CENTRALE DATA PROTECTION IMPACT ASSESSMENT AFAS CRM, HRM & PAYROLL

Versie 0.7, 16 oktober 2023

Colofon

DPIA uitgevoerd door	Coöperatie Samen Innoveren/Inkopen/Ict voor Onderwijs Nederland U.A. (SIVON) www.sivon.nl info@sivon.nl
Betrokkenen DPIA	Dimmen Smolders (juridisch adviseur ICTRecht) Gülçin Ermis (juridisch adviseur ICTRecht) Job Vos (jurist en adviseur IBP) Hans-Peter Ligthart (portfoliomanager IBP) Ferdy IJsselmuiden (DPIA-projectmanager)
Met dank aan de volgende scholen	Esprit scholen, Biezonderwijs en SCO Leiden
Auteursmodel DPIA (v.1.0)	Hans-Peter Ligthart (portfoliomanager IBP) Job Vos (jurist en adviseur IBP)

Versiebeheer

Datum	Versie	Wijziging
24 maart 2022	0.0	Concept (HL)
9 mei 2022	1.0	Basisversie model (JV)
20 januari 2023	0.1	Eerste versie (ICTRecht)
14 februari 2023	0.2	1e feedback SIVON
9 april 2023	0.3	Herziene versie op basis van 1e feedback SIVON
2 mei 2023	0.4	Nadere aanpassingen ICTRecht
31 mei 2023	0.5	Verwerking input AFAS en nieuwe inzichten.
30 september 2023	0.6	Nadere verwerking en uitsplitsing van (lokale) risico's en maatregelen
16 oktober 2023	0.7	Aanscherping niet-inhoudelijke verschillende DPIA-onderdelen.

Inhoudsopgave

1. Samenvatting

Het gebruik van het softwarepakket van AFAS als personeelsadministratiesysteem vormt voor veel organisaties een belangrijke hoeksteen voor de bedrijfsvoering. Dit geldt ook voor schoolbesturen hetgeen benadrukt dat, zowel ten behoeve van de bedrijfscontinuïteit als de waarborging van de informatiebeveiliging en privacy, hoge eisen gesteld moeten worden aan een applicatie die zorgdraagt voor personeelszaken zoals HRM en Payroll.
Ook op lokaal niveau van het schoolbestuur moet de basis op orde zijn. Hiervoor is in onderdeel C van de lokale DPIA in dit document een overzicht opgenomen met organisatiespecifieke- en algemene applicatierisico's.
Voor wat betreft het gebruik van AFAS voor softwareonderdelen CRM, HRM en Payroll is tijdens deze DPIA gebleken dat er op het gebied van de informatiebeveiliging een solide basis ligt. Er wordt voldaan aan de in redelijkheid te stellen technische en organisatorische maatregelen voor een veilige verwerking. Er zijn echter aantal privacyrisico's aan de oppervlakte gekomen die door het nemen van de juiste maatregelen kunnen worden gemitigeerd. Met AFAS is overeengekomen dat de door hun te treffen maatregelen op uiterlijk 1 april 2024 zullen zijn doorgevoerd waardoor er geen hoge risico's meer zullen zijn. Hier zal vervolgens een evaluatie op volgen waarvan de resultaten kort na de deadline zullen worden gepubliceerd op de website van SIVON.

Samenvatting van de risico's en maatregelen:

1. **Risico**: Onduidelijkheid en ontbrekende onderdelen in verwerkingsbepalingen (artikel 28 AVG) binnen de Algemene Voorwaarden en Service Overeenkomst van februari 2022 (hierna: AV) van AFAS. Dit heeft tot gevolg dat er niet wordt voldaan aan AVG nalevingsvereisten en er op verschillende vlakken onduidelijkheid is over de verwerkingsvoorwaarden. AFAS is (nog) niet bereid om de Algemene Verwerkersovereenkomst 4.0, gebaseerd op de Model verwerkersovereenkomst 4.0 behorend bij het Privacyconvenant Onderwijs, als standaard te gebruiken.
   Maatregel: AFAS> Aanpassing van de AV door de ontbrekende en ontoereikende bepalingen en bijlagen alsnog toe te voegen. Het door AFAS in gebruik nemen van de Algemene Verwerkersovereenkomst 4.0 waaronder het compleet vullen van de verplichte bijlagen is ook een mogelijkheid om de risico's voor een groot deel weg te nemen.
2. **Risico**: Mailsysteem AFAS versleutelt het berichtenverkeer niet. Het versturen van gevoelige gegevens zoals loonstroken en re-integratierapporten brengt daarom een hoog risico met zich mee. De vertrouwelijke aard van deze gevoelige en bijzondere persoonsgegevens benadrukt het belang van een verhoogd beveiligingsniveau bij het mailen ervan. Notificaties van algemene aard kunnen wel via het intern mailsysteem verzonden blijven worden.
   Maatregel: Schoolbestuur> Omdat end-to-end encryptie niet door AFAS wordt ingevoerd zal de maatregel op het organisatorisch vlak vanuit het schoolbestuur toegepast moeten worden. Dit zal in de vorm zijn van het niet (langer) versturen van gevoelige mails via het interne mailsysteem. Het afdwingen hiervan vindt plaats door middel van duidelijke communicatie naar de gebruikers en strikte richtlijnen en procedures die het verzenden van gevoelige gegevens via de AFAS mail moeten voorkomen.
3. **Risico:** Onduidelijkheid over gebruik van gegevens door AFAS ten behoeve van productverbetering. In de AV van AFAS staat dat geanonimiseerde gegevens over het gebruik van producten en diensten wordt verwerkt. Tijdens de DPIA-sessies is kenbaar gemaakt dat enkel anonieme gegevens worden verwerkt. Er bestaat een privacyrisico wanneer het onduidelijk is welke gegevens door AFAS voor welke doeleinden worden

verwerkt.
Maatregel: AFAS> AFAS zal helderheid verschaffen over welke gegevens zij op welke manier ten behoeve van welk doel verzameld en verwerkt. Vervolgens zal deze verwerking opnieuw door SIVON beoordeeld worden.

4. **Risico**: Er ontbreekt een meldingsmechanisme dat aangeeft wanneer gegevensverwerkingen hun bewaartermijn hebben bereikt en gereed zijn om te worden verwijderd.
   Maatregel: AFAS en Schoolbestuur> AFAS kan een technische aanpassing implementeren die automatisch notificaties genereert wanneer de naderende bewaartermijnen worden bereikt. Tot die tijd moet het schoolbestuur een procedure opstellen die bewaartermijnen bewaakt en overschrijdingen ervan voorkomt.
5. **Risico**: AFAS geeft in de Algemene Voorwaarden aan een tweetal verwerkersovereenkomst branchemodellen te “ondersteunen” zonder deze daadwerkelijk overeen te komen met de gebruiker. Dit heeft tot gevolg dat hier misverstanden over kunnen ontstaan. Onterecht kan de veronderstelling leven dat AFAS branchemodellen ondertekent.
   Maatregel: AFAS> AFAS zal de betreffende bepaling verwijderen uit de Algemene Voorwaarden of anderzijds helderheid geven over de precieze betekenis van de *ondersteuning* van de branchemodellen en ondubbelzinnig naar voren laten komen of deze overeengekomen kunnen worden met de afnemende partijen.

Conclusie

Na uitvoering van het DPIA-onderzoek kan geconcludeerd worden dat, rekening houdend met de voornamelijk door AFAS te nemen risicobeperkende maatregelen, de verwerking van persoonsgegevens van betrokkenen (veelal medewerkers van schoolbesturen) geen onaanvaardbare risico's voor de rechten en vrijheden met zich meebrengt. De resterende risico's worden als aanvaardbaar beschouwd voor het schoolbestuur. Deze conclusie gaat uit van de aanwezigheid van een reeks beheersmaatregelen zoals vastgelegd in de lokale DPIA (hoofdstuk 7c), die een solide basis vormen voor gegevensverwerking door het schoolbestuur.

2. Introductie en achtergrond DPIA

In het onderwijs maken we 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 en andere ict-systemen. 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: Informatiebeveiling en privacy. Een onderdeel daarvan is het gebruik van veilige en verantwoorde ict-middelen. Een Data Protection Impact Assesments (DPIA) zou je ook kunnen omschrijven als een privacytoets en is een hulpmiddel om vast te stellen of de IBP van een ICT-applicatie op orde is!

I. DPIA

Schoolbesturen of colleges van bestuur (CvB) zijn als verwerkingsverantwoordelijken verplicht om te onderzoeken of persoonsgegevens voldoende beschermd zijn. Daarvoor voeren zij een privacytoets uit: een Data Protection Impact Assesments uit (DPIA). In de AVG wordt dit een gegevensbeschermingseffectbeoordeling (GEB) genoemd. Een DPIA wordt uitgevoerd op een applicatie of verwerking van een leverancier (verwerker). Bij een DPIA wordt het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens onderzocht. Vastgesteld wordt of het gebruik van persoonsgegevens (verwerking) een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen (leerlingen, hun ouders en medewerkers). 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 en mitigerende maatregelen. Mitigerende maatregelen zijn maatregelen die het risico beperken.

Bij applicaties die door veel verwerkingsverantwoordelijken – op dezelfde wijze – worden gebruikt, is het zinvol om deze DPIA samen uit te voeren. Hierdoor hoeft niet elk schoolbestuur zelf het spreekwoordelijke wiel uit te vinden. SIVON voert daarom namens haar leden zogenaamde **centrale DPIA's** uit. Door hierbij samen op te trekken met verschillende schoolbesturen die hun ervaring uit de onderwijspraktijk meebrengen, wordt expertise en ervaring samengebracht. Door samen op te trekken staan de onderwijsinstellingen via SIVON sterker in de gesprekken met de leverancier. En voor deze leveranciers is duidelijk dat afspraken over verbeteringen alleen via SIVON worden gemaakt in plaats van met vele individuele onderwijsinstellingen. Door deze centrale DPIA's uit te voeren op veel gebruikte systemen, helpt SIVON onderwijsinstellingen op weg om veilig en verantwoord gebruik te maken van persoonsgegevens en ict.

Na de uitvoering van de centrale DPIA moeten de schoolbesturen volgens de AVG zelf afwegen of de uitkomsten uit de centrale DPIA ook op hun organisatie van toepassing zijn. Daarvoor moeten zij nog wel een **lokale DPIA** uitvoeren en daarin een eigen afweging maken. SIVON helpt besturen hiermee doordat in de centrale DPIA de meest voorkomende risico's voor onderwijsinstellingen worden bepaald. De centrale DPIA wordt voor de lokale DPIA als uitgangspunt genomen, waarbij het schoolbestuur enkel nog een eigen afweging moet maken of de meest voorkomende risico's en

maatregelen ook voor hen gelden en of zij nog aanvullende risico's zien op basis van hun eigen omstandigheden.

II. Verplichting DPIA

Een DPIA 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 privacy van onderwijsdeelnemers en medewerkers. Ook is het mogelijk dat het uitvoeren van een DPIA verplicht is volgens de regels van de privacytoezichthouder Autoriteit Persoonsgegevens die een lijst gepubliceerd heeft bij welke verwerkingen het uitvoeren van aan DPIA verplicht is[1]. De onderwijsinstelling voert door middel van een DPIA vooraf een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.

Bij het onderzoeken van het personeeladministratiesysteem AFAS is het uitvoeren van een DPIA verplicht omdat er op grote schaal persoonsgegevens worden verwerkt van werknemers. Deze persoonsgegevens zijn niet zelden gevoelig en persoonlijk van aard maar regelmatig ook aan te merken als bijzonder (artikel 9 AVG).

III. Toetsing rolverdeling verwerkingsverantwoordelijke en verwerker

Bij de DPIA wordt uitgegaan van een rolverdeling tussen school en leverancier gebaseerd op de Algemene verordening gegevensbescherming (AVG). Onder de AVG is een schoolbestuur **verwerkingsverantwoordelijke** die te allen tijde de controle moet houden over de persoonsgegevens (privacy) van haar leerlingen, hun ouders en medewerkers. Het schoolbestuur bepaalt dus voor welke doelen deze gegevens mogen worden gebruikt. Een leverancier van software waarin de persoonsgegevens 'van de school' zijn opgenomen, wordt **verwerker** genoemd. Deze mag die persoonsgegevens niet zomaar voor eigen doeleinden gebruiken. Gebruik van persoonsgegevens bijvoorbeeld voor het verbeteren van de dienst, is dus niet zomaar toegestaan. Het (her)gebruik van persoonsgegevens van leerlingen, hun ouders en medewerkers wordt daarom door het schoolbestuur vastgesteld. Het gaat hierbij om gerechtvaardigde legitieme (zakelijke) doeleinden. Vaak zal een leverancier die persoonsgegevens wil hergebruiken, de gegevens moeten pseudonimiseren of anonimiseren zodat ze niet meer (direct) herleidbaar zijn tot personen.

In alle gevallen is het uitgangspunt dat de leverancier verwerker is en dat verwerking van gegevens beperkt is tot legitieme doeleinden. Een leverancier kan ook persoonsgegevens verwerken als verwerkingsverantwoordelijke. Denk hierbij aan de gegevens van de beheerder van de dienst, die gegevens registreert om een rekening te sturen etc.

IV. Centrale DPIA versus lokale DPIA

Een centrale DPIA wordt uitgevoerd door SIVON op applicatie niveau. Een centrale DPIA toetst of en wat de impact is van het gebruik (verwerking) van de applicatie is in relatie tot de bescherming van persoonsgegevens. Hoe kan de applicatie veilig gebruikt worden en welke (extra) maatregelen en instellingen zijn daarvoor nodig?

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

De toetsing of er sprake is van adequate gegevensbescherming, wordt in het kader van een DPIA ingegeven door de:

1. **gegevensverwerkingsanalyse:** kenmerken van de (voorgenomen) gegevensverwerkingen: een beschrijving van de voorgenomen verwerkingen, verwerkingsdoeleinden en werking van de applicatie,
2. **rechtmatigheid van de gegevensverwerkingen:** beoordeling van de rechtsgrond, de noodzaak, evenredigheid en verenigbaarheid van de voorgenomen verwerkingen in relatie tot de verwerkingsdoeleinden,
3. **aanwezige risico's**: beoordeling van de gevolgen van de verwerkingen voor de rechten en vrijheden van de betrokkenen,
4. **maatregelen:** adequate technische en organisatorische beveiligingsmaatregelen die zijn of worden genomen om de gevolgen (van de risico's) te beperken.

In het proces rondom de uitvoering van de DPIA, worden o.a. de volgende elementen uitgevoerd en opgeleverd:

1. Het beoordelen van (privacy) afspraken in de verwerkersovereenkomst en vastleggen van eventuele (verbeter)afspraken;
2. Het (technisch) toetsen van de applicatie of dit voldoet aan de afspraken;
3. Het maken van afspraken over maatregelen die nog niet zijn genomen;
4. Een correcte implementatie van de applicatie op de school;
5. Omgang door gebruikers en beheerders met de systemen (beleid en gedragscodes).

In de centrale DPIA worden de punten 1, 2 en 3 uitgevoerd door SIVON. Het schoolbestuur krijgt aanbevelingen voor punt 4 (bijvoorbeeld in de vorm van een technische handleiding). De school zal zelf met punt 5 aan de slag moeten.

In de lokale DPIA neemt de school – voor zover van toepassing – de punten 1, 2, en 3 over. Hierbij past de school de centrale bevindingen toe op de eigen organisatie: zijn alle onderdelen ook van toepassing op eigen organisatie? Er wordt beschreven op welke wijze op de school invulling wordt gegeven aan de implementatie (punt 4). Daarbij wordt overwogen of er nog daarbij specifieke risico's spelen en maatregelen nodig zijn die niet in de centrale DPIA benoemd zijn. De school zorgt zelf voor punt 5: een school zal zelf interne richtlijnen moeten opstellen wie toegang heeft tot welke data en hoe het verstrekken en intrekken van autorisaties georganiseerd is, etc. Welke handelingen je met welke ICT middelen mag uitvoeren ligt vast in een intern beleid of gedragscode.

De lokale DPIA is dus altijd noodzakelijk: SIVON heeft een algemene, centrale DPIA uitgevoerd en kan geen rekening houden met mogelijke lokale risico's van gebruik van de applicatie op scholen.

V. Gebruik model

De centrale DPIA volgt het model van de Rijksoverheid[2], aangevuld met onderwijs-specifieke informatie uit de *Handleiding uitvoeren data protection impact assessment (DPIA) voor het po en vo (versie 1.0)*[3]. Het model is daarnaast aangepast aan specifieke informatie over de applicatie en aangevuld met een model lokale dpia.

[2] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia.pdf
[3] https://aanpakibp.kennisnet.nl/app/uploads/Handreiking-DPIA-v1.0-1.pdf

Hierbij wordt rekening gehouden met de richtlijn van de gezamenlijke Europese toezichthouders, (EDPB) die in de Richtsnoeren voor gegevensbeschermingseffectbeoordelingen (2016/679, 4 april 2017) overwegen:

"De [EDPB] stimuleert de ontwikkeling van sectorspecifieke kaders voor gegevensbeschermingseffectbeoordelingen. De reden hiervoor is dat dergelijke kaders kunnen steunen op specifieke sectorkennis, wat betekent dat de gegevensbeschermingseffectbeoordeling kan worden gericht op de bijzonderheden van een bepaald type verwerking (bijvoorbeeld bepaalde soorten gegevens, bedrijfsactiva, mogelijke effecten, bedreigingen, maatregelen). Dit betekent dat de gegevensbeschermingseffectbeoordeling de problemen kan aanpakken die zich voordoen in een bepaalde economische sector, bij gebruik van specifieke technologieën of bij uitvoering van bepaalde soorten verwerkingen."

Deze DPIA bestaat derhalve uit 5 delen:

- Deel A is de beschrijving kenmerken gegevensverwerkingen (gegevensverwerkingsanalyse).
- Deel B is de beoordeling rechtmatigheid gegevensverwerkingen
- Deel C is de beschrijving en beoordeling risico's voor de betrokkenen
- Deel D is de beschrijving voorgenomen maatregelen die risico's moeten beperken
- Deel E is het model lokale DPIA

VI. Scope van deze DPIA

In deze DPIA ligt de focus op het softwarepakket AFAS (met daarin opgenomen AFAS Profit, AFAS InSite/Outsite en AFAS Poclet) ("de applicatie"), dat gebruikt kan worden om bedrijfsprocessen binnen een school te stroomlijnen. Het pakket bevat hiervoor verschillende soorten modules zoals:

- CRM;
- Financieel;
- HRM;
- Ordermanagement;
- Payroll;
- Projecten;
- Workflowmanagement.

In deze DPIA wordt ingezoomd op de modules **CRM**, **HRM** en **Payroll**. Alle modules van AFAS werken met één onderliggend systeem en database waarin persoonsgegevens verwerkt worden. Dit betekent dat de verwerking van persoonsgegevens voor alle modules dezelfde gegevens zullen bevatten. Ook vallen alle modules onder dezelfde verwerkersovereenkomst.

Verder is deze DPIA een momentopname. De DPIA vindt plaats aan de hand van de dienstverlening zoals die op dit moment wordt aangeboden. Wijzigingen in de overeenkomst of in de dienstverlening kunnen invloed hebben op de uitkomst van deze DPIA.

AFAS heeft in de algemene voorwaarden & service voorwaarden aangegeven dat ze continu bezig zijn met het verbeteren en het veranderen van de dienstverlening. De voorwaarden kunnen soms ook verbeterd of veranderd worden. Klanten die het niet eens zijn met een wijziging, kunnen een 'verbetersuggestie' insturen. AFAS zal vervolgens onderzoeken of een wijziging noodzakelijk is. De

overeenkomst kan in het uiterste geval na wijziging beëindigd worden. De oude voorwaarden gelden dan nog twee maanden.

SIVON zal elke drie jaar de DPIA opnieuw uitvoeren en zal tussentijdse wijzigingen monitoren en beoordelen of een tussentijdse evaluatie nodig is.

VII. Buiten scope

In deze DPIA zijn er ook bepaalde diensten die buiten de scope vallen en niet meegenomen worden in de beoordeling. Voorliggende DPIA ziet uitsluitend op de applicatie die gebruikt wordt door het schoolbestuur. De werkzaamheden en verwerkingen die door administratiekantoren worden uitgevoerd, worden niet meegenomen en vallen dus buiten de scope van deze DPIA. Wat ook buiten scope valt zijn de applicaties, bijvoorbeeld een arbodienst, die kunnen koppelen met AFAS. De buiten scope vallende verwerkingen zijn echter veelvoorkomend binnen schoolbesturen. Dit onderstreept het belang om in aanvulling op deze centrale DPIA een lokale DPIA uit te voeren.

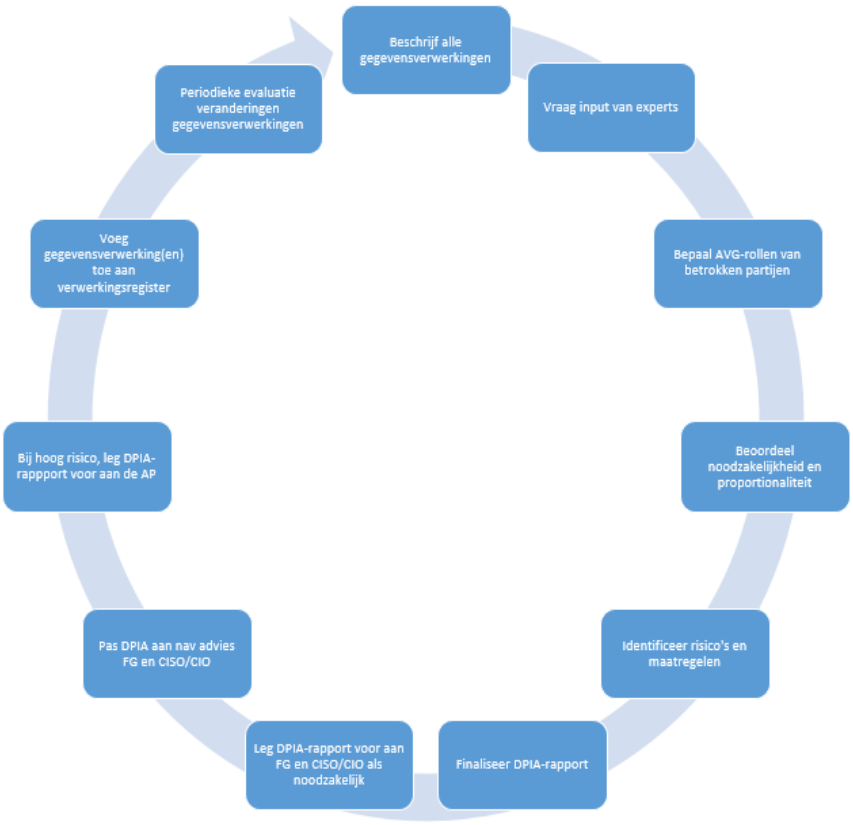
VIII. Methodiek

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

- Beoordeling van de verwerkingen, (verwerkers)overeenkomsten en rechtmatigheid
- Beoordeling van de mogelijkheid om als verwerkingsverantwoordelijke te voldoen aan rechten van betrokkenen (inclusief uitoefenen recht op inzage etc)
- Beoordeling van de default settings (privacy by design)
- Analyse van rapportage van (service) data beschikbaar voor verwerkingsverantwoordelijke
- Opstellen rapportage
- Overleg met leverancier over (aanvullende) maatregelen.

In november 2022 hebben drie meetings plaatsgevonden met met ondersteuning van ICTRecht, waarbij input is gegeven door vertegenwoordigers van AFAS en vertegenwoordigers van twee schoolbesturen (Esprit scholen en SCO Leiden) die gebruik maken van de applicatie. Tijdens deze meetings is voor de verwerkingen een procesbeschrijving vastgesteld.

Schematisch weergegeven volgt deze DPIA het volgende proces[4]:



IX. Definitie van verschillende gegevens

Alle type gegevens worden beschouwd als persoonsgegevens als ze direct of indirect tot een persoon te herleiden zijn. Hieronder vallen ook gepseudonimiseerde gegevens.

Diagnostische 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 service gegevens genoemd.]

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

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

Gewone persoonsgegevens zijn voor de hand liggende gegevens zoals iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens.

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 onderwijs geven aan en het begeleiden van een leerling. Ze zijn bijzonder omdat het gebruik van deze gegevens iemands privacy ernstig kan

[4] Model DPIA Rijksdienst versie 2.0, november 2021

beïnvloeden. Voorbeelden zijn gezondheidsgegevens, levensovertuiging, lidmaatschap van de vakbond, ras of etnische afkomst.

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, gezondheid of zelfs mishandeling. Het is extra belangrijk dat scholen zeggenschap houden over deze gegevens en weten wat daarmee gebeurt. Naarmate de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden volgens de AP[5] zwaardere eisen gesteld aan de beveiliging van de gegevens.

[5] https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013_snappet.pdf

3. 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

De AFAS-modules HRM en Payroll zijn door schoolbesturen in te zetten voor personeelsadministratie, verzuimregistratie, salarisverwerking, financiële administratie, projectadministratie en klantenrelaties. De persoonsgegevens zijn in eerste instantie afkomstig van de medewerker. In de loop van het dienstverband wordt door het schoolbestuur informatie toegevoegd over verzuim, functioneren en andere informatie omtrent het dienstverband.

Een gedetailleerde beschrijving van het proces HRM is beschikbaar op de pagina en (met name) de subpagina's onderaan op: https://help.afas.nl/help/NL/SE/Hrm.htm

Een gedetailleerde beschrijving van het proces Payroll is beschikbaar op de pagina en (met name) de subpagina's onderaan op: https://help.afas.nl/help/nl/se/Pay.htm

2. Persoonsgegevens

In dit onderdeel wordt beschreven welke categorieën persoonsgegevens van welke betrokkenen worden verwerkt binnen de applicatie.

De betrokkenen wiens persoonsgegevens worden verwerkt in AFAS zijn onderverdeeld in de volgende categorieën:

- Werknemers;
- Oud-werknemers;
- Stagiaires;
- Sollicitanten;
- Partner/kinderen van (oud)-werknemers;
- Noodcontactpersoon van (oud)-werknemers/stagiaires.

Persoonsgegevens

De verwerkte persoonsgegevens per categorie betrokkenen, de categorieën persoonsgegevens en op hoofdlijnen de bron van de persoonsgegevens worden hieronder samengebracht in één tabel:

Categorie betrokkene	Categorieën persoonsgegevens	Persoonsgegevens	Bron/verkrijging persoonsgegeven
Werknemers, oud-werknemers	• Gewoon • Bijzonder • Gevoelig • Wettelijk identificatie-nummer	naam; adres; e-mailadres (privé); e-mailadres (zakelijk) telefoonnummer; geboortedatum;	• Werknemer • Werkgever

		burgerservicenummer (Alle informatie op) identiteitsbewijs; bankrekening-nummer; burgerlijke staat; nationaliteit; geboorteplaats; geslacht; VOG; personeelsnummer; functietitel/-beschrijving; salarisgegevens; verzuimgegevens; overige informatie met betrekking tot de arbeidsrelatie; AOW-datum; autorisatiegegevens; overige gegevens (vrije invulvelden).	
Stagiaires	• Gewoon • Gevoelig • Bijzonder • Wettelijk identificatie-nummer	naam; adres; contactgegevens; sociale netwerken; geboortedatum; burgerservicenummer alle informatie op identiteitsbewijs; bankrekening-nummer; burgerlijke staat; nationaliteit; geboorteplaats; geslacht; VOG; personeelsnummer; functietitel/-beschrijving; salaris/vergoeding; overige informatie met betrekking tot de arbeidsrelatie; autorisatiegegevens; overige gegevens (vrije invulvelden).	• Werknemer • Werkgever
Sollicitanten	• Gewoon • Bijzonder	naam; adres; contactgegevens; sociale netwerken; geboortedatum;	• Sollicitant

		geslacht; VOG; CV; motivatiebrief; salarisindicatie; overige gegevens (vrije invulvelden).	
Partner/kinderen van (oud)-werknemers	• Gewoon • Bijzonder (in potentie als de relatie iets zegt over de seksuele voorkeur van de betrokkene)	naam; geboortedatum; adres; contactgegevens; geslacht.	• Werknemer
Noodcontactpersoon van (oud)-werknemers/stagiaires	• Gewoon • Bijzonder (in potentie als de relatie iets zegt over de seksuele voorkeur van de betrokkene)	naam; adres; contactgegevens; relatie tot werknemer.	• Werknemer
Werknemers (als gebruikers van het systeem)	• Gewoon	accountgegevens; metadata omtrent het gebruik van het systeem (zoals tijdstip, activiteit).	• Werknemer

3. Gegevensverwerkingen

Om de rechtmatigheid te kunnen beoordelen, is het noodzakelijk alle gegevensverwerkingen in beeld te krijgen. Denk hierbij aan het gehele verwerkingsproces, hoe de applicatie past in het applicatielandschap, de koppelingen en de gegevensstromen van en binnen de onderwijsinstelling. Het gaat er hier vooral om een beeld te schetsen van de scope van de gegevensverwerkingsanalyse.

Applicatielandschap

In deze DPIA ligt de focus puur op de applicatie AFAS. In het applicatielandschap van een schoolbestuur kunnen vanuit de applicatie koppelingen worden gelegd met andere applicaties. De andere applicaties vallen niet binnen de scope van deze DPIA.

Koppelingen

AFAS kent veel gecertificeerde koppelingen (“App connectoren”). Er komt onder andere een koppeling met de Belastingdienst, Arbodiensten, Fiscfree en Capisci. In AFAS Profit zijn enkele van de koppelingen standaard aanwezig. Deze koppelingen hebben voornamelijk te maken met de functionaliteit van AFAS zelf. Het schoolbestuur heeft de mogelijkheid om zelf Connectorgroepen aan te maken. AFAS heeft geen invloed op welke koppelingen de klant aanmaakt of in gebruik neemt. Alle koppelingen werken wel volgens dezelfde standaard functionaliteit.

Het is mogelijk om de verbindingen met de externe applicaties te beheren met een app connector. Vanuit de app connector is het mogelijk om tokens aan te maken of aan te vragen via One Time Password. Vervolgens is het via tokens mogelijk om toegang te geven tot de Connectoren/endpoints. AFAS werkt met zogenaamde GetConnectoren. De getconnector maakt record restricties mogelijk in de app connector. De app connector kan alleen records ophalen voor zover dit is toegestaan op basis van de filterautorisatie in de getconnector (welke gegevens gaan over de verbinding).

Meer gedetailleerde informatie over de koppelingen die bestaan/aan te maken zijn binnen AFAS is te vinden op de volgende pagina's van AFAS:

- App connector
- GetConnector

Beveiliging

Bij het maken van een koppeling is TLS1.2 vereist. Hier kan meer informatie gevonden over het gebruik van TLS1.2. Daarnaast kan er additionele beveiliging plaatsvinden op basis van IP restricties.

4. Verwerkingsdoeleinden

De verwerkingsdoeleinden zijn schematisch weergegeven en gekoppeld aan de bijbehorende gegevensverwerking(en). We maken voor de verwerkingsdoeleinden gebruik van de referentiearchitectuur (de FORA[6] voor het primair en voortgezet onderwijs).

Doeleinde verwerking(par.4 Verwerkingsdoeleinden)	Gegevensverwerking (par. 3. Gegevensverwerkingen.)[7]
Beheer personeelsgegevens	Opslaan, wijzigen, raadplegen, gebruiken, verwijderen gegevens van alle betrokkenen (alle categorieën betrokkenen)
Competentiemanagement	Opslaan, wijzigen, raadplegen, gebruiken, verwijderen gegevens met betrekking tot arbeidsrelatie (werknemers, oud-werknemer, stagiaires)
Formatieplanning en personeelsroostering	Opslaan, wijzigen, raadplegen, gebruiken, verwijderen gegevens met betrekking tot arbeidsrelatie (werknemers, oud-werknemers, stagiaires)
Instroom personeel	Opslaan, wijzigen, raadplegen, gebruiken, verwijderen gegevens met betrekking tot sollicitaties (sollicitanten, werknemers, oud-werknemers, stagiaires)
Opleiding en ontwikkeling	Opslaan, wijzigen, raadplegen, gebruiken, verwijderen gegevens met betrekking tot arbeidsrelatie (werknemers, oud-werknemers, stagiaires)
Personeelsbeoordeling	Opslaan, wijzigen, raadplegen, gebruiken, verwijderen gegevens met betrekking tot arbeidsrelatie (werknemers, oud-werknemers, stagiaires)

[6] https://www.wikixl.nl/wiki/fora/index.php/DPIA
[7] Zie https://fora.wikixl.nl/index.php/Bedrijfsfunctiemodel.

Uitstroom personeel	Opslaan, wijzigen, raadplegen, gebruiken, verwijderen gegevens met betrekking tot arbeidsrelatie (werknemers, oud-werknemers)
Verlof- en verzuimadministratie en -begeleiding	Opslaan, wijzigen, raadplegen, gebruiken, verwijderen gegevens met betrekking tot arbeidsrelatie en verzuim (werknemers, oud-werknemers, stagiaires)
Authenticatie en autorisatie	Opslaan, wijzigen, raadplegen, gebruiken, verwijderen autorisatiegegevens (werknemers, oud-werknemers, stagiaires)
Salarisverwerking	Opslaan, wijzigen, raadplegen, gebruiken, verwijderen salarisgegevens, gegevens met betrekking tot arbeidsrelatie en bankrekeningnummer (werknemers, oud-werknemers, stagiaires)

5. Betrokken partijen

Naam partij	AVG-rol	Functie/taak	Betrokken persoonsgegevens en toegang
Schoolbestuur	Verwerkings-verantwoordelijke	Werkgever	Alle persoons-gegevens die een schoolbestuur invoert.
AFAS	Verwerker	Voert de verwerking uit in opdracht van verwerkingsverantwoordelijke	Alle persoons-gegevens die een schoolbestuur invoert
LeaseWeb	Subverwerker	Hosting	Alle persoons-gegevens die een schoolbestuur invoert

6. Belangen bij de gegevensverwerking

De bedrijfsprocessen zoals beschreven in par. 4 dienen allen de essentiële bedrijfsbelangen (waaronder financiële belangen en het belang van goed werkgeverschap) van de school.

Het inschakelen van een hostingpartij dient het bedrijfsbelang van AFAS om betrouwbare opslag en beschikbaarheid van de gegevens te kunnen bieden.

7. Verwerkingslocaties

De persoonsgegevens die door de scholen in AFAS worden geregistreerd, worden opgeslagen op servers van LeaseWeb. AFAS gebruikt uitsluitend datacenters die zich in Nederland (Schiphol-rijk en Haarlem) bevinden. Bij het gebruik van Europese datacenters vindt er geen doorgifte van gegevens plaats naar buiten de EER.

Wanneer het nodig is dat medewerkers van AFAS toegang hebben tot persoonsgegevens van het schoolbestuur, bijvoorbeeld voor ondersteuning op afstand, gebeurt dat binnen Nederland.

8. Technieken en methoden van gegevensverwerking

De applicatie AFAS is een SaaS-applicatie. Dit houdt in dat AFAS een op de cloud gebaseerd softwareleveringsmodel is waarin de provider (AFAS) cloudapplicatiesoftware ontwikkelt, onderhoudt en automatische softwareupdates levert.

Elke dag wordt een back-up gemaakt die 31 dagen wordt bewaard. De eerste back-up van de maand wordt daarnaast 12 maanden bewaard en de eerste back-up van het jaar wordt 7 jaar bewaard. Back-ups ouder dan 7 jaar worden verwijderd. Het terugzetten van een back-up gebeurt geautomatiseerd, en is voor klanten beschikbaar om zelfstandig uit te voeren.

Continuïteit wordt verder gewaarborgd op de manieren zoals beschreven op: https://klant.afas.nl/afas-online/continuiteit.

AFAS voert diverse controles uit en heeft certificeringen zoals ISO 9001 en ISO27001.[8] Verder verloopt alle authenticatie via een login portal met verplichte 2-factor authenticatie. Daarnaast is de informatiebeveiliging gecontroleerd door een externe auditor.

AFAS Online is beveiligd middels de volgende maatregelen:[9]

- De systemen zijn geïnstalleerd met het 'Least privilege principe'.
- Verschillende anti-virus en anti-malware maatregelen zijn geïmplementeerd.
- 'Applicatie allowlisting' is ingericht.
- Alerting op basis van verdachte log-gebeurtenissen.
- Minimaal jaarlijkse manuele attack- and penetration tests door externe partijen zoals Computest.
- Dagelijkse scans/base-lining op bekende kwetsbaarheden met behulp van Marvin_ van Computest.
- 24x7 netwerkmonitoring op basis van Managed Detection and Response van Fox-IT.
- Patchbeleid om securitypatches zeer snel uit te rollen.
- Constante job-rotation onder de systeembeheerders.
- Applicatie en server hardening.
- VLAN scheiding en gebruik van een zero-trust model.
- Content scanning: AFAS Online controleert de door gebruikers vastgelegde gegevens op virussen en andere malware op plaatsen waar deze gevaar kunnen vormen voor de infrastructuur van AFAS Online.
- Just-in-time administration: tijdelijk geldige beheer accounts.
- Moderne TLS-verbindingen: TLS 1.2.
- Verplichte sterke authenticatie.
- Gescheiden Out-Of-Band (OOB) netwerken.
- Automatische DDoS mitigatie.

Het inrichten van de authenticatie en het veilig houden van de toegang tot de applicatie, ligt bij het schoolbestuur.

[8] https://klant.afas.nl/file/download/default/FBFB9E2F42A43EF0887F9E8CEDDB71DC/AFAS%20Algemene%20Voorwaarden%20en%20Service%20overeenkomst%20v%2015-4%20gefixte%20branche%20bijlages.pdf, p. 26

[9] Zie https://klant.afas.nl/afas-online/security

9. Juridisch en beleidsmatig kader

Hieronder is beschreven welke wet- en regelgeving, naast de AVG, nog meer van toepassing zijn op de gegevensverwerking.

Specifieke wetgeving / beleid	Doeleinde	Gegevens
Artikel 7:611 Burgerlijk Wetboek	Rechtmatig gebruik persoonsgegevens (goed werkgeverschap)	Gegevens medewerkers, oud-medewerkers, stagiaires
o.a. Artikel 6 , 9, 18 en 18a Wet op de loonbelasting 1964	Nakomen belastingplichten en pensioenregelingen	Gegevens medewerkers, oud-medewerkers, stagiaires
o.a. Artikel 3, 14, lid 1 sub b, en 29a Arbeidsomstandighedenwet	Nakomen wettelijke verplichtingen werkgever	Gegevens medewerkers, oud-medewerkers, stagiaires
Wet Arbeidsmarkt in Balans (WAB)	Nakomen wettelijke verplichtingen werkgever	Gegevens medewerkers, oud-medewerkers, stagiaires
Wet verbetering poortwachter	Nakomen wettelijke verplichtingen werkgever	Gegevens medewerkers, oud-medewerkers, stagiaires
o.a. artikel 4:4a Wet arbeid en zorg	Nakomen wettelijke verplichtingen werkgever	Gegevens medewerkers, oud-medewerkers, stagiaires
Wetboek van Strafrecht	Nakomen wettelijke verplichtingen werkgever	Alle gegevens
Artikel 12, eerste lid, sub m Wet Medezeggenschap op scholen	Instemming op de beleidsregels voor verwerking van persoonsgegevens	Gegevens medewerkers

10. Bewaartermijnen

In AFAS[10] is het mogelijk om zelf bewaartermijnen in jaren vast te leggen voor een type dossieritem en/of voor een kenmerkcombinatie van een type dossieritem. Het is daarbij mogelijk om zelf te bepalen wanneer een bewaartermijn gaat lopen. Dit kan zijn vanaf de aanmaakdatum van het dossieritem, de begin- en of einddatum of de uitdienstdatum van de werknemer.

Dossieritems worden overigens niet automatisch verwijderd na de bewaartermijn. Er dient een verwijderset aangemaakt te worden, gebaseerd op een peildatum. Vervolgens kan bepaald worden welke typen dossieritems verwijderd mogen worden.

Per schoolbestuur dienen de bewaartermijnen voor een type dossieritem vastgelegd te worden. Daarbij dienen de wettelijke bewaartermijnen ook in acht genomen te worden.[11]

Categorie betrokkene	Persoonsgegevens	Bewaartermijnen

[10] Zie: https://help.afas.nl/help/NL/SE/CRM_Doss_Legal_Del.htm#o118431. Zie voor algemene informatie over het verwijderen van persoonsgegevens en bewaartermijnen ook: https://help.afas.nl/help/NL/SE/Crm_PerOrg_Relat_Delete_AVG.htm

[11] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering/personeelsdossiers#hoe-lang-mag-ik-als-werkgever-de-gegevens-in-een-personeelsdossier-bewaren-8618

Werknemers, oud-werknemers	Gegevens betreffende een werknemer, vereist voor de Uitvoeringsregeling loonbelasting.[12] Te weten: - naam; - geboortedatum; BSN; - adresgegevens; - gegevens voor de inkomstenbelasting; - kopie ID-bewijs.	Tot **5 jaar** na einde van het kalenderjaar, waarin werknemer uit dienst treedt.
Werknemers, oud-werknemers	Gegevens betreffende een werknemer, verwerkt in het kader van de Wet verbetering poortwachter.[13]	**2 jaar** na uitdiensttreding en en 10~~5~~ **jaar** na uitdiensttreding voor eigen risicodragers voor de WIA (artikel 1 van de Regeling vaststelling periode eigenrisicodragers WGA-uitkeringen).
Werknemers, oud-werknemers	Salarisadministratie inclusief afspraken betreffende salaris en arbeidsvoorwaarden.[14]	**7 jaar** na uitdiensttreding.
Werknemers, oud-werknemers	Fiscale gegevens. Te weten: - Uitgaande facturen - Inkomsten - Ontvangen facturen Privégebruik van goederen en diensten.	**7 jaar** nadat de actualiteitswaarde is vervallen.
Werknemers, oud-werknemers	Gegevens vereist voor de Uitvoeringsregeling loonbelasting.	**5 jaar** na het kalenderjaar waarin werknemer uit dienst treedt.
Werknemers, oud-werknemers	Verslagen in het kader van de Wet verbetering poortwachtwachter	**2 jaar of 5 jaar** voor eigenrisicodragers na uitdiensttreding.
Werknemers, oud-werknemers	Personeelsdossier. Te weten: - Arbeidsovereenkomst en wijzigingen - Correspondentie over benoemingen, promotie, demotie en ontslag	Maximaal **2 jaar** na uitdiensttreding.

[12] Art. 7.9 Uitvoeringsregeling loonbelasting
[13] Wet verbetering poortwachter.
[14] Art. 52 Algemene wet inzake rijksbelastingen.

	Verslagen over functioneringsgesprekken	
Stagiaires	Alle voornoemde gegevens	Maximaal **6 maanden** na einde stage.
Sollicitanten	Sollicitatiegegevens	**4 weken of 1 jaar** (bij verkrijging toestemming)
Partner/kinderen van (oud)-werknemers	naam; geboortedatum; adres; contactgegevens; geslacht.	Maximaal **6 maanden** na uitdiensttreding.
Noodcontactpersoon van (oud)-werknemers/stagiaires	naam; adres; contactgegevens; relatie tot werknemer.	Maximaal **6 maanden** na uitdiensttreding.
Werknemers (als gebruikers van het systeem	accountgegevens; metadata omtrent het gebruik van het systeem (zoals tijdstip, activiteit).	maximaal **1 jaar** na uitdiensttreding; maximaal **1 jaar** na verzameling.

4. 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

Ieder schoolbestuur is zelf verantwoordelijk voor het vaststellen van de rechtsgrond voor iedere verwerking/ieder doeleinde. Voor de doeleinden van het gebruik van de applicatie is echter vanuit de ervaring en 'best practices' een waarschijnlijk toepasselijke rechtsgrond beschikbaar. Hieronder worden die rechtsgronden per verwerking/doeleinde aangegeven.

Artikel 6, eerste lid, AVG noemt de volgende mogelijke grondslagen voor de verwerking van gegevens:

a) Toestemming van de betrokkene
b) Uitvoering van een overeenkomst
c) Wettelijke verplichting[15]
d) Vitaal belang van de betrokkene
e) Taak van algemeen belang[16] (of openbaar gezag)
f) Gerechtvaardigd belang

Verwerking/doeleinde	Grondslag AVG	Toelichting
Beheer personeelsgegevens	Uitvoering van een overeenkomst of Wettelijke verplichting Artikel 6, eerste lid, sub b en c, AVG.	Arbeidsovereenkomst, nakoming wettelijke (fiscale) verplichtingen
Competentiemanagement	Uitvoering van een overeenkomst Artikel 6, eerste lid, sub f, AVG.	Gerechtvaardigd belang
Formatieplanning en personeelsroostering	Uitvoering van een overeenkomst Artikel 6, eerste lid, sub f, AVG.	Gerechtvaardigd belang
Instroom personeel	Toestemming en gerechtvaardigd belang Artikel 6, eerste lid, sub a en f, AVG.	Toestemming in geval CV langer dan 4 weken in portefeuille blijft. Gerechtvaardigd

[15] 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.
[16] 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.

		belang t.a.v. werving i.hk.v. bedrijfsvoering
Opleiding en ontwikkeling	Uitvoering van een overeenkomst Artikel 6, eerste lid, sub b en f, AVG.	Arbeidsovereenkomst Gerechtvaardigd belang
Personeelsbeoordeling	Uitvoering van een overeenkomst Artikel 6, eerste lid, sub b en f, AVG.	Arbeidsovereenkomst Gerechtvaardigd belang
Uitstroom personeel	Uitvoering van een overeenkomst Wettelijke verplichting Artikel 6, eerste lid, sub b en c, AVG.	Arbeidsovereenkomst, nakoming wettelijke (fiscale) verplichtingen
Verlof- en verzuimadministratie en -begeleiding	Uitvoering van een overeenkomst Wettelijke verplichting Artikel 6, eerste lid, sub b en c, AVG.	Arbeidsovereenkomst, nakoming wettelijke (Arbo) verplichtingen
Authenticatie en autorisatie	Gerechtvaardigd belang Artikel 6, eerste lid, sub f, AVG.	Gerechtvaardigd belang informatiebeveiliging
Salarisverwerking	Uitvoering van een overeenkomst Wettelijke verplichting Artikel 6, eerste lid, sub b en c, AVG.	Arbeidsovereenkomst, nakoming wettelijke (fiscale) verplichtingen

13. Bijzondere persoonsgegevens

Middels de applicatie worden bijzondere persoonsgegevens verwerkt. Zoals onder 12. beschreven is het vaststellen van de juiste grondslag aan het schoolbestuur. Dit kan namelijk verschillen per situatie en verdient een zorgvuldige juridische afweging.
Het verwerken van bijzondere persoonsgegevens is in beginsel verboden. De uitzonderingsgronden voor het verwerken van bijzondere persoonsgegevens zijn te vinden in artikel 9 lid 2 sub b van de AVG, de uitvoeringswet AVG of wanneer een andere wet van toepassing is. Dit geldt ook voor de verwerking van een wettelijke identificatienummer zoals het BSN.
Een gemiddeld schoolbestuur zal, voor de uitvoering van haar HR-taken, mogelijk gegevens verwerken met betrekking tot etniciteit (monitoring t.b.v. stimuleren gelijke kansen), seksuele voorkeur (uit de registratie contactgegevens partner kan dit indirect worden afgeleid), religieuze overtuigingen (mogelijk herleidbaar aan de hand van op te nemen vrije religieuze dagen en/of specifieke dieetwensen) en gezondheid (bijvoorbeeld ziekmeldingen en re-integratietrajecten).

De werkgever mag uitsluitend de bijzondere persoonsgegevens van de werknemer verwerken op basis van art. 9 lid 2 sub b van de AVG, evenals artikel 22-24 en 30 van de UAVG. Deze verwerking is slechts toegestaan indien deze noodzakelijk is om te voldoen aan de geldende wettelijke verplichtingen en verwerkingsdoeleinden die voortkomen uit zowel het arbeidsrecht als het sociale zekerheids- en sociale beschermingsrecht. Het is van essentieel belang dat de verwerking in lijn is met deze rechtmatige grondslagen.

14. Doelbinding

Van doelbinding is sprake wanneer het schoolbestuur zich houdt aan de eigen vooraf vastgestelde verwerkingsdoelen bij het gebruik van de applicatie. Het is alleen middels beleid van het schoolbestuur mogelijk om de doelen van de gegevensverwerking te beperken. Dit dient te gebeuren door het toevoegen, wijzigen of inzien van gegevens te beperken tot gebruikers waarvoor dat nodig is voor doelen die passen bij hun functie.

De beoordeling van de noodzakelijkheid, proportionaliteit en subsidiariteit van het opnemen van persoonsgegevens in de applicatie, gebeurt door het schoolbestuur. Het schoolbestuur kan middels beleid rondom het gebruik van de applicatie waarborgen dat er alleen noodzakelijke gegevens worden verwerkt (en dat deze gegevens ook alleen worden verwerkt op manieren die noodzakelijk zijn). Gezien de grote vrijheid bij het invullen van gegevens in de applicatie, bijvoorbeeld de aanwezigheid van vrije invulvelden en de mogelijkheid van maatwerk van invulvelden in het algemeen, is het belangrijk dat schoolbesturen dit beleid ook opstellen en de naleving controleren. Bij de inventarisatie voor deze DPIA is niet gebleken dat het gebruik van de applicatie per definitie niet-noodzakelijke gegevens met zich meebrengt. Wel dient het schoolbestuur beleid te implementeren om te zorgen dat vrije invulvelden niet worden gevuld met informatie die niet strikt noodzakelijk is voor de vastgestelde doelen.

15. a. Noodzakelijkheid

De schoolbesturen zijn ervoor verantwoordelijk om vast te stellen of de voorgenomen verwerkingen van persoonsgegevens noodzakelijk zijn voor de doeleinden zoals beschreven onder 4. Uit de inventarisatie voor deze DPIA zijn geen verwerkingen gebleken die niet noodzakelijk zijn voor de verwerkingsdoeleinden. Wel dient elk schoolbestuur de afweging te maken of de vaste en de vrije invulvelden noodzakelijk zijn voor de verwerkingsdoeleinden die het schoolbestuur heeft vastgesteld, bij het gebruik van de applicatie. Het is aan de schoolbesturen om ten aanzien van dit onderdeel de doelen voor het vastleggen nader te specificeren en hierover te communiceren.

15. b. Proportionaliteit en subsidiariteit

De schoolbesturen zijn ervoor verantwoordelijk om vast te stellen of de voorgenomen verwerkingen van persoonsgegevens binnen de eisen van proportionaliteit en subsidiariteit vallen, voor de doeleinden zoals beschreven onder 4. Net als beschreven onder 15. a. Noodzakelijkheid, dient elk schoolbestuur ook hier de afweging te maken rond proportionaliteit en subsidiariteit, voor de verwerkingsdoeleinden die het schoolbestuur heeft vastgesteld, bij het gebruik van de applicatie. Denk hierbij aan het hanteren van de juiste bewaartermijnen, inregelen van passende autorisaties en het op orde hebben van de beveiliging.

16. Rechten van de betrokkenen

Recht van betrokkene	Toelichting procedure	Evt. beperking verwerking*
Het recht op informatie	Betrokkenen dienen middels een interne privacyverklaring op de hoogte te worden gesteld van de gegevensverwerking. Er dient een contactpersoon beschikbaar te zijn (zoals een privacy officer of de FG) die	n.v.t.

	desgevraagd nadere toelichting kan geven over de gegevensverwerking. Informatie over de gegevensverwerking gaat buiten de applicatie om.	
Het recht van inzage	Er dient een procedure aanwezig te zijn waarmee binnen de wettelijke termijn inzage kan worden geboden in de persoonsgegevens, wanneer een betrokkene daarom verzoekt. De applicatie biedt een employee self service (ESS) waarmee alle gegevens over de ingelogde persoon kunnen worden getoond.	n.v.t.
Het recht op rectificatie	Er dient een procedure aanwezig te zijn waarmee binnen de wettelijke termijn persoonsgegevens kunnen worden gewijzigd, wanneer een betrokkene daarom verzoekt, zover de persoonsgegevens daadwerkelijk onjuist zijn en deze kunnen worden gewijzigd binnen de wettelijke en contractuele verplichtingen om de verwerkingsdoelen te kunnen naleven.	n.v.t.
Het recht op gegevenswissing	Er dient een procedure aanwezig te zijn waarmee binnen de wettelijke termijn persoonsgegevens kunnen worden verwijderd, wanneer een betrokkene daarom verzoekt, zover mogelijk binnen de verplichtingen om de verwerkingsdoelen te kunnen naleven. Hieraan wordt binnen de applicatie voldaan. Deze beschikt over voldoende mogelijkheden om het verwijderingsrecht uit te voeren.	Wettelijke bewaartermijnen
Het recht op beperking van de verwerking	Er dient een procedure aanwezig te zijn waarmee binnen de wettelijke termijn kan worden voldaan aan het recht op beperking van de verwerking, wanneer een betrokkene daarom verzoekt, zover mogelijk binnen de verplichtingen om de verwerkingsdoelen te kunnen naleven. Het is in de applicatie mogelijk om gegevens die niet meer in gebruik zijn, te blokkeren. In alle gegevensverzameling is het mogelijk om geblokkeerde gegevens	n.v.t.

	niet te tonen. Het gebruik (of misbruik) van gegevens kan daardoor worden voorkomen.	
Een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens	Wanneer gegevens in de applicatie zijn gerectificeerd of gewist, dient het schoolbestuur eventuele derde ontvangers op de hoogte te brengen.	n.v.t.
Het recht op overdraagbaarheid van gegevens	Er is eenvoudig een machine-leesbare export te downloaden van de gegevens per medewerker.	n.v.t.
Het recht van bezwaar	Er dient binnen de school een procedure aanwezig te zijn waarmee binnen de wettelijke termijn kan worden gereageerd op een bezwaar tegen een verwerking waar dit op basis van de geldende rechtsgrond (zie 12.) mogelijk is. Zie ook de lokale DPIA.	n.v.t.
Het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit	Middels de applicatie worden geen geautomatiseerde conclusies getrokken of besluiten genomen. Scholen dienen te voorkomen dat de gegevens uit de applicatie worden gebruikt voor uitsluitend op een geautomatiseerde verwerking gebaseerde besluiten.	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.*

5. 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[17] om risico's te classificeren. Hierbij wordt 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.

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.

[17] 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

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 of gevolgen	Grote – onvermijdelijke – ernstige schade 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 voordoen; per maand, week of zelfs dag

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

17. Risico’s

In onderstaande tabel worden de applicatie-specifieke risico’s beschreven. Deze risico's zijn inherent aan het gebruik van AFAS. 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 AFAS wordt ingezet of dat het risico het systeem zelf betreft (de AFAS applicatie). Er is gebruik gemaakt van de Algemene Voorwaarden en Service Overeenkomst van februari 2022.

Naast de applicatie-specifieke risico's zijn er ook organisatie-risico's en algemene applicatie-risico's. Omdat de focus hier verschuift van de AFAS applicatie naar de noodzakelijke basis die op het gebied van privacy inbedding door het schoolbestuur wordt verondersteld zijn deze opgenomen in de lokale DPIA.

Risico nr.	Risico-omschrijving	Oorzaak en mogelijke gevolgen voor betrokkenen	Gevolgen	Kans	Impact	Risico	Proces en/of systeemrisico
1.	Er kan binnen AFAS gemaild worden, maar niet beveiligd bijv. door encryptie met wachtwoord, beperkte beschikbaarheidstermijn of het niet kunnen doorsturen of downloaden.	Mailverkeer wordt onvoldoende beveiligd of beperkt in de applicatie.	Mails kunnen onderschept worden. Gevoelige gegevens van medewerkers worden openbaar. Voornoemde kan verder leiden tot reputatieschade en juridische consequenties.	3	2	hoog	Proces en Systeem
2.	Wijziging van de verwerking van persoonsgegevens of een daarmee samenhangend onderdeel zoals genoemd in artikel 28, derde lid, aanhef en sub a tot en met h, van de AVG kan plaatsvinden door AFAS	De artikel 28 AVG bepalingen die veelal in een verwerkers-overeenkomst worden	Gegevens kunnen worden verwerkt onder voorwaarden waar het schoolbestuur niet mee heeft	2	2	Midden	Proces

	door de eenzijdig opgelegde, algemene voorwaarden (AV) aan te passen.	overeengekomen kunnen in de AV eenzijdig door AFAS worden aangepast.	ingestemd. Dit ondermijnd de verhouding tussen verwerker en verwerkingsverant woordelijke ten aanzien van de gezamenlijke afspraken die zij maken over de naleving van de AVG.				
2a	De AV vermeldt niet om welke verwerking(en) en soort persoonsgegevens het gaat (ook geen onderscheid tussen 'onlosmakelijk verbonden' en 'optioneel'). Deze vermelding is verplicht (AVG artikel 28 lid 3 aanhef). Voorstel is een bijlage toe te voegen met een volledige uitwerking. > Verwijzing naar het AFAS (Help) Center is onvoldoende (dit is een dynamische bron; bij wijzigingen wijzigt ook de verwerkersovereenkomst/AV). Voornoemde velden worden veelal door de verwerkingsverantwoordelijke gevuld in de verwerkingsbijlage van de verwerkersovereenkomst.	Geen opsomming van de te verwerken persoonsgegevens, categorieën van betrokkenen etc. opgenomen.	De basis van de verwerkingen is onvoldoende vastgelegd waardoor niet of onvoldoende kan worden voldaan aan de rechten van betrokkenen, kunnen de verwerkingsregister s niet goed gevuld worden, is er geen goede beoordeling mogelijk bij een datalek, etc.	3	2	Hoog	Proces
2b	De AV kent geen expliciete looptijd welke is gekoppeld aan de	Geen afspraken over duur en	Tot het moment waarop verwerker	2	2	Midden	Proces

	bepalingen die specifiek zien op de verwerking van persoonsgegevens. Dat is riskant, omdat hij moet gelden gedurende de hele duur van de verwerkingen. Hier moet expliciet worden aangesloten bij de hoofdovereenkomst.	beëindiging van de bepalingen opgenomen in de AV.	kan beschikken over de persoonsgegevens van de verwerkingsverant woordelijke dienen de hiervoor relevante bepalingen van toepassing te blijven. Onzekerheid over duur van de verwerking en mogelijk niet-naleving van de AVG en verhoogde risico's op ongeoorloofde gegevensverwerkin g.				
2c	Er is geen regeling over wanneer doorgifte van persoonsgegevens naar buiten de EER is toegestaan. Dit is verplicht (artikel 28 lid 3 sub a AVG) en moet dus worden toegevoegd.	Bepaling over doorgiftevoorwaar den niet opgenomen in de AV	Toestemming door de verwerker zou voorwaardelijk gesteld moeten zijn aan doorgifte van persoonsgegevens buiten de EER. Geen regeling kan leiden tot onrechtmatige gegevensoverdrach t, geen	2	2	Midden	Proces

			mogelijkheid tot controle op aanvullende waarborgen.				
2d	De AV bevat weliswaar een bepaling over vernietiging van persoonsgegevens, maar geen bepaling over teruggave na afloop van de verwerking. Dat is verplicht (artikel 28 lid 3 sub g AVG) en moet dus worden toegevoegd. 'Verwijdering van alle persoonsgegevens' mag explicieter, bijvoorbeeld door op te nemen dat dit de vernietiging van alle kopieën van de persoonsgegevens betreft, ook die in backups en bij subverwerkers.	Ontbreken specifieke bepalingen over vernietiging en teruggave na afloop van de verwerking in de AV	Het niet opnemen van verplicht gestelde onderdelen uit artikel 28 van de AVG is een, zowel voor de verwerker als de verwerkingsverantwoordelijke, op zichzelf staande schending van de AVG. Daarnaast zijn er de volgende risico's: onnodig behouden van persoonsgegevens zonder grondslag, onduidelijkheid over verantwoordelijkheid en verplichting van de verwerker om alle persoonsgegevens en kopieën ervan terug te geven en welke technologie hiervoor wordt	2	2	Midden	Proces

			gebruikt, toename kans op geschillen en juridische complicaties bij onduidelijkheid over wijze van verwijderen en mogelijkheden tot teruglevering van de gegevens.				
2e	Nergens wordt vermeld dat de verwerker bijstand moet verlenen bij het nakomen van de verplichtingen uit artikel 32 tot en met en 36 AVG. Dat moet worden toegevoegd, want dat is verplicht (artikel 28 lid 3 sub f AVG). Wel wordt aangegeven dat AFAS de klant hulp biedt bij de uitvoering van de rechten van betrokkenen.	Het ontbreken van de verplichting voor de verwerker om bijstand te verlenen bij het naleven van de AVG-artikelen 32 tot en met 36 kan leiden tot inadequaat gegevensbeheer en schendingen van de privacyrechten van betrokkenen. Dit kan juridische risico's en verminderde gegevensbescherming tot gevolg hebben.	Verminderde en onduidelijke medewerkingsverplichtingen op het gebied van het eerbiedigen van de bepalingen in artikel 32 tot en met 36 brengen grote en uiteenlopende AVG nalevingsrisico's met zich mee. Bijvoorbeeld het niet voldoen aan deze vereisten hetgeen kan leiden tot inbreuken op de privacy en een gebrek aan effectieve beschermingsmaatregelen.	2	2	Midden	Proces

2f	De AV vermeldt niet dat de verwerker het moet melden als instructies kennelijk in strijd met de AVG zijn. Dat is vereist (artikel 28 lid 3 laatste zin) en moet dus worden toegevoegd.		Het niet opnemen van verplicht gestelde onderdelen uit artikel 28 van de AVG is een, zowel voor de verwerker als de verwerkingsverantwoordelijke, op zichzelf staande schending van de AVG.	2	2	Midden	Proces
2h	Uit artikel 28, derde lid, sub c, van de AVG volgt dat verwerker alle overeenkomstige artikel 32 vereiste maatregelen neemt (passende technische en organisatorische maatregelen om een op het risico afgestemde beveiligingsniveau te waarborgen). De beveiligingsplicht is slechts gegeven als een algemene plicht tot adequate beveiliging. Dit moet worden gecomplementeerd met een concrete verwijzing naar een bijlage met maatregelen. > Verwijzing naar een ISO/NEN-certificering is onvoldoende. Verwijzing naar de Product online pagina (ofwel naar de AFAS Klantportal) is mooi, maar dit is een dynamische bron; bij wijzigingen wijzigt ook de		Het niet opnemen van verplicht gestelde onderdelen uit artikel 28 van de AVG is een, zowel voor de verwerker als de verwerkingsverantwoordelijke, op zichzelf staande schending van de AVG.	2	2	Midden	Proces

	verwerkersovereenkomst/AV). BIV-classificatie ontbreekt.						
3.	1.Onduidelijkheid gebruik gegevens t.b.v. verbetering product of informeren klant over gebruik. De algemene voorwaarden informeren de gebruiker onder het kopje “instructie verwerking” p.22 dat er sprake is van een verzameling van geanonimiseerde gegevens over het gebruik van de producten en diensten. Ten tijde van de DPIA is kenbaar gemaakt dat er geen sprake is van analyse van gebruikersgegevens die tot de gebruiker herleidbaar zijn. 2.In de zin "*Daarnaast kunnen we anonieme gegevens verzamelen waarbij deze herleidbaar zijn naar het abonnement en zullen deze doorgeven aan de afdelingen Customer Care en Succesmanagement. Zij kunnen je dan informeren bij programmafouten of adviezen geven over het gebruik van de programmatuur.*" is er een tegenstrijdigheid tussen het begrip "anonieme gegevens" en "herleidbaar zijn naar het	1.Tegenstrijdigheid in de algemene voorwaarden over de verwerking van gebruikersdata nu wordt gesteld dat hier geen sprake van is. 2. Er ontstaat onduidelijkheid over de verwerking van de vermeende anonieme gegevens, aangezien deze te herleiden zijn naar de abonnementhouder. Het is onduidelijk welke specifieke gegevens precies worden verwerkt.	1.Zonder aanpassing van de bepaling over gebruik van gebruikersdata blijft onduidelijkheid voor de gebruiker ontstaan over welke data dit betreft. 2. Verwerking voldoet niet aan het transparantiebeginsel.	3	1	Midden	Proces

	abonnement." Hierdoor ontstaat een onlogische en tegenstrijdige situatie. Anonieme gegevens horen per definitie niet herleidbaar te zijn tot individuele personen, abonnementen of andere identificeerbare informatie. Correctie en verduidelijking van de verwerking is noodzakelijk om duidelijk inzicht te krijgen in wat er voor welk doeleinde wordt verwerkt. In deze gecorrigeerde versie wordt duidelijk gemaakt dat de gegevens niet herleidbaar zijn naar individuele abonnementen, wat de term "anonieme gegevens" ondersteunt. Hiermee wordt de tegenstrijdigheid opgelost en wordt de zin logisch en begrijpelijk.						
4.	Geen (automatische) toepassing van en/of controle op bewaartermijnen.	De applicatie kent geen systeem om documenten waarvan de bewaartermijn verloopt geautomatiseerd te verwijderen of te signaleren voor verwijdering.	Persoonsgegevens worden niet tijdig opgeschoond. Er wordt niet voldaan aan de bewaar- en opschoonplicht.	2	2	Midden	Proces

5.	Onduidelijkheid betekenis “ondersteuning” branchemodellen verwerkersovereenkomst op p.25 Algemene voorwaarden. Hierin staat een link naar de bijlagen van het model. AFAS “ondersteunt” een tweetal branchemodellen verwerkersovereenkomsten zonder dat de gebruiker deze overeen kan komen met AFAS. Er volgt geen concrete uiting van het feitelijk van toepassing verklaren of verbinden aan de bepalingen van de branchemodellen hetgeen tot gevolg heeft dat deze alinea verwarring over de interpretatie kan opleveren	Het verouderde Generiek Model Verwerkersovereen komst 3.0 framework IBP behorend bij het convenant ‘Digitale onderwijsmiddelen en privacy 3.0” in beheer bij edu-k, van Kennisnet wordt benoemd in de AV als zijnde een branchemodel die door AFAS wordt ondersteund, zonder de precieze status te beschrijven.	De gebruiker kan niet goed inschatten welke afspraken van toepassing zijn op de verwerking van persoonsgegevens en kan ten onrechte veronderstellen dat een branchemodel verwerkersovereen komst kan worden gebruikt.	2	2	Midden	Proces

6. 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.

18. Maatregelen

Hieronder staat beschreven welke technische, organisatorische en juridische maatregelen in redelijkheid (kunnen) worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen.

Risicon	Omschrijving risico	Risico	Mogelijke maatregel (Org= Organisatorisch / Techn= Technisch) *Indien maatregel voor* AFAS *zelf geldt, is dit hieronder aangegeven.*	Restrisico en toelichting	Eigenaar maatregel	Toelichting	datum implementatie

r .						
2 t/ m 2h	Er kleven uiteenlopende risico's aan de binnen de algemene voorwaarden opgenomen verwerkingsbepalingen ex artikel 28, aanhef en derde lid, van de AVG. Er ontbreken verschillende verplicht gestelde onderdelen en er zijn verschillende onderdelen onvoldoende duidelijk opgeschreven.	3	Organisatorisch. Gebruik van generiek model verwerkersovereenkomst uit het privacyconvenant 4.0 voor overeenkomsten met schoolbesturen of aanpassing van de Algemene Voorwaarden. Als AFAS ervoor kiest om de Algemene Voorwaarden in lijn te brengen met de maatregelen vermeld in de risicotabel, kan er daarnaast een clausule worden opgenomen in de contractuele overeenkomst tussen AFAS en het schoolbestuur. Deze clausule bepaalt dat wijzigingen in de verwerking van persoonsgegevens of gerelateerde aspecten, zoals beschreven in artikel 28 van de AVG, alleen kunnen worden doorgevoerd na schriftelijke instemming van beide partijen, namelijk de	Laag indien wordt voldaan aan de bepalingen van artikel 28 AVG.	AFAS	1 april 2024

			verwerker en de verwerkingsverantwoordelijke. Hierdoor wordt eenzijdige aanpassing van de voorwaarden voorkomen en wordt de gezamenlijke naleving van de AVG gewaarborgd.				
1	Interne mailmogelijkheden zijn niet beveiligd door middel van encryptie.	3	Organisatorisch Mailmogelijkheid beperken tot algemene kennisgevingsboodschappen. Voorkom gebruik van bijzondere en gevoelige pgg in de mail. Gebruik hiervoor een alternatief beveiligd mailsysteem.	Laag, risico is gemitigeerd wanneer scholen geen gevoelige gegevens mailen via dit systeem.	Schoolbestuur	Technische aanpassing gaat voorlopig niet plaatsvinden door AFAS. Om die reden is het aan de schoolbesturen om te voorkomen dat er gevoelige gegevens zoals loonsgegevens worden verzonden over de mail.	Per direct
3	Onduidelijkheid gebruik van gegevens voor productverbetering	2	Organisatorisch Aanpassen bepaling in de AV, deze in overeenstemming	Laag tot midden afhankelijk	AFAS	AFAS heeft aangegeven dat er geen	1 april 2024

			brengen met de feitelijke situatie.	van de aanpassing		sprake is van herleidbare gegevens-verzameling t.b.v. verbetering van hun product. Daarom risico voorlopig op laag/midden	
4	Geen (automatische) toepassing van en/of controle op bewaartermijnen	2	Technisch. Implementeer een geautomatiseerd systeem voor het beheren en controleren van bewaartermijnen voor gegevens.	Laag tot midden afhankelijk van de aanpassing	AFAS en schoolbestuur	Technische ondersteuning versterkt de tijdige verwijdering van documenten echter dient het schoolbestuur hier ook een procedure voor te hebben ingericht.	1 april 2024
5	Onduidelijkheid over betekenis “ondersteuning”	2	Organisatorisch Tekst en betekenis ervan verhelderen of verwijderen.	Laag tot midden	AFAS		1 april 2024

branchemodellen in de algemene voorwaarden				

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 PIA-tool 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 in de terminologie van de DPIA's op Microsoft en Google van SURF SIVON en SLM Rijk (het ministerie van Justitie & Veiligheid). Het verbeterplan vermeldt – met een planning - de voorgenomen maatregelen om de risico's verder te mitigeren. 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.

Verbeterplan

Tijdens het DPIA-traject heeft AFAS zich gecommitteerd aan het aanpakken van de risico's die in de maatregelentabel zijn vermeld door de voorgestelde maatregelen op te volgen. In een verbeterplan worden afspraken vastgelegd met betrekking tot de naleving, uitwerking en concrete uitvoering van de door AFAS te nemen maatregelen zoals vermeld in de risicotabel. Alleen onder deze voorwaarden kunnen de oorspronkelijke (hoge) risico's worden verminderd tot een niveau van midden tot laag. Op basis van de gemaakte afspraken is het zeker dat AFAS de maatregelen gaat doorvoeren en hiermee de risico's binnen een redelijke termijn zullen zijn gemitigeerd. Over de feitelijke opvolging

en toepassing van de maatregelen zal kort na de hiervoor overeengekomen deadline van 1 april 2024 worden bericht op de website van SIVON.

7. Deel E: MODEL lokale DPIA

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

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

A. Uitvoering lokale DPIA

Binnen [NAAM ONDERWIJSINSTELLING] 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:

- [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 kanttekeningen […].

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 van AFAS 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 voor.		
8	Het bestuur voldoet aan het transparantieverplichting (artikel 13 en 14 AVG) en geeft de juiste informatie in de privacyverklaring over de toepassing van AFAS		
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 AFAS 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 AFAS		

14	De onderwijsinstelling neemt verantwoordelijkheid voor het veilig koppelen van het AFAS met een ander systeem zoals een leerlingadministratiesysteem.		
15	Kennis over applicatiebeheer is belegd bij één persoon en verder niet gedocumenteerd.		

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

Risico	**Te nemen maatregel**	**Uitgevoerd?**	**Opmerking/toelichting**
Er kan intern gemaild worden, maar niet beveiligd bijv. door encryptie met wachtwoord, beperkte beschikbaarheidstermijn of het niet kunnen doorsturen of downloaden.	Mailmogelijkheid beperken tot algemene kennisgevingsboodschappen. Voorkom gebruik van bijzondere en gevoelige persoonsgegevens in de mail. Gebruik hiervoor een alternatief beveiligd mailsysteem. Maak dit duidelijk en kenbaar voor de gebruikers van AFAS aan de hand van instructies/beleid of een andere regeling.		
Geen (automatische) toepassing van en/of controle op bewaartermijnen vanuit AFAS.	Omdat er (nog) geen sprake is van een automatische melding van gegevensverwerkingen die de bewaartermijn dreigen te overschrijden is het van belang om naast een duidelijk gegevensbewaarbeleid een geautomatiseerde herinneringen of waarschuwingen in te stellen om ervoor te zorgen dat gegevens binnen de vastgestelde termijnen worden		

	verwijderd of geanonimiseerd.		
De beoordeling van de noodzakelijkheid, proportionaliteit en subsidiariteit van het opnemen van persoonsgegevens in de applicatie, gebeurt door het schoolbestuur. Het schoolbestuur kan middels beleid rondom het gebruik van de applicatie waarborgen dat er alleen noodzakelijke gegevens worden verwerkt (en dat deze gegevens ook alleen worden verwerkt op manieren die noodzakelijk zijn). Gezien de grote vrijheid bij het invullen van gegevens in de applicatie, bijvoorbeeld de aanwezigheid van vrije invulvelden en de mogelijkheid van maatwerk van invulvelden in het algemeen, is het belangrijk dat schoolbesturen dit beleid ook opstellen en de naleving controleren.	Het maken van een eigen afweging door het schoolbestuur m.b.t. de noodzakelijkheid, proportionaliteit en subsidiariteit. Daarnaast een eigen gedragsregel maken en/of toevoegen in de gedragscode ICT en Internet m.b.t. het slechts gebruiken van persoonsgegevens die noodzakelijk zijn om te verwerken en het beperken van de teksten in de 'vrije tekstvelden'.		

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 ONDERWIJSINSTELLING] 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 ONDERWIJSINSTELLING] 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 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]					
Risico-afweging RESTRISICO	**kans**		**impact**		**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 ONDERWIJSINSTELLING]. [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, is 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/goed] mate zijn gemitigeerd.

Deze conclusie wordt anders als de in deze DPIA genoemde maatregelen door de het schoolbestuur [College van Bestuur] 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 dit DPIA vallen omdat zij niet in de invloedssfeer van (de leverancier van] [SYSTEEM] ligt, 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 [College van Bestuur], aangemerkt als verwerkingsverantwoordelijke voor [NAAM ONDERWIJSINSTELLING], 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 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: