerende maatregelen schoolbestuur 42

I. Aanbevelingen 43

J. Verklaring schoolbestuur 43

Bijlage 1: Gebruikte termen en definities 44

Bijlage 2: Uitleg risico's 47

Bijlage 3: Uitwerking Data Transfer Impact Assessment 48

1. Leeswijzer

Dit DPIA-rapport bestaat uit de volgende opbouw en hoofdstukken:

Hoofdstuk 1 betreft deze leeswijzer.

In hoofdstuk 2 staat de samenvatting van de uitkomsten van deze DPIA voor communicatiedoeleinden.

Hoofdstuk 3 geeft een algemene uitleg over wat een DPIA is, wanneer deze verplicht is, wat het gevolgde model is, en wat de door SIVON gevolgde methodiek is.

Hoofdstuk 4 beschrijft de applicatie waarop deze DPIA ziet, en wat er wel en niet meegenomen is in het onderzoek (scope en buiten scope).

De uitvoering van de DPIA bestaat uit de volgende onderdelen:

- Hoofdstuk 5: deel A bevat de gegevensverwerkingsanalyse (beschrijving van de gegevensverwerkingen).
- Hoofdstuk 6: deel B bevat de beoordeling van de rechtmatigheid van de gegevensverwerkingen
- Hoofdstuk 7: deel C bevat de beschrijving en beoordeling van de risico's
- Hoofdstuk 8: deel D is de beschrijving voorgenomen maatregelen die de gevonden risico's beperken
- Hoofdstuk 9: deel E is het model lokale DPIA die schoolbesturen gebruiken voor het zelf uitvoeren van deze DPIA binnen hun eigen organisatie.

Bijlage 1 bevat veelgebruikte termen en definities.

Bijlage 2 bevat een uitleg van de in deze DPIA genoemde risico's

Bijlage 3 bevat de data transfer impact assessment (DTIA) - indien van toepassing

2. Samenvatting

[Samenvatting van de risico's en maatregelen. De intentie is dat dit deel het uitgangspunt is voor een nieuwsbericht bijv. op SIVON.nl

In het nieuwsbericht wordt ook de tabel met *rest*risico's toegelicht]

3. Uitleg en achtergrond DPIA

1. Informatiebeveiliging en privacy (IBP)

In het onderwijs maken we steeds meer gebruik van persoonsgegevens en ict. We slaan steeds meer informatie op en wisselen digitaal steeds meer informatie uit. Dit doen niet alleen scholen, maar ook de leveranciers van digitale leermiddelen. Leerlingen, ouders en medewerkers willen erop kunnen vertrouwen dat scholen correct met hun gegevens omgaan en de privacy waarborgen.

Privacy is enerzijds het recht om met rust te worden gelaten. Anderzijds gaat het over het recht om gegevens over jezelf te kunnen controleren. Als je bij alles wat je doet, gevolgd wordt én je denkt of weet dat dit gevolgen voor jou kan hebben, dan pas je jouw gedrag daarop aan. Zonder het recht op privacy kan een mens niet vrij zijn. Privacy is een randvoorwaarde in een democratische samenleving. Daarom blijft het belangrijk dat scholen privacy goed organiseren. Het beschermen van privacy gaat niet zonder het beschermen van persoonsgegevens; gegevens van betrokkenen mogen immers niet in verkeerde handen vallen. Daarom spreken we vaak over IBP: Informatiebeveiliging en privacy.

2. Privacyconvenant en toetsing verwerkers-overeenkomsten

Volgens de Europese privacywet Algemene Verordening Gegevensbescherming (AVG) is een schoolbestuur eindverantwoordelijk voor de bescherming van de privacy en persoonsgegevens van leerlingen, hun ouders, en medewerkers. Het schoolbestuur wordt **verwerkingsverantwoordelijke** genoemd. Het schoolbestuur moet de controle houden over het gebruik van deze persoonsgegevens en zij bepaalt dus voor welke doelen deze gegevens mogen worden gebruikt. Een leverancier van software waarin al deze persoonsgegevens zijn opgenomen, wordt in de AVG **verwerker** genoemd. Deze mag die persoonsgegevens niet zomaar voor eigen doeleinden gebruiken. In een **verwerkersovereenkomst** legt het schoolbestuur afspraken vast met deze leverancier. In het onderwijs wordt hiervoor gebruik gemaakt van de model-verwerkersovereenkomst van het Privacyconvenant onderwijs[1].

Scholen kunnen gemakkelijk verwerkersovereenkomsten goedkeuren en digitaal ondertekenen met behulp van de Dienst Verwerkersovereenkomsten van Kennisnet[2]. SIVON toetst voor het primair en voortgezet onderwijs vooraf of de verwerkers-overeenkomsten van leveranciers van de meest-gebruikte applicaties voldoen aan de eisen van het privacyconvenant[3]. Deze rapportages zijn (binnenkort) beschikbaar in de Dienst Verwerkersovereenkomsten en [VIA HET NETWERK IBP FO].

1 https://www.privacyconvenant.nl/
2 https://www.kennisnet.nl/dienst-verwerkersovereenkomsten/
3 https://sivon.nl/toetsen-verwerkersovereenkomsten/

3. DPIA

Om vast te stellen of de gegevens van leerlingen en medewerkers (persoonsgegevens) in een applicatie, software of ict-middel veilig en verantwoord gebruikt worden, is volgens de AVG verplicht om een Data Protection Impact Assessment (DPIA) uit te voeren. In de AVG wordt dit een gegevensbeschermingseffectbeoordeling (GEB) genoemd. Een DPIA wordt uitgevoerd op een proces, applicatie of verwerking van persoonsgegevens. Meestal gaat het om een applicatie van een leverancier (verwerker). De DPIA wordt uitgevoerd volgens de eisen van artikel 35 van de AVG.

Met een DPIA wordt beoordeeld wat de risico's en (mogelijke) gevolgen zijn van het gebruik van de applicatie voor de bescherming van de persoonsgegevens van de leerlingen, hun ouders en medewerkers. Er wordt vastgesteld wordt of het gebruik van persoonsgegevens (verwerking) een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen. Als de privacyrisico's (te) hoog zijn, moet er worden gezocht naar maatregelen om deze risico's te beperken. Dit worden mitigerende maatregelen genoemd. Als de hoge risico's niet weggenomen kunnen worden, dan mag volgens de AVG deze verwerking (gebruik applicatie) niet worden uitgevoerd of voortgezet.

De uitkomst van de DPIA is o.a. een rapportage met daarin een overzicht van geclassificeerde risico's voor de rechten en vrijheden van betrokkenen. In het rapport staan ook de nodige mitigerende maatregelen benoemd. De verwerkingsverantwoordelijke stelt uiteindelijke de DPIA vast, hiermee wordt vastgesteld welke maatregelen nog moeten worden uitgevoerd en dat het schoolbestuur de resterende vastgestelde risico's accepteert.

4. Verplichte uitvoering DPIA

Deze privacytoets is verplicht als de verwerking van persoonsgegevens - gelet op de aard, de omvang, de context en de doeleinden van die verwerking - waarschijnlijk een hoog risico inhoudt voor de 'rechten en vrijheden' (privacy) van leerlingen en medewerkers. Ook is het mogelijk dat het uitvoeren van een DPIA verplicht is volgens de regels van de privacy toezichthouder Autoriteit Persoonsgegevens (AP) die een lijst gepubliceerd heeft bij welke verwerkingen het uitvoeren van aan DPIA verplicht is[4]. Voor het onderwijs betekent dit dat een DPIA altijd verplicht is op tenminste het leerlingvolg- en/of -administratiesysteem (LVS/LAS), personeelsadministratiesysteem en breed ingezette applicaties met digitaal leermateriaal.

5. Centrale en lokale DPIA

Bij applicaties die door veel verwerkingsverantwoordelijken – op dezelfde wijze – worden gebruikt, is het zinvol om deze DPIA samen uit te voeren. Denk bijvoorbeeld aan een leerlingadministratiesysteem. Hierdoor hoeft niet elk schoolbestuur zelf het spreekwoordelijke wiel uit te vinden. SIVON voert daarom in opdracht van OCW namens het primair en voortgezet onderwijs **centrale DPIA's** uit. Deze DPIA's worden door SIVON

4 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf

uitgevoerd namens een aantal schoolbesturen (leden) als verwerkingsverantwoordelijke(n). Door hierbij samen op te trekken met verschillende schoolbesturen die hun ervaring uit de onderwijspraktijk meebrengen, wordt expertise en ervaring samengebracht. Ook is het makkelijker om afspraken te maken met de leverancier als er aanvullende mitigerende maatregelen moeten worden getroffen omdat SIVON namens de leden spreekt. Door deze centrale DPIA's uit te voeren op veel gebruikte systemen, helpt SIVON leerlingen en medewerkers aan een digitale veilige leeromgeving.

Schoolbesturen moeten volgens de AVG zelf als verwerkingsverantwoordelijke een DPIA uitvoeren en zelf de risico's afwegen. Dat kan SIVON niet doen. Na de uitvoering van de centrale DPIA moet daarom ieder schoolbestuur de uitkomsten uit de centrale DPIA op hun organisatie toepassen. We noemen dit een **lokale DPIA**. In deze lokale DPIA weegt het schoolbestuur de door SIVON gevonden risico's, identificeert eventuele aanvullende risico's en bepaalt zij zelf of er binnen het schoolbestuur nog mitigerende maatregelen moeten worden genomen.

SIVON helpt besturen hiermee doordat in de centrale DPIA de meest voorkomende risico's voor schoolbesturen worden bepaald. Het uitvoeren van een lokale DPIA is wel altijd noodzakelijk: SIVON heeft een algemene, centrale DPIA uitgevoerd en kan geen rekening houden met mogelijke lokale risico's van gebruik van het systeem op scholen.

6. Methodiek DPIA

SIVON volgt bij de uitvoering van de centrale DPIA het model van de Rijksoverheid[5], aangevuld met onderwijs-specifieke informatie uit de *Handleiding uitvoeren data protection impact assessment (DPIA) voor het po en vo (versie 1.0)*[6]. Het model is daarnaast aangepast aan specifieke informatie over de applicatie en aangevuld met een model lokale DPIA voor schoolbesturen. Er wordt rekening gehouden met Europese richtlijnen van de gezamenlijke Europese toezichthouders (EDPB) waaronder de "Richtsnoeren voor gegevensbeschermingseffectbeoordelingen (2016/679, 4 april 2017)".

SIVON voert bij de uitvoering van de centrale DPIA de volgende activiteiten uit:

- Beschrijving van de (methoden van) gegevensverwerkingen (gegevensverwerkingsanalyse) en toegepaste (beveiligings)technieken;
- Beoordeling van de rechtmatigheid van de gegevensverwerkingen, inclusief afweging van kinderrechten;
- Beschrijving en beoordeling risico's voor de betrokkenen;
- Beschrijving en beoordeling van (eventuele) voorgenomen maatregelen die de gevonden (privacy) risico's beperken;
- Toetsen van de verwerkersovereenkomst:
- Beoordeling beveiligingsmaatregelen aan de hand van de BIV-classificatie en het ROSA certificeringsschema;
- Beoordeling van de mogelijkheden om te voldoen aan rechten van betrokkenen;
- Beoordeling van de default settings (privacy by design);
- Technologie-scan naar gebruikte webtechnologiën

5 Model DPIA Rijksdienst v3.0.pdf (kcbr.nl)
6 https://aanpakibp.kennisnet.nl/app/uploads/Handreiking-DPIA-v1.0-1.pdf

- Analyse van de wijze waarop het systeem voorziet in logging en de wijze waarop dit door de onderwijsinstelling gemonitord en gecontroleerd kan worden;
- Uitvoeren van test-script gevolgd door inzage verzoek bij leverancier;
- Overleg met betrokken schoolbesturen en leverancier over (aanvullende) mitigerende maatregelen;
- Opstellen en bespreken DPIA-rapportage.

7. Funderend onderwijs referentie architectuur (FORA)

Gebruik FORA: Funderend Onderwijs Referentie Architectuur

Applicatie landschap

Het hebben van een architectuur helpt bij het tijdig en goed reageren op zakelijke of juridische (AVG) eisen en/of (externe) dreigingen die een (mogelijke) aanpassing in de informatiehuishouding vragen. (Norm 1.4 architectuur van het Normenkader IBP https://aanpakibp.kennisnet.nl/normenkader/)

Voor het funderend onderwijs is de FORA (Funderend Onderwijs Referentie Architectuur) ontwikkeld. (https://fora.wikixl.nl/index.php/Hoofdpagina)

FORA is een gestandaardiseerde methodiek die inzicht geeft in verplichte processen en onderwijsactiviteiten in het primair en voortgezet onderwijs.

De FORA biedt inzicht in wat de bedrijfsfuncties zijn van een po en vo school. Het hoofd-bedrijfsfunctiemodel beschrijft op hoofdlijnen wat een onderwijsorganisatie doet. Verdieping daarvan vindt plaats in het bedrijfsfunctiemodel dat in meer detail weergeeft op welke manier een invulling gegeven wordt aan het ‘wat’. Hiermee is het mogelijk om ‘referentiecomponenten’ toe te voegen. Referentiecomponenten zijn typen systemen - zoals een LAS, een Toetssysteem, of een ELO - met bijbehorende functionaliteiten (‘applicatiefuncties’).

In deze DPIA gebruiken we FORA om een applicatie te kunnen plaatsen in het applicatie landschap. (welke plaats neemt de applicatie in in het totaal aan applicatie die een school gebruikt

SIVON voert centrale DPIA’s uit op een applicatie. Een applicatie kan in de FORA vertaald worden naar een of meerdere kan een of meerdere referentie componenten https://fora.wikixl.nl/index.php/Referentiecomponentenmodel

Een referentiecomponent is een functionele afbakening van een modulair, zelfstandig inzetbaar en vervangbaar (deel van een) systeem.

4. Motivering DPIA [applicatie]

1. Verplichting uitvoeren DPIA

Bij gebruik van [applicatie] door schoolbesturen is het uitvoeren van een DPIA verplicht omdat sprake is van:

- grootschalige verwerkingen en/of stelselmatige monitoring van financiële gegevens waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden;
- grootschalige verwerkingen van gegevens over gezondheid;
- grootschalige en/of stelselmatige monitoring van openbaar toegankelijke ruimten door middel van cameratoezicht;
- grootschalige verwerkingen van persoonsgegevens waarbij op stelselmatige wijze via geautomatiseerde verwerking gedrag van natuurlijke personen geobserveerd of beïnvloed (observatie en beïnvloeding van gedrag);

2. Scope van deze DPIA

[Korte beschrijving over welke applicatie, en daar onder vallende modules/processen, deze DPIA gaat en waarvoor deze wordt gebruikt]

3. Buiten scope

[Beschrijving van de diensten die buiten scope vallen]

5. Deel A: Gegevensverwerkingsanalyse

In dit hoofdstuk wordt een gegevensverwerkingsanalyse uitgevoerd: een uitgebreide beschrijving van de gegevensverwerking. Op gestructureerde wijze worden de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen beschreven.

1. Beschrijving van het gegevensverwerkende proces

Beschrijf op hoofdlijnen waar de DPIA op ziet. Wat is het systeem, uit welke modules en/of processen bestaat het en wat is het voorziene gebruik en toepassing in de onderwijspraktijk?

2. Persoonsgegevens

In dit onderdeel wordt beschreven welke categorieën persoonsgegevens van welke betrokkenen worden verwerkt binnen het systeem. Zie ook de definitiebepalingen onder IX.

Betrokkenen

Geef een beschrijving van de categorieën betrokkenen wiens persoonsgegevens worden verwerkt. De AVG biedt specifieke bescherming aan kwetsbare betrokkenen zoals kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader. Maak hierbij kenbaar of het mogelijk gaat om kwetsbare betrokkenen (zoals minderjarigen, verstandelijk gehandicapten, mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven, etnische minderheden, of vluchtelingen).

Voorbeelden:

- Leerlingen
- Wettelijk vertegenwoordigers
- Medewerkers (loondienst)
- Medewerkers (extern/detachering)
- Alumni
- Oud-medewerkers
- Leveranciers
- Partners (samenwerking)

Persoonsgegevens

Geef per categorie van aan van welke categorie betrokkenen, welke typen persoonsgegevens verwerkt worden: gewoon, gevoelig, bijzonder, strafrechtelijk en/of wettelijk identificatienummer.

Voorbeelden:

- Contactgegevens: naam, e-mail en org.eenheid
- Contactgegevens: geboortedatum en geslacht
- Contactgegevens ouder/verzorger
- Studentennummer/leerlingnummer
- Nationaliteit[7] en geboorteplaats
- Gezondheidsgegevens
- Godsdienst
- Studievoortgang (exam.,traject voortg., begeleiding, medisch dos., klas leerj. opleid.)
- Onderwijsorganisatie (roosters, boekenlijsten, etc.)
- Financiën (volledige cyclus)
- Beeldmateriaal (b.v. pasfoto, camera beelden enz.)
- Docenten, mentoren en mbo adviseur
- BSN/PGN

7 Het gegeven 'nationaliteit' op zichzelf is geen bijzonder persoonsgegeven en wordt ook niet zo genoemd in de AVG en de UAVG als zodanig. Maar een persoonsgegeven is niet alleen bijzonder wanneer het direct het desbetreffende bijzondere persoonsgegeven onthult, ook gegevens die indirect dergelijke informatie onthullen, dienen aangemerkt te worden als bijzondere categorieën van persoonsgegevens.

Tabel 3.1 Persoonsgegevens

Categorie persoonsgegevens	Leerling	Medewerker	Ouder/voogd/ verzorger	Overig	Bron verkrijging
Algemene contactgegevens	Voorna(a)me(en) Voorletter(s) (s)Achternaam Geslacht Woonadres Postcode Woonplaats Telefoonnummer E-mailadres (privé) Emailadres (school)				Betrokkene School
Onderwijsdeelnmernummer	Een administratienummer dat onderwijsdeelnemers identificeert				
ECK-ID					
Nationaliteit					
Geboortedatum					
Geboorteplaats					
Financiële gegevens met het oog op het berekenen, vastleggen en innen van gelden en bijdragen.	Bankrekeningnummer Facturenadministratie				
Gegevens over gezondheid					
Godsdienst					
Feiten en waarderingen over iemand zijn gedragingen, eigenschappen of opmerkingen					
Studievoortgang	Klas, leerjaar, ILT-code Examinering Studievoortgang en/of studietraject Begeleiding Onderwijsdeelnemers, inclusief handelingsplan Aan- en afwezigheidsregistraties				
Personeelsnummer					
Gebruikersgegevens	Diagnostische gegevens, loggegevens, metadata, anders namelijk				
Ervaringen (werkervaring en opleidingen)					
Beeldmateriaal	Foto's en videobeelden (beeldmateriaal) van betrokkene met of zonder geluid van activiteiten van de onderwijsinstelling				
Verzuimregistratie					
Burgerservicenummer (BSN) of PGN[8] (Persoonsgebonden nummer)					
Overige gegevens					

8 https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/burgerservicenummer-bsn/bsn-in-het-onderwijs#:~:text=Iedereen%20die%20onderwijs%20volgt%20dat,aan%20het%20Burgerservicenummer%20(BSN).

3. Gegevensverwerkingen

In dit onderdeel beschrijf je in algemene bewoordingen alle gegevensverwerkingen. Onder verwerking van persoonsgegevens wordt verstaan: elke bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens. Met een bewerking wordt iedere handeling bedoeld die met een persoonsgegeven kan worden verricht.

Om de rechtmatigheid te kunnen beoordelen, is het noodzakelijk alle gegevensverwerkingen in beeld te krijgen. Denk hierbij aan het gehele verwerkingsproces, hoe het systeem past in het applicatielandschap, de koppelingen en de gegevensstromen van en binnen het schoolbestuur. Het gaat er hier vooral om een beeld te schetsen van de scope van de gegevensverwerkingsanalyse. Maak hiervoor gebruik van een referentiearchitectuur (de FORA[9] voor het primair en voortgezet onderwijs).

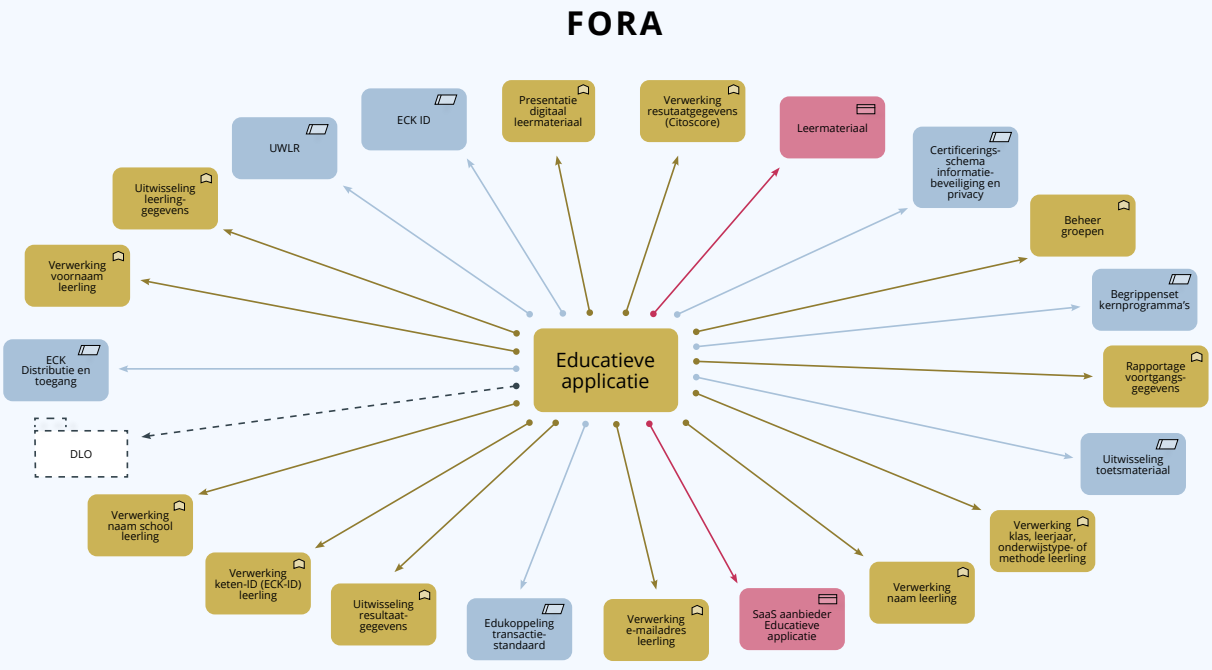
Applicatielandschap

Neem hierbij een korte beschrijving op van het applicatielandschap van het schoolbestuur waarbinnen het systeem wordt gebruikt. DOEL: hulpmiddel om te komen tot oplossing.

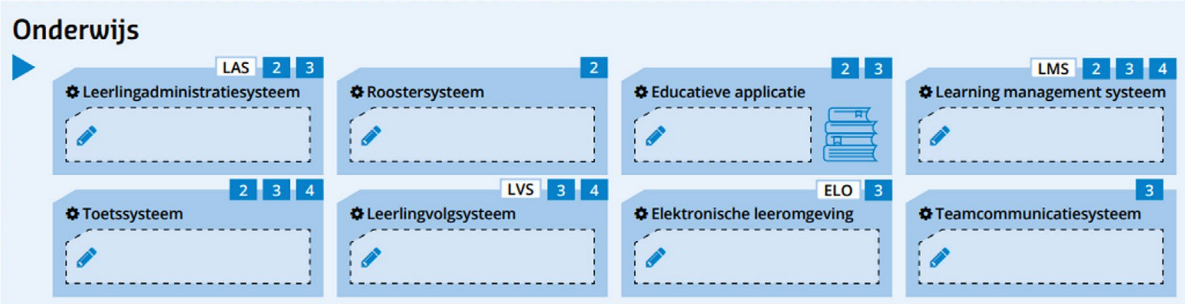
Schets de applicatie in de context van het applicatielandschap, zie link en FORA.
Educatieve applicatie - Funderend Onderwijs Referentie Architectuur (wikixl.nl)

Bijvoorbeeld:

Contextdiagram



9 https://www.wikixl.nl/wiki/fora/index.php/DPIA



Koppelingen

Een korte beschrijving van de van toepassing zijnde (externe) koppelingen van het systeem met andere systemen en processen. Beschrijf tevens op welke manier de gegevens tijdens de overdracht zijn beveiligd.

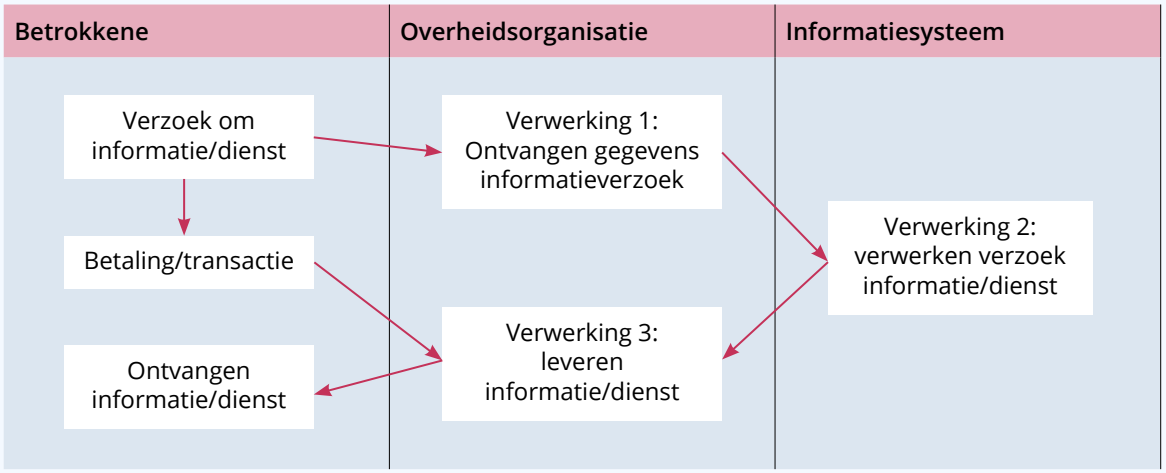
Gegevensstromen/stroomschema

Omdat de gegevensverwerkingen gecompliceerd kunnen zijn en het niet altijd gemakkelijk is om het geheel van gegevensverwerkingen in woorden uit te drukken kan het van belang zijn om de gegevensverwerkingen te visualiseren, bijvoorbeeld aan de hand van een input-proces-output model, stroomschema of workflow.

Let hierbij op:

- benoem alle betrokken partijen (punt 5) in het stroomschema
- geef de AVG-rol aan van iedere betrokken partij
- Herkomst data
- geef zo nodig duidelijk aan over welke gegevensverwerkingen de DPIA gaat
- voeg per gegevensverwerking toe of specifieke applicaties, software, online platformen of cloud opslag wordt gebruikt.

Voorbeeld DPIA Rijksmodel 3.0



4. Verwerkingsdoeleinden

De AVG heeft het uitgangspunt dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. De vaststelling van de verwerkingsdoeleinden is een noodzakelijke voorwaarde om te kunnen beoordelen of de gegevensverwerkingen rechtmatig zijn (onderdeel B) en om vast te stellen welke maatregelen getroffen dienen te worden om de risico's (onderdeel C) te voorkomen of te verkleinen (onderdeel D).

Gebruik de FORA[10] om de verwerkingsdoeleinden te bepalen. Maak de vertaling van applicatie naar referentie component en bekijk per referentie component voor welke bedrijfsprocessen deze gebruikt wordt. De bedrijfsprocessen zijn de doelen.

Bijvoorbeeld: De applicatie is het referentie component Leerlingadministratiesysteem.
De relatie tussen referentie component en bedrijfsfuncties wordt gebruikt als definitie van het doel van de verwerking. "Het Digitaal leerlingadministratiesysteem van een schoolbestuur. Hiermee wordt het totaal van informatiesystemen en modules aangeduid die een schoolbestuur gebruikt voor het beheren van aanmeldingen, inschrijvingen en resultaten van leerlingen."

De verwerkingsdoeleinden sluiten aan bij de in het Privacyconvenant[11] opgenomen verwerkingsdoeleinden:

Selecteer van toepassing zijnde doeleinden

a) de opslag van leer- en toetsresultaten;
b) het terugontvangen door het schoolbestuur van leer- en toetsresultaten;
c) de beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een Onderwijsdeelnemer;
d) analyse en interpretatie van leer- en toetsresultaten;
e) het kunnen uitwisselen van leer- en toetsresultaten tussen Digitale Onderwijsmiddelen;
f) de indeling en aanpassing van roosters;
g) het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgen van onderwijs;
h) het begeleiden en ondersteunen van leerkrachten / docenten en andere medewerkers binnen het schoolbestuur;
i) de communicatie met Onderwijsdeelnemers en ouders en medewerkers van het schoolbestuur;
j) monitoring en verantwoording, met name ten behoeve van: (prestatie)metingen van het schoolbestuur, kwaliteitszorg, tevredenheidsonderzoek, effectiviteitsonderzoek van onderwijs(vormen) of de geboden ondersteuning van Onderwijsdeelnemers bij passend onderwijs;
k) het voor zover noodzakelijk en wettelijk toegestaan uitwisselen van Persoonsgegevens met Derden, waaronder:
   - toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak;
   - samenwerkingsverbanden in het kader van passend onderwijs en regionale samenwerkingen;
   - partijen betrokken bij de invulling van stage- of leer-werkplekken;

10 https://fora.wikixl.nl/index.php/Hoofdpagina en https://fora.wikixl.nl/index.php/DPIA
11 https://www.privacyconvenant.nl/downloads

- het leveren van Persoonsgegevens aan schoolbesturen in geval van overstappen tussen schoolbesturen en bij vervolgonderwijs;
- het in opdracht van het schoolbestuur leveren van Persoonsgegevens aan een andere partij;

l) het geleverd krijgen / in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen het schoolbestuur en de Leverancier;

m) het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;

n) de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens;

o) de continuïteit, verbetering en de goede werking van het Digitale Onderwijsmiddel in opdracht van het schoolbestuur conform de afspraken die zijn gemaakt tussen het schoolbestuur waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen onder andere na geconstateerde fouten of onjuistheden, en het krijgen van ondersteuning;

p) het door het schoolbestuur beschikbaar kunnen stellen van (geanonimiseerde of gepseudonimiseerde) Persoonsgegevens voor wetenschappelijk onderzoek of statistische doeleinden ten behoeve van het (optimaliseren van het) leerproces of het beleid van het schoolbestuur op basis van strikte voorwaarden vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek;

q) het door het schoolbestuur voor onderzoeks- en analysedoeleinden beschikbaar kunnen stellen van geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren;

r) het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen;

s) het behandelen van geschillen;

t) financieel beheer;

u) de uitvoering of toepassing van een Unierechtelijke of lidstaatrechtelijke wettelijke bepaling of regeling.

De verwerkingsdoeleinden zijn schematisch weergegeven en gekoppeld aan de verwerking

Tabel 4.1 Verwerkingsdoeleinden en verwerking

Doeleinde verwerking (par.4. Verwerkingsdoeleinden)	Gegevensverwerking (par.3 Gegevensverwerkingen)	Toelichting
Beheer personeelsgegevens	Opslaan, wijzigen, raadplegen, gebruiken, verwijderen gegevens van alle betrokkenen (alle categorieën betrokkenen)	Ruimte voor toelichting

5. Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, sub-verwerker, leverancier, derde en of ze verstrekker of ontvanger zijn.
Benoem tevens welke personen/functies binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Tabel 5.1 Betrokken partijen en gegevensverwerking

Naam partij	AVG-rol	Functie/taak	Betrokken persoonsgegevens	Verstrekker of ontvanger
Schoolbestuur	Verw. Verant.	Werkgever	Alle pgg die een schoolbestuur invoert	V

6. Belangen bij de gegevensverwerking

Beschrijf alle belangen die de hiervoor genoemde betrokken partijen hebben bij de gegevensverwerkingen. Het benoemen van het benoemen van het belang is relevant in het kader van de toetsing van de noodzakelijkheid van de verwerking.

Voorbeelden:

- Bedrijfsbelangen,
- Financiële en commerciële belangen,
- Het handhaven van juridische vorderingen,
- Toezicht op medewerkers ten behoeve van de veiligheid
- Managementdoeleinden, (nationale of openbare) veiligheid, zoals de preventie van fraude, misbruik en netwerkbeveiliging,
- Gezondheidsredenen.

7. Verwerkingslocaties

Beschrijf waar en in welke landen de voorgenomen gegevensverwerkingen plaatsvinden. Beschrijf de wijze van doorgifte dat van toepassing is wanneer verwerkingslocaties buiten de Europese Economische Ruimte bevinden: hoe worden gegevens getransporteerd naar buiten de EER?

[beschrijving feitelijke doorgifte van persoonsgegevens aan landen + specificatie buiten de EER]

Tabel 7.1 Verwerkingslocaties

Naam partij	Statutaire vestigingsplaats (sub-) verwerker	Beknopte omschrijving taak/dienst waaruit blijkt welke informatie wordt verwerkt door deze subverwerker	Plaats/land van opslag en verwerking persoonsgegevens en doorgifte mechanisme indien buiten de EER

8. Data Transfer Impact Assessment (DTIA)

De AVG bevat specifieke regels voor de doorgifte van persoonsgegevens naar landen buiten de Europese Economische Ruimte (EER). In beginsel mogen persoonsgegevens alleen worden overgedragen aan landen buiten de EER als het land een 'passend beschermingsniveau' heeft. Dat niveau kan op verschillende manieren worden bepaald: een multinational kan bindende bedrijfsvoorschriften vaststellen (BCR's), de EU-standaardcontractbepalingen (SCC) toepassen of alleen overdragen aan landen waarvoor de Europese Commissie een zogeheten adequaatheidsbesluit[12] heeft genomen. De DTIA is uitgewerkt in bijlage 3: Uitwerking DTIA.

Het resultaat van de risicobeoordeling in het kader van de DTIA is dat [conclusie].

Beheersmaatregelen:

- transparantie (transparency reports),
- encryptie, pseudonimiseren/aggregeren,
- privacytoezeggingen (privacy pledges),
- datagrenzen (data boundaries),
- EDPB onderzoek naar clouddiensten.

9. Technieken en methoden van gegevensverwerking

Artikel 32 van de AVG schrijft voor dat er passende technische en organisatorische maatregelen genomen moeten worden om een op het risico afgestemd beveiligingsniveau te waarborgen. Om inzicht te krijgen in welke mate er vorm wordt gegeven aan deze abstracte formulering wordt gebruik gemaakt van de voor de verwerkers opgestelde standaard DPIA-vragenlijst. Deze vragenlijst wordt door de verwerker gevuld en zal voor een belangrijk deel inzicht geven in o.a. de genomen technische beheersmaatregelen en informatiebeveiliging. Gebruikmaking van bepaalde technieken en methoden van gegevensverwerking kunnen aanvullende risico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Dit is onder meer het geval bij (semi-)geautomatiseerde besluitvorming, AI/algoritmes, cloud, nieuwe technologie, profilering en big data-verwerkingen.

12 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Voorts is er technisch onderzoek verricht naar [SYSTEEM], welke uitkomsten en bevindingen als volgt zijn meegenomen in deze DPIA:

[beschrijving uitkomsten]

IAMA: mensenrechten in beeld bij algoritmes

Indien uit voornoemde vragenlijst blijkt dat er gebruik wordt gemaakt van AI technologie zal beoordeeld worden of er sprake is van een hoog risico.

Indien er sprake is van een hoog risico algoritme kan aan de hand van de uitvoering van een Impact Assessment Mensenrechten en Algoritmes (IAMA) inzichtelijk worden gemaakt of deze voldoet aan de wettelijke verplichtingen en of er sprake is van een verantwoorde inzet van AI en algoritmen.

10. Juridisch en beleidsmatig kader

Benoem alle wet- en regelgeving, en het beleid van het schoolbestuur, met mogelijke gevolgen voor de gegevensverwerkingen.

Voor het benoemen van de wet- en regelgeving en beleid die van toepassing zijn op het verwerkingsproces is het aan te raden om deze in hiërarchische wijze in een overzicht op te nemen. Bijvoorbeeld:

- [Internationale verdragen];
- [Europese verdragen, verordeningen, richtlijnen en besluiten];
- [Nationale wetgeving];
- [AMvB's, gemeentelijke verordeningen, algemeen verbindende voorschriften]; en [Intern beleid]

11. Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden. Worden bijvoorbeeld bewaartermijnen gehanteerd volgens het door de instelling vastgestelde beleid? Maak gebruik van het landelijk vastgestelde sectoraal beleid[13].

Zijn er standaard termijnen in het systeem van toepassing, wat zijn de zelf in te stellen mogelijkheden? Is er een standaard regulier opschoonactie of is dit gebonden aan een knop? Welke termijn hanteert de leverancier als data verwijderd is door beheerder? En na het beëindigen van het contract?

13 https://aanpakibp.kennisnet.nl/bewaartermijnen/

Tabel 11.1 Bewaartermijnen

Gegevensverwerking (tabel 4.1)	Bewaartermijn	Motivatie bewaartermijn
Informatieverzoek vanuit betrokkene	Gegevens worden aan het einde van de dag op de dag van het informatieverzoek automatisch verwijderd uit het systeem	Informatie over verzoeken van betrokkenen worden niet gebruikt na afandeling verzoek. Geen noodzaak om langer te bewaren dan een dag na verzoek.
Verwerken declaratieformulieren	Ten minste 7 jaar bewaard vanwege verplichting bewaren financiële administratie. Jaarlijks wordt gecontroleerd welk deel van de financiële administratie meer dan 7 jaar oud is en kan worden verwijderd.	Wettelijke verplichting op basis van de Algemene wet inzake Rijksbelastingen

6. Deel B: Beoordeling rechtmatigheid gegevensverwerkingen

In dit hoofdstuk wordt de rechtmatigheid van de gegevensverwerkingen beoordeeld. Het gaat om de rechtsgrond, noodzakelijkheid (proportionaliteit en subsidiariteit) en doelbinding, transparantie van de leverancier over de voorgenomen gegevensverwerkingen en de rechten van de betrokkene.

12. Rechtsgrond

Bepaal op welke grondslag(en) de gegevensverwerkingen zijn gebaseerd.

Artikel 6 AVG lid

a) Toestemming van de betrokkene (art.6. eerste lid, sub a, AVG)
b) Uitvoering van een overeenkomst (art.6, eerste lid, sub b, AVG)
c) Wettelijke verplichting[14] (art.6, eerste lid, sub c, AVG)
d) Vitaal belang van de betrokkene (art.6, eerste lid, sub d, AVG)
e) Taak van algemeen belang[15] (of openbaar gezag) (art.6, eerste lid, sub e, AVG)
f) Gerechtvaardigd belang (art. 6. eerste lid, sub f, AVG)

Tabel 12.1 Rechtsgrond

Verwerkingsdoeleinden (zie hiervoor 4. Verwerkingsdoeleinden)	Grondslag AVG	Relevante wet- en regelgeving (wettelijke verplichting/taak van algemeen belang)
Beheer personeelsgegevens Kopieer de tabel bij 4.1	Uitvoeren overeenkomst	N.v.t.

Onderbouwing gerechtvaardigd belang (indien van toepassing)

Bij het beoordelen van de rechtmatigheid van gegevensverwerking op basis van het gerechtvaardigd belang, is het belangrijk om te voldoen aan de volgende voorwaarden.

Naam verwerking/doeleinde:

14 De wettelijke verplichting (rechtsgrond c) hoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken. Ook is mogelijk dat de verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht of wettelijke verplichting. Zonder verwerking van de persoonsgegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn.

15 Met betrekking tot rechtsgrond taak van algemeen belang geldt dat deze taak zal moeten blijken uit regelgeving die op de verwerkingsverantwoordelijke van toepassing is. Niet noodzakelijk is dat in de regelgeving expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak persoonsgegevens verwerkt mogen worden. Indien het noodzakelijk is om voor de uitvoering van de publieke taak persoonsgegevens te verwerken, kan de wettelijke grondslag voor de publieke taak ook worden beschouwd als grondslag voor de verwerking van persoonsgegevens.

Voorwaarden voor gerechtvaardigd belang	Beschrijving
Beoordeel of er een gerechtvaardigd belang achter de verwerking zit	Onderwerpen die beoordeeld moeten worden in de afweging. • Waarom wilt u de gegevens verwerken? • Welk voordeel verwacht u te halen uit de verwerking? • Hebben derden baat bij de verwerking? • Zijn er bredere publieke voordelen aan de verwerking? • Hoe belangrijk zijn de voordelen die u hebt geïdentificeerd? • Wat zou de impact zijn als je niet door kon gaan met de verwerking? • Voldoet u aan specifieke regels voor gegevensbescherming die van toepassing zijn op uw verwerking (bijvoorbeeld profileringsvereisten of e-privacywetgeving)? • Voldoet u aan andere relevante wetten? • Voldoet u aan de richtlijnen of gedragscodes van de industrie? • Zijn er nog andere ethische problemen met de verwerking?
Beoordeel of de verwerking noodzakelijk is voor het doel dat u hebt geïdentificeerd	• Zal deze verwerking u daadwerkelijk helpen uw doel te bereiken? • Staat de verwerking in verhouding tot dat doel? • Kunt u hetzelfde doel bereiken zonder de verwerking? Kunt u hetzelfde doel bereiken door minder gegevens te verwerken of door de gegevens op een andere meer voor de hand liggende of minder opdringerige manier te verwerken
Beoordeel de impact op de belangen en rechten en vrijheden van de betrokkene	• Zijn het gegevens van speciale categorieën of gegevens over strafbare feiten? • Zijn het gegevens die betrokkene waarschijnlijk als bijzonder 'privé' beschouwen? • Verwerkt u gegevens van kinderen of gegevens met betrekking tot andere kwetsbare personen? • Zijn de gegevens over betrokkene persoonlijk of professioneel?
Beoordeel of de verwerking in overeenstemming is met de redelijke verwachtingen van de betrokkene.	• Heeft u een bestaande relatie met de betrokkene? • Wat is de aard van de relatie en heeft u in het verleden eerder gegevens gebruikt? • Heeft u de gegevens rechtstreeks van de betrokkene verzameld? Wat heeft u ze toen verteld? • Als u de gegevens van een derde partij hebt verkregen, wat hebben zij de betrokkene dan verteld over hergebruik door derden voor andere doeleinden en geldt dit voor u? • Hoe lang geleden heeft u de gegevens verzameld? Zijn er sindsdien veranderingen in technologie of context die de verwachtingen zouden beïnvloeden? • Wordt uw beoogde doel en methode breed begrepen? • Bent u van plan om iets nieuws of innovatiefs te doen? • Heeft u enig bewijs over verwachtingen – bijvoorbeeld van marktonderzoek, focusgroepen of andere vormen van overleg? • Zijn er andere factoren in de specifieke omstandigheden die betekenen dat ze de verwerking wel of niet zouden verwachten?
Waarschijnlijke impact	• Wat zijn de mogelijke effecten van de verwerking op betrokkene? • Verliezen betrokkenen de controle over het gebruik van hun persoonsgegevens? • Wat is de waarschijnlijkheid en ernst van mogelijke gevolgen? • Zullen sommige betrokkenen waarschijnlijk bezwaar maken tegen de verwerking of deze opdringerig vinden? • Wilt u de verwerking graag uitleggen aan particulieren? • Kunt u waarborgen nemen om de impact tot een minimum te beperken?

De antwoorden op de voorwaarden uit de bovenstaande tabel vormen de basis om te beslissen of de grondslag van het gerechtvaardigd belang kan worden toegepast.

Voor deze verwerking kan een succesvol beroep worden gedaan op het gerechtvaardigde belang	Ja/Nee

13. 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.

14. 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. Neem hierbij in overweging of de doelen uitdrukkelijk en welbepaald zijn. *Controleer of:*

- 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
- het verband tussen het oorspronkelijke doel en het nieuwe/toekomstige doel;
- de context waarin de persoonsgegevens worden verzameld (wat is de relatie tussen de verwerkingsverantwoordelijke en de betrokkene?)
- de soort en aard van de persoonsgegevens (gaat het om gevoelige of bijzondere persoonsgegevens?)
- de mogelijke gevolgen van de verdere verwerking (wat zijn de gevolgen voor de betrokkene?)
- het bestaan van passende waarborgen voor de gegevensverwerking (bv. versleuteling van persoonsgegevens en anonimisering of pseudonimisering).

15. Kinderrechten-afweging (Best Interests Assessment Children)

Artikel 3 van het Verdrag inzake de rechten van het kind, schrijft voor dat bij alle maatregelen betreffende kinderen - ongeacht of deze worden genomen door openbare of particuliere instellingen, rechterlijke instanties, bestuurlijke autoriteiten of wetgevende lichamen - de belangen van het kind de eerste overweging (moeten) vormen. Deze belangenafweging gaat verder dan een veilige gegevensverwerking maar ziet ook op de mogelijke gevolgen van de verwerking. Met schoolbesturen als leden van SIVON in het primair en voortgezet onderwijs, betekent dit dat SIVON in haar DPIA's rekening houdt met o.a. gebruikers (betrokkenen) in de leeftijd van 4 tot 18 jaar (of ouder). Kinderen hebben recht op specifieke bescherming van hun persoonsgegevens. Dit volgt uit het feit dat zij zich minder bewust zijn van de risico's, gevolgen en waarborgen en van hun rechten in verband met de verwerking van hun persoonsgegevens. SIVON geeft hier in deze DPIA invulling aan door af te wegen of het gebruik van het [SYSTEEM] en/of de gegevensverwerking(en) die daarmee samenhangen, in het belang zijn van de betrokkenen (kind/leerling als betrokkene). SIVON maakt hierbij gebruik van de systematiek van de best interests assessment children van de Britse ICO[16].

16 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/best-interests-self-assessment/

De afweging bestaat uit 4 stappen:

1. Wat zijn de (relevante) rechten van kinderen in het kader van deze DPIA?

Bepaal en beschrijf hier welke rechten[17] van en voor kinderen relevant zijn in het kader van deze DPIA. Ga hierbij uit van de leeftijd van de kinderen (leeftijdsadequaat). Overweeg in het bijzonder of de gegevensverwerking (negatieve) gevolgen heeft voor de ondersteuning en van de behoeften van het kind op het gebied van veiligheid, gezondheid, welzijn, familierelaties, fysieke, psychologische en emotionele ontwikkeling, identiteit, vrijwaring van economische commerciële en/of fysieke uitbuiting, vrijheid van meningsuiting, privacy en de mogelijkheid om een eigen mening te vormen en deze te laten horen, het belang van toegang tot informatie, omgang met anderen en spel (buiten spelen) om de ontwikkeling van het kind te ondersteunen. Het gaat er om dat het kind zich om in overeenstemming met zijn of haar ontwikkelende capaciteiten, een stem heeft (kan hebben) in zaken die hem of haar aangaan.

Indien het [SYSTEEM] gebruikt kan worden door kinderen, dan wordt overwogen of het gebruik van de applicatie leeftijdsadequaat is en past bij de leeftijd van de leerlingen. De leeftijdscategorie en de verschillende behoeften van kinderen van verschillende leeftijden en ontwikkelingsstadia moeten centraal staan bij het ontwerpen van [SYSTEEM] en de daarmee samenhangende gegevensverwerkingen.

2. Identificeer het effect van de gegevensverwerking en gebruik van [SYSTEEM] op deze rechten

Beschrijf of, hoe, waarom en wanneer het [SYSTEEM] en gegevensverwerking (potentiële) gevolgen heeft of kan hebben voor de rechten van het kind zoals omschreven onder 1.

3. Beoordeel of dit effect wenselijk is

Bepaal de kans en waarschijnlijkheid, impact en ernst van mogelijke gevolgen voor de rechten van het kind.

4. Bepaal of aanvullende maatregelen noodzakelijk zijn om effecten te beperken

Indien de uitkomst van de afweging van vraag 3 tot onwenselijke uitkomsten leidt, moeten maatregelen worden bepaald om de gevolgen en impact voor de kinderrechten en vrijheden van de leerlingen te beperken. Geef hierbij de prioriteit aan van te nemen stappen en acties.

Deze kinderrechtenafweging inclusief (extra) te nemen maatregelen, kan desgewenst onderdeel uitmaken van hoofdstuk D: Maatregelen.

17 https://wetten.overheid.nl/BWBV0002508/2002-11-18#Verdrag_2

16 a. Noodzakelijkheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden.

16 b. Proportionaliteit en subsidiariteit

Ga hierbij in ieder geval in op proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden? Beoordeel verder of de voorgenomen gegevensverwerkingen evenredig is, in verhouding staat tot het te behalen doel. Ga hierbij in ieder geval in op subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt? Benoem hierbij de overwogen alternatieven.

17. 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.

[behandel hier evt. technisch onderzoek/DSAR etc]

Denk aan:

- Het recht op informatie,
- Het recht van inzage,
- Het recht op rectificatie,
- Het recht op gegevenswissing,
- Het recht op beperking van de verwerking,
- Een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens,
- Het recht op overdraagbaarheid van gegevens,
- Het recht van bezwaar en
- Het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit.

Recht van betrokkene	Toelichting procedure	Evt. beperking verwerking*
Het recht op informatie	Bijvoorbeeld: • Openbaar gepubliceerde privacyverklaring; • Intern gepubliceerde privacyverklaring; • Versturen van een fysieke brief naar huisadres betrokkenen; • Versturen van een digitale brief naar e-mailadres betrokkenen; • Betrokkenen worden gebeld	n.v.t.
Het recht van inzage		n.v.t.
Het recht op rectificatie		n.v.t.
Het recht op gegevenswissing		n.v.t.
Het recht op beperking van de verwerking		n.v.t.
Een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens		n.v.t.
Het recht op overdraagbaarheid van gegevens		n.v.t.
Het recht van bezwaar		n.v.t.
Het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit		n.v.t.

* *Er zijn uitzonderingen mogelijk op de uitoefening van deze rechten, op voorwaarde dat de wezenlijke inhoud van de grondrechten en fundamentele vrijheden niet wordt aangetast en dat het gaat om noodzakelijke en evenredige maatregelen ter waarborging van enkele expliciet opgesomde belangrijke doelstellingen van algemeen belang. Uitzonderingen moeten altijd op een nationale wet berusten, of in de AVG direct zijn toegestaan op grond van de bepalingen in de Europese privacyregelgeving. Uitzonderingen op de rechten van betrokkenen zijn, onder meer, geregeld in artikel 23 AVG en artikel 41 UAVG.*

18. Beoordeling verwerkersovereenkomst

Voor leveranciers die deelnemer of medestander zijn van het Convenant digitale onderwijsmiddelen en privacy 4.0 (ook wel: Privacyconvenant Onderwijs, hierna: Convenant) en daarbij gebruik maken van het daarbij horende model verwerkersovereenkomst vindt een toetsing plaats welke wordt afgezet tegen de vereisten van het convenant. Dit wordt de theoretische toets genoemd. Aanvullend hierop zal ook, aan de hand van de inzichten die deze DPIA heeft gebracht, een praktische toets plaatsvinden. Hierbij zal een vergelijk worden gemaakt tussen de in de theorie genoemde afspraken en de verwerkingen die in de praktijk plaatsvinden. De hiervoor gebruikte toetsingskaders zijn in de bijlage (verwerkersovereenkomst Toetsformulier met link) terug te vinden.

Voor leveranciers die geen deelnemer of medestander zijn van het convenant zal de verwerkersovereenkomst worden getoetst aan de vereisten van de AVG.

Na de bespreking van het verwerkersovereenkomst Toetsformulier en eventuele afspraken wordt uiteindelijk een verwerkersovereenkomst Toetsrapport met de bevindingen opgeleverd die via de Dienst Verwerkersovereenkomsten (van Kennisnet) of afgeschermd op de website van SIVON gedeeld wordt met alle schoolbesturen.

Tabel 18.1 **Bevindingen toets verwerkersovereenkomst**

TOETSRAPPORT (o.b.v. Model VWO)	Toelichting	
Toets - Verwerkersovereenkomst • Betreft <criterium>		
Toets - Bijlage 1: Privacybijsluiter • Betreft <criterium>		
Toets - Bijlage 2: Beveiligingsbijlage • Betreft <criterium>		
Toets - Bijlage 3: Wijzigingenbijlage • Betreft <criterium>		

De risico's die in deze tabel zijn opgesomd zijn uitgewerkt in de risicotabel van hoofdstuk 19

7. Deel C: Beschrijving en beoordeling risico's voor de betrokkenen

In dit hoofdstuk vindt de Risicoanalyse plaats: de gegevensverwerkingsanalyse (Deel A), aangevuld met een beoordeling van de rechtmatig (Deel B) worden afgewogen tegen de rechten en vrijheden van betrokkenen. De risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen worden beschreven en beoordeeld. Hierbij wegen de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen mee.

Beoordelingskader risico's

Alle mogelijke risico's van de gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen worden beschreven en afgewogen. Het gaat hierbij om de negatieve gevolgen die de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, de oorsprong van deze gevolgen, de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden en de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden: kans (waarschijnlijkheid) X impact (ernst) = risico.

De methodiek die wordt gevolgd, is beschreven door de Britse toezichthouder[18] om risico's te classificeren. Hierbij een objectieve inschatting gemaakt van de kans en impact van negatieve gevolgen (eventuele fysieke, emotionele of materiële schade).

Onderstaande matrix toont op een gestructureerde manier de classificatie van risico's:

RISICO	Kans Laag (1)	Kans Midden (2)	Kans Hoog (3)
Impact Hoog (3)	Risico Midden (Score: 3)	Risico Hoog (Score: 6)	Risico zeer hoog (Score: 9)
Impact Midden (2)	Risico Laag (Score: 2)	Risico Midden (Score: 4)	Risico Hoog (Score: 6)
Impact Laag (1)	Risico Zeer laag (Score: 1)	Risico Laag (Score: 2)	Risico Midden (Score: 3)

NB: een score van 1 levert dus een zeer laag risico op, terwijl een score van 9 een zeer hoog risico oplevert.

18 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how10

Het gaat hier om een risicogerichte benadering en beoordelingsproces dat bestaat uit de volgende drie stappen:

1) risico's identificeren;
2) risico's inschatten/analyseren;
3) risico's beoordelen/evalueren.

In het volgende hoofdstuk (deel D: maatregelen) worden de geconstateerde risico's aangevuld met 2 vervolgstappen beperkt (gemitigeerd):

4) Mitigeren risico's: maatregelen die de aangetroffen risico's voorkomen of verminderen (mitigeren);
5) Herbeoordeling risico's: restrisico.

19. Risico's

De in deze centrale DPIA geconstateerde risico's betreffen:

In onderstaande risicotabel worden de risico's beschreven. Per risico worden de mogelijke oorzaken en gevolgen aangegeven met daarbij de kans dat het zich voordoet en de impact. Tevens is aangegeven of het risico betrekking heeft op een proces waarbij <naam applicatie> wordt ingezet of dat het risico het systeem zelf betreft (de applicatie).

Toelichting MAPGOOD-methode

De MAPGOOD methode helpt om inzicht te krijgen in de verschillende risico's van de verwerking. Via deze methode wordt aan de hand van verschillende invalshoeken naar de risico's gekeken. Het MAPGOOD-model biedt houvast om de risico's te inventariseren. Zo zijn er verschillende invalshoeken die je kunt gebruiken om naar bedreigingen en risico's te kijken om zo beveiligingsmaatregelen in kaart te brengen:

Mens – de mensen die nodig zijn om het informatiesysteem te beheren en gebruiken, denk aan: directe en indirecte gebruikers, en functioneel en technisch applicatiebeheer.

Apparatuur – de apparatuur die nodig is om het informatiesysteem te laten functioneren, denk aan: webserver, applicatieserver, beheer van werkplekken en werkplekken van gebruikers.

Programmatuur – de programmatuur waaruit het informatiesysteem bestaat, denk aan: de diverse applicaties die gebruikt worden.

Gegevens – de gegevens die door het systeem worden verwerkt, denk aan: basisregistraties, financiële verantwoording en vergunningen.

Organisatie – de organisatie die nodig is om het informatiesysteem te laten functioneren, denk aan: beheer-, gebruikers- en ontwikkelorganisatie.

Omgeving – de omgeving waarbinnen het informatiesysteem functioneert, denk aan: locatie, serverruimte en werkplekken.

Diensten – de externe diensten die nodig zijn om het systeem te laten functioneren, denk aan: technisch systeembeheer, netwerkinfrastructuur en onderhoudscontracten met externe dienstverleners.

Tabel 19.1 Risico's:

Risiconr.	Mapgood	Risico-omschrijving	Oorzaak/bevinding	Kans	Impact	Risico	technisch of organisatorisch?
1		Gegevens worden te lang bewaard	Verzamelde gegevens worden niet (automatisch) na einde bewaartermijn verwijderd	3	3	**9**	
2		Ongeautoriseerde gebruiker krijgt toegang tot het systeem waarin persoonsgegevens zijn opgeslagen	MFA niet mogelijk	2	3	**6**	
3		Geen doelbinding gebruik gegevens	Financiële persoonsgegevens worden voor ander doeleinde gebruikt dan bepaald (function/mission creep)	2	2	**4**	
4				1	3	**3**	
5				1	2	**2**	
6				1	1	**1**	
7							

Gebruik evt. het hulpmiddel beoordelen risico's, of gebruik deze tabel met aanvullingen in hoofdstuk D maatregelen

8. Deel D: Beschrijving voorgenomen maatregelen

Dit hoofdstuk bevat de maatregelen die zijn of worden genomen om de geconstateerde risico's van de voorgenomen gegevensverwerkingen voor de vrijheden en rechten van de betrokkenen (Deel C) te beperken. Beoordelingskader maatregelen

De AVG geeft in artikel 5 lid 1 als beginsel dat persoonsgegevens door het nemen van passende technische en organisatorische maatregelen op dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat de persoonsgegevens onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. De verschillende maatregelen betreffen:

a) Maatregelen die al zijn/worden genomen door de betrokken partijen die direct betrekking hebben op de risico's van de gegevensverwerkingen. Bijvoorbeeld, beveiligingsbeleid dat direct van toepassing is op de gegevensverwerkingen.

b) Maatregelen die nog zullen worden genomen om de risico's van de gegevensverwerkingen zoveel mogelijk te mitigeren. Het betreft hier reeds voorgenomen maatregelen, of maatregelen die naar aanleiding van deze DPIA nog zullen worden genomen.

Hierbij wordt aangesloten bij de methodiek van de Franse toezichthouder (CNIL): verwerkingsverantwoordelijke en verwerker stellen bij onacceptabele risico's (los van de vraag of deze laag, middel of hoog zijn) gezamenlijk een actieplan op. Dit wordt een verbeterplan genoemd. Het verbeterplan vermeldt – met een planning - de voorgenomen maatregelen om de risico's aan te mitigeren besproken worden. Dit betreffen waarborgen, maatregelen en beveiligingsmechanismen om de bescherming van persoonsgegevens te waarborgen en de naleving van de AVG aan te tonen. Hierbij worden alleen maatregelen in aanmerking genomen waarvan het zeker is dat deze maatregelen genomen zullen (gaan) worden en dus de beschreven risico's daadwerkelijk zullen voorkomen of beperken. De maatregelen moeten met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn.

Risico's kunnen worden beperkt door maatregelen te nemen. Deze maatregelen zullen de kans en/of impact verkleinen. Daarmee blijft er een risico over: het restrisico. Rekenkundig uitgelegd betekent dit: [kans (waarschijnlijkheid) X impact (ernst)] -/- [risico-mitigerende maatregelen] = restrisico.

Het schoolbestuur moet beschrijven hoe tot het restrisico is gekomen en waarom deze aanvaardbaar wordt geacht.

Gedacht kan worden aan de volgende maatregelen, mede bedoeld om ervoor te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor ze worden verwerkt, juist en nauwkeurig zijn:

- Fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;
- Opslag van gegevens in een kluis;
- Project-, risico- en incidentenmanagement;
- Data opsplitsen;
- Dataminimalisatie;
- Back-ups;
- Integriteitscontroles;
- 2FA/MFA;
- Monitoring en logging;
- Controle van toegekende bevoegdheden;
- Privacybewustzijn- en beveiligingstrainingen;
- Managementrapportages over risicobeheer;
- Beperken inzageniveau;
- Periodiek een audit of hack- of penetratietest uitvoeren;
- Richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;
- Resonsible-disclosurebeleid;
- Geheimhoudingsverklaringen;
- Service level agreements (met boeteclausules);
- Verwerkersovereenkomsten.
- Screening personeel en VOG-verklaring.

20. Maatregelen

Beschrijf hierna welke technische en organisatorische maatregelen in redelijkheid (kunnen) worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf daarbij 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.

[LET OP: vergeet par. 8 DTIA maatregelen niet!]

Toelichting maatregelentabel:

Eigenaar maatregel: wees hierin specifiek zoals leverancier en/of schoolbestuur, wie moet maatregelen nemen of een product veranderen. Meerdere maatregelen zijn mogelijk, dus ook meerdere eigenaren. Geef toelichting welke impact de toepassing(en) heeft/hebben op het restrisico.

Indien een toelichting nodig is doe dat dan aan de hand van de nummering onder aan de maatregelentabel.

Wees zo volledig mogelijk in de maatregelentabel. Daar waar dit niet werkbaar is kan er aan de hand van de nummers een afzonderlijke toelichting gegeven worden over aspecten die samenhangen met de eigenaar maatregel, datum van implementatie en de toelichting over de aanvaardbaarheid van het restrisico.

Maatregelentabel:

Risiconr.	Omschrijving risico (steek-woord)	Risico	Maatregel(en) (Org/Techn/Jur)	Maatregel voor (naam applicatie/ school)	Restrisico (cijfer)	Toelichting aanvaardbaarheid restrisico	(datum)maatregel geïmplementeerd?
1		9					
2		6					
3		4					
4		3					
5		2					
6		1					

9. Deel E: MODEL lokale DPIA

Dit hoofdstuk bevat de afweging die iedere individueel schoolbestuur zelf moet maken. Het gaat om de rechtmatigheid van de voorgenomen verwerkingen, geconstateerde risico's en genomen en nog te nemen maatregelen om de gevolgen van die risico's te beperken. Daarnaast benoemt het schoolbestuur – indien van toepassing – extra risico's en aanvullende maatregelen die van toepassing zijn binnen het eigen schoolbestuur.

De tekst van deze bijlage kan gebruikt worden als model/rapportage voor de lokale DPIA.

A. Uitvoering lokale DPIA

Binnen [NAAM SCHOOLBESTUUR] is op basis van de door SIVON uitgevoerde centrale DPIA op [SYSTEEM] een lokale DPIA uitgevoerd in de periode [PERIODE].

Bij de beoordeling in deze lokale DPIA zijn betrokken:

- Bijvoorbeeld [ict-afdeling]
- [lid IBP-team]
- [privacy officer]
- [key-user/gebruiker]
- [vertegenwoordiging betrokkenen]

B. Overwegingen over centrale DPIA

[Bij de uitvoering van de lokale DPIA, worden de volgende onderdelen in de centrale DPIA overwogen:

- beschrijving kenmerken gegevensverwerking;
- beoordeling rechtmatigheid gegevensverwerkingen;
- beschrijving en beoordeling risico's voor de betrokkenen;
- beschrijving voorgenomen maatregelen]

Het team dat betrokken is bij de lokale DPIA heeft de in de centrale DPIA benoemde gegevensverwerking, rechtmatigheid, risicobeoordeling en voorgenomen maatregelen beoordeeld en overgenomen. Hierbij gelden de volgende uitzonderingen en/of toevoegingen: [...].

C. Organisatiespecifieke- en algemene applicatierisico's

Om tot een goede en volledige overweging te komen om onderdeel D te vullen dient er inzicht te komen in de aanwezigheid van basale privacyvereisten binnen het schoolbestuur. Onderstaande tabellen bieden een kader om inzicht te krijgen op de aan- of afwezigheid van belangrijke basismaatregelen. Betrek de bevindingen bij de risicobeoordeling en voer maatregelen door waar nodig.

Risicotabel 1. Organisatie-specifieke risico's

Veilige gegevensverwerking omvat meer dan alleen de verwerkingsomgeving van de applicatie/ het systeem. Het vergt ook dat de basis op orde is voor o.a. het besturingssysteem waarop het draait, de kennis en kunde van de gebruiker en het hebben en toepassen van relevant beleid.

Nr.	Beheersmaatregel	Uitgevoerd?	Opmerking/toelichting
1	Het bestuur heeft een eigen privacycoördinator of privacy officer.		
2	Binnen de organisatie zijn de volgende formele structuren geïmplementeerd: een autorisatiebeleid, toegangsbeheer, toewijzing van verantwoordelijkheden en eigenaarschap betreffende gegevensverwerking.		
3	Het gedetailleerde autorisatiebeleid specificeert welke toegangsniveaus en rechten per medewerker of rol vereist zijn om hun taken uit te voeren. Het autorisatiebeleid wordt regelmatig geëvalueerd en bijgewerkt om te blijven voldoen aan de veranderende behoeften en veiligheidsvereisten van de school.		
4	Het bestuur heeft een (externe) Functionaris Gegevensbescherming.		
5	Het bestuur heeft een datalekprotocol/beleid en past dit actief toe.		
6	Het bestuur heeft een IBP beleid en deze vastgesteld.		
7	Er is een PDCA m.b.t. de AVG waarbij er periodiek wordt gekeken of men compliant is en wat er verbeterd kan worden.		
8	Het bestuur heeft een gedragscode waarin diverse maatregelen voor gedrag en ICT beveiliging is opgenomen.		
9	Het bestuur heeft op elke schoolwebsite een pagina, dan wel een link naar de juiste pagina, over de AVG waarop informatie wordt verstrekt met betrekking tot de verwerking van persoonsgegevens, waaronder het gebruik van digitale leermiddelen (Privacyverklaring).		
10	Er is een actueel proces voor de rechten van betrokkenen.		
11	Ouders en medewerkers kunnen altijd en met succes de rechten van betrokkenen inroepen.		
12	Het bestuur heeft op elke schoolwebsite een pagina, dan wel een link naar de juiste pagina, over de wijze waarop de ouders (of leerlingen > 16 jaar) hun rechten kunnen uitoefenen (Privacyreglement).		

Risicotabel 2. Algemene applicatiespecifieke risico's

Deze risicotabel presenteert een overzicht van beheersmaatregelen die bedoeld zijn om de algemene risico's, die inherent zijn aan de verwerking, te adresseren. Deze maatregelen zijn tevens van toepassing op vergelijkbare verwerkingen bij andere leveranciers. Ze omvatten diverse aspecten, zoals het afsluiten van passende verwerkersovereenkomsten en het verstrekken van instructies aan medewerkers over het invullen van gegevens in open velden.

Nr.	Beheersmaatregel	Uitgevoerd?	Opmerking/toelichting
1	De verwerkersovereenkomst met verwerker is getekend.		
2	De verwerking is opgenomen in het register van verwerkingen.		
3	Het bestuur zal de DPIA minimaal eens per drie jaar herbeoordelen.		
4	Er zijn duidelijke afspraken over de invoer bij open velden. Dit kan bijvoorbeeld aan de hand van vastgesteld beleid of protocollen zijn geïmplementeerd. Hierin is vastgesteld of het gebruik van vrije invulvelden noodzakelijk is en zo ja voor welke informatie. Over deze uitgangspunten is duidelijk gecommuniceerd met alle medewerkers die gebruik maken van de applicatie.		
5	Het bestuur houdt rekening met dataminimalisatie voor verwerken van persoonsgegevens in de applicatie.		
6	Het bestuur hanteert de wettelijke bewaartermijnen. De bewaartermijnen zijn vastgesteld en beschreven.		
7	Het bestuur zorgt ervoor dat persoonsgegevens na afloop van de bewaartermijn daadwerkelijk worden geschoond en heeft een procedure hiervoor. De logbestanden (m.n. exports) worden periodiek gecontroleerd en de downloadmap wordt periodiek geleegd.		
8	Het bestuur voldoet aan het transparantieverplichting (artikel 13 en 14 AVG) en geeft de juiste informatie in de privacyverklaring over de toepassing van NAAM APPLICATIE		
9	Het bestuur heeft autorisaties ingericht op basis van 'need to know' (role based access).		
10	Afstemming met betrokkenen. Het bestuur heeft bij het uitvoeren van de lokale DPIA de betrokkenen om hun mening gevraagd over de verwerking en deze meegenomen in de DPIA (artikel 35 lid 9 AVG). Dit kan bijvoorbeeld via de medezeggenschapsraad.		
11	Gebruikers van de applicatie zijn/worden afdoende geschoold in het gebruik ervan.		
12	Persoonsgegevens worden niet op verkeerde plekken opgeslagen omdat regels en/of bekendheid met Studiemeter dit voorkomt. Er is daarom geen sprake van een schaduwadministratie op verschillende schijven en mappen van medewerkers.		
13	Er is een functioneel beheerder aangewezen voor NAAM APPLICATIE		

Risicotabel 3. Uit de centrale DPIA op schoolniveau te mitigeren risico's.

Risico	Te nemen maatregel	Uitgevoerd?	Opmerking/toelichting

D. Overwegingen implementatie en lokale DPIA: aanvullende risico's en maatregelen

In aanvulling op de in de centrale DPIA gevonden risico's en maatregelen, heeft de implementatie en gebruik van [SYSTEEM] binnen [NAAM SCHOOLBESTUUR] verdere gevolgen voor de rechten en vrijheden van de betrokkenen.

[Overweeg hierna de mogelijke impact op de rechten en vrijheden van betrokkenen en eventuele schade of zelfs (fysiek of emotioneel) letsel die het gebruik van [SYSTEEM] kan veroorzaken. Weeg hierbij mogelijk risico's mee op het gebied van:

- onvermogen om rechten uit te oefenen (inclusief maar niet beperkt tot privacyrechten);
- onvermogen om toegang te krijgen tot diensten of kansen;
- verlies van controle over het gebruik van persoonsgegevens;
- discriminatie;
- identiteitsdiefstal of fraude;
- financieel verlies;
- reputatieschade;
- verlies van vertrouwelijkheid;
- heridentificatie van gepseudonimiseerde gegevens; of
- elk ander significant economisch of sociaal nadeel
- gevolgen en risico's voor de beveiliging van [SYSTEEM].]

[NAAM SCHOOLBESTUUR] identificeert een aantal aanvullende risico's. Deze worden beoordeeld aan de hand van de kans (waarschijnlijkheid) als de impact (ernst). Het risico wordt beoordeeld aan de hand van de volgende indeling en berekening:

kans (waarschijnlijkheid) X impact (ernst) = risico

Om een objectieve inschatting maken van de risico's wordt gebruik gemaakt van de volgende gestructureerde matrix van risicoclassificatie:

RISICO	Kans Laag (1)	Kans Midden (2)	Kans Hoog (3)
Impact Hoog (3)	Risico Midden (Score: 3)	Risico Hoog (Score: 6)	Risico zeer hoog (Score: 9)
Impact Midden (2)	Risico Laag (Score: 2)	Risico Midden (Score: 4)	Risico Hoog (Score: 6)
Impact Laag (1)	Risico Zeer laag (Score: 1)	Risico Laag (Score: 2)	Risico Midden (Score: 3)

NB een score van 1 levert dus een zeer laag risico op, terwijl een score van 9 een zeer hoog risico oplevert.

Risico's kunnen worden beperkt door maatregelen te nemen. Deze maatregelen zullen de kans en/of impact verkleinen. Daarmee blijft er een risico over: het restrisico. Rekenkundig uitgelegd betekent dit:

[kans (waarschijnlijkheid) X impact (ernst)] -/- [de risico-mitigerende maatregelen] = restrisico

De in de lokale DPIA geconstateerde risico's betreffen:

[RISICO] **[toelichting risico]**			
Risico-afweging	**kans**	**impact**	**Risico**
Maatregel/maatregelen	[beschrijving maatregel]		
Eigenaar maatregel	[wie is verantwoordelijk voor uitvoeren maatregel: benoem de eigenaar]		
Maatregelen geïmplementeerd?	[is de maatregel al gepland, zo niet wanneer wordt deze gepland]		
IRisico-afweging	**kans**	**impact**	**RESTRISICO**
RESTRISICO	NB: het restrisico betreft het risico indien de maatregel wel wordt uitgevoerd. Zonder maatregel resteert het oorspronkelijke risico.		

[dupliceer de tabel zo vaak als nodig om aanvullende risico's te beschrijven]

E. Verklaring en advies functionaris voor gegevensbescherming (fg)

De fg heeft kennis genomen van de in de door SIVON uitgevoerde centrale DPIA, geconstateerde risico's en aanbevolen maatregelen.

De fg is [wel/niet] betrokken geweest bij uitvoering en opstellen van de lokale DPIA voor [NAAM SCHOOLBESTUUR]. [beschrijving rol fg schoolbestuur bij deze DPIA]

Het advies van de fg is [...].

F. Visie betrokkenen

In het kader van dit DPIA zijn de betrokkenen, te weten [leerlingen, hun ouders en medewerkers] [betrokken/geïnformeerd] over de uitkomst.

[Zijn de betrokkenen, op wie de verwerking betrekking heeft, geraadpleegd over dit DPIA en wat is hun mening over de verwerking? Zo nee, waarom niet?]

De concept DPIA wordt aan (G)MR voorgelegd, waarbij de (G)MR als vertegenwoordiging van betrokken kan aangeven of de gegevensverwerking aansluit bij hun verwachting en of hierover zorgen bestaan.

G. Conclusie

Op basis van het onderzoek dat in het kader van de centrale DPIA, alsmede de lokale DPIA is uitgevoerd, zijn de gevolgen voor de rechten en vrijheden van deze betrokkenen door de verwerking van persoonsgegevens van onderwijsdeelnemers en medewerkers in [SYSTEEM] - na toepassing van risico-mitigerende maatregelen – in [onvoldoende/voldoende/goede] mate beheerst.

Deze conclusie wordt anders als de in deze DPIA genoemde maatregelen door het schoolbestuur niet of onvoldoende worden uitgevoerd.

De genomen en te nemen maatregelen, waarborgen, veiligheidsmaatregelen en mechanismen die binnen [SYSTEEM] de bescherming van persoonsgegevens garanderen, zijn [onvoldoende/voldoende/goed] gericht op het beperken van de risico's voor de rechten en vrijheden van betrokkenen.

Er is [wel/niet] gebleken van hoge risico's voor de rechten en vrijheden van betrokkenen die moet leiden tot een 'voorafgaande raadpleging' zoals omschreven in artikel 36 AVG.

H. Risico-mitigerende maatregelen schoolbestuur

Bij deze beoordeling zijn een aantal risico's geïdentificeerd waarbij de leverancier een aantal maatregelen neemt. Hiernaast moet het schoolbestuur maatregelen nemen of treffen om de benoemde risico's te beperken. Het betreffen de hierna te noemen maatregelen waarbij de verantwoordelijkheid voor de implementatie bij het schoolbestuur (de verwerkingsverantwoordelijke) ligt.

Het schoolbestuur moet daarom zorgen voor:

1. goede gebruiksinstructies voor beheerder en gebruikers (op school) van [SYSTEEM], om verkeerd gebruik, misbruik of beveiligingsincidenten te voorkomen. Hierbij wordt gebruikt gemaakt van de [HANDLEIDING LEVERANCIER] en de [WERKINSTRUCTIES SCHOOL].
2. het inregelen van de correcte autorisaties in [SYSTEEM]. Zorg hierbij voor functiescheiding waarbij in geval van autorisatieverlening gewerkt wordt met het vier-ogenprincipe.
3. het informeren de leerlingen, hun ouders en medewerkers over deze DPIA en de (mogelijke) gevolgen voor de rechten en vrijheden die deze betrokkenen.
4. [BESCHRIJF HIER DE MAATREGELEN ZOALS OPGENOMEN BIJ HET ONDERDEEL "Overwegingen implementatie en lokale DPIA"]

De onder de nummers [NUMMER] genoemde punten moeten op een termijn van [TERMIJN] worden uitgevoerd.

I. Aanbevelingen

Naast de hiervoor genoemde bevindingen en maatregelen, zijn er een aantal aanbevelingen die buiten scope van deze DPIA vallen omdat zij nietbinnen de invloedssfeer van (de leverancier van] [SYSTEEM] liggen, terwijl deze aanbevelingen cq. maatregelen in beeld zijn gekomen bij deze DPIA en/of wel bijdragen aan het beperken van risico's:

A. ...

B. ...

J. Verklaring schoolbestuur

Het schoolbestuur, aangemerkt als vertegenwoordiging van verwerkingsverantwoordelijke [NAAM SCHOOLBESTUUR], overwegende de conclusies, risico-mitigerende maatregelen en het aanbevelingen, verklaart hierbij:

I. kennis te hebben genomen van inhoud en uitkomsten van deze centrale en lokale DPIA;

II. in te stemmen met de in de rapportage genoemde beheersmaatregelen;

III. opdracht te geven voor het uitvoeren van de beheersmaatregelen (zie hiervoor onder H.) binnen de daarbij genoemde termijnen;

IV. de - in dit rapport - vermelde resterende risico's te aanvaarden;

V. deze DPIA na een periode van [PERIODE/JAAR] te laten herzien, of eerder indien nodig;

VI. [wel/geen] voorafgaande raadpleging bij de Autoriteit Persoonsgegevens in te dienen;

VII. het DPIA-team decharge te verlenen.

EN BESLUIT [NA (HER)OVERWEGING] HET GEBRUIK VAN [SYSTEEM] [WEL/NIET] TE [GEBRUIKEN/CONTINUEREN].

Naam bestuurder(s):

Plaats:

Datum:

Ondertekening:

Bijlage 1:
Gebruikte termen en definities

Alle type gegevens worden beschouwd als persoonsgegevens als ze direct of indirect tot een persoon te herleiden zijn. Deze definitiebepalingen hebben tot doel om consistentie te bieden bij het begrijpen van verschillende (wettelijke) termen en concepten die worden gebruikt bij de naleving van de AVG.

Anonieme gegevens Anonieme en geanonimiseerde gegevens zijn geen persoonsgegevens. Relevante privacy wet- en regelgeving zijn niet van toepassing op deze gegevens. Met anoniem en geanonimiseerd wordt bedoeld dat de persoon op wie de persoonsgegevens betrekking hebben, niet (meer) identificeerbaar is. Let op: het anonimiseren van persoonsgegevens als handeling is een verwerking van persoonsgegevens en valt wel onder privacy wet- en regelgeving.

Betrokkenen personen waarop de gegevens betrekking hebben Betrokkenen zijn alle geïdentificeerde of identificeerbare natuurlijke personen binnen de gegevensverwerkingen, oftewel de personen over wie de persoonsgegevens worden verwerkt. Denk hierbij aan: leerlingen, medewerkers, cliënten, zakelijke contacten, gebruikers en bezoekers.

Bijzondere persoonsgegevens mogen alleen verwerkt worden als je een beroep kunt doen op een uitzondering. Voor het onderwijs geldt bijvoorbeeld dat gezondheidsgegevens alleen gebruikt mogen worden als dat noodzakelijk is voor het geven van onderwijs en het begeleiden van een leerling. Ze zijn bijzonder omdat het gebruik van deze gegevens iemands privacy ernstig kan beïnvloeden. Voorbeelden zijn gezondheidsgegevens, levensovertuiging, lidmaatschap van de vakbond, ras of etnische afkomst.

D**iagnostische gegevens** zijn gegevens over het individuele gebruik van de diensten. Bijvoorbeeld: hoe vaak je inlogt, welk soort documenten je opslaat, leest etc.. Deze gegevens komen in logbestanden terecht van de clouddienst. [Deze data wordt ook soms servicegegevens genoemd.] **Metadata** is een andere categorie gegevens die ook over gebruik gaan, zoals de locatie van gebruik, tijdstip, en device type.

Functionele gegevens zijn gegevens die een (cloud)dienst nodig heeft om de dienst te kunnen leveren.

Gevoelige persoonsgegevens gaan over gegevens die volgens de Autoriteit Persoonsgegevens (AP) snel inbreuk (kunnen) maken op de persoonlijke levenssfeer. Het gaat bijvoorbeeld om leerresultaten van kinderen, omdat daar conclusies aan kunnen worden verbonden met gevolgen voor het latere maatschappelijke leven. Of het gaat om grote verzamelingen van informatie van (zeer) jonge kinderen, gegevens over (problematische) gezinssituatie of[19] zwaardere eisen gesteld aan de beveiliging van de gegevens.

Inhoudelijke gegevens is de inhoud van bijvoorbeeld een document dat je online opslaat.

19 https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013_snappet.pdf

Kwetsbare groepen De categorieën van betrokkenen kunnen invloed hebben op de effecten van het voorstel. Bepaalde betrokkenen zijn kwetsbaarder dan anderen. Met kwetsbaar wordt bedoeld dat de negatieve effecten van een (onrechtmatige) gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen dan voor andere betrokkenen. Denk hierbij aan minderjarigen en etnische minderheden. De AVG biedt specifieke bescherming aan kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader.

Nationale identificatienummers
Nummers ter identificatie van een persoon die bij wet zijn voorgeschreven, mogen slechts worden verwerkt voor doeleinden die bij wet zijn bepaald. Het gebruik van deze nummers dient dus met uiterste zorgvuldigheid plaats te vinden en de noodzakelijkheid om deze nummers te gebruiken dient goed onderbouwd te zijn. De gedachte hierachter is dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijkt en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormt. Het gaat hierbij enkel om in de wet voorgeschreven persoonsidentificerende nummers. Denk hierbij aan:

• Burgerservicenummer (BSN)
• BIG-nummer (beroepen in de individuele gezondheidszorg),
• A-nummer (basisregistratie personen),
• Onderwijsnummer of Persoonsgebonden nummer (PGN),
• Strafrechtketennummer

Persoonsgegevens Onder persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. De term ‘natuurlijke personen’ betekent hier levende mensen. Informatie over overleden personen, rechtspersonen, dieren, zaken en objecten zijn in principe geen persoonsgegeven. Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken.

Hieronder staan voorbeelden van categorieën persoonsgegevens en type persoonsgegevens die binnen die categorie vallen:
- Naam (voornaam, achternaam, voorvoegsel, initialen)
- Contactgegevens (huisadres, telefoonnummer, e-mailadres)
- Demografische gegevens (leeftijd, geboortedatum en -plaats, geslacht, nationaliteit, opleiding, IQ)
- Apparaat- en internetgegevens (IP-adres, MAC-adres, metadata, locatie-informatie en geografische informatie)
- Financiële gegevens (bankrekeningnummer en -saldo, inkomens- en vermogensgegevens, loonschaal, kredietwaardigheid, winst eenmanszaak)
- Werk gerelateerde gegevens (KvK-nummer, verslag van een functioneringsgesprek, documentatie over negatief gedrag op de werkvloer)
- Overige persoonsgegevens (voertuigidentificatienummer, persoonlijke voorkeuren)

Ook metadata zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Over het algemeen is een type metadata op zichzelf niet voldoende identificerend, maar meestal worden meerdere type metadata verzameld van gebruikers. Al deze gegevens gecombineerd met elkaar kan leiden tot identificeerbaarheid van een individu.

Pseudonieme persoonsgegevens Onder pseudonimisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eisen verbonden dat de sleutels apart worden bewaard en dat maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.
Of pseudonieme gegevens door de ontvanger (verwerker) als persoonsgegevens aangemerkt moeten worden hangt af van de omstandigheden van het geval. Het uitvoeren van een toets zal kunnen uitwijzen in hoeverre deze door de leverancier te herleiden zijn tot persoonsgegevens[20].

20 Het Gerecht EU 23 april 2023, T557/20, ECLI:EU:T:2023:219

Bijlage 2: Uitleg risico's

Negatieve gevolgen van de gegevensverwerking zijn bijvoorbeeld (het risico op):

- onvermogen om rechten uit te oefenen (inclusief maar niet beperkt tot privacyrechten);
- onvermogen om toegang te krijgen tot diensten of kansen;
- verlies van controle over het gebruik van persoonsgegevens;
- discriminatie;
- identiteitsdiefstal of fraude;
- financieel verlies;
- reputatieschade;
- lichamelijk letsel;
- verlies van vertrouwelijkheid;
- heridentificatie van gepseudonimiseerde gegevens; of
- elk ander significant economisch of sociaal nadeel
- Inbreuk op de rechten van kinderen (kinderrechten).

Om te beoordelen wat het risico is, wordt de kans dat het risico zich voordoet (waarschijnlijkheid) gewogen tegenover de ernst van de mogelijke schade. Schade hoeft niet onvermijdelijk te zijn om als risico of hoog risico te kwalificeren. Het moet meer dan ver weg zijn, maar elke significante kans op zeer ernstige schade kan nog steeds voldoende zijn om als een hoog risico te kwalificeren. Evenzo kan een grote kans op wijdverspreide maar meer kleine schade nog steeds als een hoog risico gelden.

Hulpmiddel beoordelen score laag, midden en hoog

Laag	Midden	Hoog
Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende meerdere dagen brengt geen merkbare (meetbare) schade toe. Blijvende juistheid van informatie (vanaf de bron tot het laatste gebruik) is gewenst, maar hoeft niet gegarandeerd te zijn.	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een of meerdere dagen brengt merkbare schade toe. Sommige afwijkingen in data zijn toelaatbaar, juistheid data is belangrijk maar niet kritisch.	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een werkdag brengt merkbare schade toe. Juistheid informatie moet gegarandeerd zijn, noodzakelijk dat data correct is.
Weinig tot geen schade	Enige schade, invloed of gevolgen	Grote – onvermijdelijke –ernstige schade, nadeel en gevolgen; imago.
Kans = gebeurt bijna nooit; 1 maal per school jaar of minder	Kans = gebeurtenis kan zich voordoen; meerdere malen per schooljaar	Kans = deze gebeurtenis zal zich bijna zeker voor-doen; per maand, week of zelfs dag
Kleine kans	Een redelijke kans	De kans dat het zich voordoet is groter, dan de kans dat het niet gebeurt

Bijlage 3: Uitwerking Data Transfer Impact Assessment

[beschrijving juridisch onderzoek + uitkomsten + juridische onderbouwing uit par. 8 DTIA / Bijlage wordt niet standaard gepubliceerd ivm gevoeligheid onderzoek]
Op 16 juli 2020 oordeelde het Europese Hof van Justitie[21] dat de doorgifte van persoonsgegevens op basis van het Privacy Shield niet langer geldig was, met onmiddellijke ingang. Deze uitspraak was de uitkomst van de rechtszaak die Max Schrems voerde tegen Facebook Ierland en de Ierse Data Protection Commissioner. Eerder, in 2015, in een andere zaak aangespannen door Max Schrems, verklaarde het Europese Hof de Safe Harbor-overeenkomst ongeldig, de voorloper van het Privacy Shield. Het Privacy Shield zelf is sindsdien ongeldig als rechtsgrondslag voor de doorgifte van persoonsgegevens. Als belangrijkste redenen voert het Hof aan dat de beperkingen van de persoonlijke levenssfeer die voortvloeien uit de Amerikaanse regelgeving onvoldoende gedefinieerd en onevenredig zijn en daarom een te grote inbreuk op de persoonlijke levenssfeer vormen. Het Hof beschrijft de risico's van massasurveillance (verzameling van gegevens in bulk) door de Amerikaanse inlichtingendiensten in het kader van de op Section 702 FISA en op E.O. 12333 gebaseerde surveillanceprogramma's PRISM en Upstream, en het ontbreken van effectieve en afdwingbare rechten voor EU-ingezetenen bij de verwerking van deze gegevens door de Amerikaanse overheidsdiensten als een inbreuk.]

[Standaardcontractbepalingen (SCC): persoonsgegevens kunnen vanuit de EER naar derde landen buiten de EER worden doorgegeven met gebruikmaking van door de Europese Commissie goedgekeurde modelcontractbepalingen (hierna: "standaardcontractbepalingen" genoemd). Deze bepalingen waarborgen contractueel een hoog beschermingsniveau.

Adequaatheidsbesluit: een adequaatheidsbesluit betekent dat het beschermingsniveau in het land in kwestie vergelijkbaar is met het niveau dat binnen de EER wordt toegepast. Momenteel zijn er adequaatheidsbesluiten ten aanzien van Andorra, Argentinië, Canada (commerciële organisaties), Faeröer, Guernsey, Israël, Isle of Man, Japan, Jersey, Nieuw-Zeeland, Republiek Korea, Zwitserland, het Verenigd Koninkrijk en Uruguay. Het adequaatheidsbesluit voor (sommige doorgiften onder het Privacy Shield naar) de VS is sinds de zomer van 2020 niet meer geldig.]

Een Data Transfer Impact Assessment (DTIA) is noodzakelijk om na te gaan of de SCC's een in wezen gelijkwaardige bescherming bieden voor de buiten de EER getransporteerde gegevens. De DTIA is separaat bijgevoegd in Excel. De analyse is gebaseerd op het door de Zwitserse rechtsgeleerde David Rosenthal opgestelde format, met enkele aanvullingen.

21 European Court of Justice, C-311/18, Data Protection Commissioner against Facebook Ireland Ltd and Maximillian Schrems (Schrems-II), 16 July 2020.

De EDPB heeft een toelichting gegeven dat er geen sprake is van doorgifte wanneer een cloud provider kan beloven dat alle gegevens uitsluitend in de EU worden verwerkt: *"Houd er rekening mee dat toegang op afstand vanuit een derde land (bijvoorbeeld in ondersteuningssituaties) en/of opslag in een cloud gelegen buiten de EER, aangeboden door een dienstverlener, ook wordt beschouwd als een doorgifte. Meer in het bijzonder moet u, indien u gebruik maakt van een internationale cloudinfrastructuur, beoordelen of uw gegevens zullen worden doorgegeven naar derde landen en waar, tenzij de cloudprovider in de EER is gevestigd en het in zijn contract duidelijk vermeldt dat de gegevens in het geheel niet in derde landen zullen worden verwerkt."*[22]. De EDPB suggereert in voetnoot 23 dat elke toegang vanuit een derde land als een doorgifte geldt: "Please note that remote access by an entity from a third country to data located in the EEA is also considered a transfer". Deze DPIA gaat ervan uit dat de term doorgifte ook (de mogelijkheid) inhoudt van bevelen van Amerikaanse overheidsinstanties om persoonsgegevens van EU-klanten openbaar te maken, vandaar de noodzaak van een Data Transfer Impact Assessment. Zelfs voor de streaming [DATA] in [SYSTEEM] en de opgeslagen gegevens in [SYSTEEM], ook al worden deze al in de EU verwerkt en opgeslagen.

De EDPB beschrijft[23] verschillende elementen van het risicoassessment in haar richtsnoeren voor technische maatregelen die verwerkers en voor verwerking verantwoordelijken kunnen nemen om de daaruit voortvloeiende hoge risico's voor de gegevensbescherming te beperken.

[Het assessment bevat ten minste:

- de relevante wetgeving
- de doeleinden waarvoor de gegevens worden verwerkt
- de categorieën van doorgegeven gegevens en de gevoeligheid ervan
- of de gegevens in het derde land worden opgeslagen of dat er toegang op afstand is tot gegevens die binnen de EU/EER zijn opgeslagen
- de rol van de partijen (publiek/privaat, verwerker/controleur)
- alle actoren, inclusief subverwerkers
- het formaat van de gegevens
- mogelijkheid van verdere doorgifte.]

22 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, Par. 13, p. 11.

23 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, URL: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf