CENTRALE DPIA

Visma.net HRM & Payroll

Versie 1.0 (januari 2025)

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	Stefan Ridder (jurist en adviseur IBP) Ferdy IJsselmuiden (DPIA-projectmanager) Pascal Marcelis (adviseur IBP) Marcel de Rijke (ISO) Hans-Peter Ligthart (portfoliomanager IBP)
Met dank aan Peple	Marjan de Haan (Product Development Director) Nico van der Reijden (HRM Development Manager) Rick van Egmond (IT & Compliance Officer)
Auteurs model DPIA (v.1.2)	Hans-Peter Ligthart (portfoliomanager IBP SIVON) Job Vos (jurist en adviseur IBP SIVON) Ferdy IJsselmuiden (DPIA-projectmanager)

Versie beheer

Datum	Versie	Wijziging
Januari t/m december 2024	1.0	Uitvoeren DPIA en opstellen DPIA rapport

Inhoudsopgave

1. Samenvatting 5

2. Introductie en achtergrond DPIA 7

I. DPIA 7

II. Verplichting DPIA 8

III. Toetsing rolverdeling verwerkingsverantwoordelijke en verwerker 8

IV. Centrale DPIA versus lokale DPIA 9

V. Gebruik model 10

VI. Scope van deze DPIA 11

VII. Buiten scope 11

VIII. Methodiek 11

IX. Definitie van verschillende gegevens 11

3. Deel A: Gegevensverwerkingsanalyse 15

1. Beschrijving van het gegevensverwerkende proces 15

2. Persoonsgegevens 15

3. Gegevensverwerkingen 18

4. Verwerkingsdoeleinden 19

5. Betrokken partijen 21

6. Belangen bij de gegevensverwerking 22

7. Verwerkingslocaties 22

8. Technieken en methoden van gegevensverwerking 23

10. Juridisch en beleidsmatig kader 25

11. Bewaartermijnen 26

4. Deel B: Beoordeling rechtmatigheid gegevensverwerkingen 29

12. Rechtsgrond 29

13. Bijzondere persoonsgegevens 31

14. Doelbinding 31

15 a. Noodzakelijkheid 32

15. b. Proportionaliteit en subsidiariteit 32

16. Rechten van de betrokkenen 32

17. Beoordeling verwerkersovereenkomst 34

5. Deel C: Beschrijving en beoordeling risico's voor de betrokkenen 35

18. Beoordelingskader risico's 35

19. Risico's 37

6. Deel D: Beschrijving voorgenomen maatregelen 41

20. Maatregelen 41

7. Deel E: MODEL lokale DPIA 44

A. Uitvoering lokale DPIA 44

B. Overwegingen over centrale DPIA 44

C. Organisatiespecifieke- en algemene applicatierisico's 44

D. Verklaring en advies functionaris voor gegevensbescherming (fg) 50

E. Visie betrokkenen 50

F. Conclusie 50

G. Risico-mitigerende maatregelen schoolbestuur 50

H. Verklaring schoolbestuur 51

1. Samenvatting

De DPIA heeft betrekking op Visma.net HRM & Payroll (voor het onderwijs) van de leverancier Peple.

Uitvoering van de DPIA

In een periode van ruim een jaar is de DPIA door SIVON uitgevoerd. Peple heeft op een constructieve en plezierige manier meegewerkt aan het uitvoeren van de DPIA. Peple heeft op een transparante wijze inzicht gegeven in de gegevensverwerkingen en de daarmee verbonden risico's.

Conclusie

Visma.net HRM & Payroll wordt door schoolbesturen ingezet voor personeelsadministratie, verzuimregistratie, en salarisverwerking. 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. Uit de DPIA is naar voren gekomen dat de onderwerpen privacy en informatiebeveiliging in Visma.net HRM & Payroll veel aandacht krijgen en hebben gekregen. Op het gebied van informatiebeveiliging zijn er in de DPIA geen grote risico's aangetroffen die nadere actie behoeven vanaf de kant van Peple, en slechts kleine risico's waarvoor scholen maatregelen moeten treffen.

Peple is niet aangesloten bij het Privacyconvenant en gebruikt een eigen verwerkersovereenkomst. Deze verwerkersovereenkomst is parallel aan het DPIA-traject gecontroleerd en getoetst aan de eisen van de AVG. Gedurende de uitvoering van de DPIA is de door Peple gebruikte verwerkersovereenkomst aangescherpt op een zodanige wijze, dat er een up-to-date en goede verwerkersovereenkomst beschikbaar is voor de onderwijsinstellingen. Een kwalitatief sterke verwerkersovereenkomst komt de duidelijkheid ten goede en helpt de onderwijsinstellingen om heldere afspraken te maken met de verwerker van haar persoonsgegevens. Deze nieuwe verwerkersovereenkomst moet wel eerst door de onderwijsinstelling geaccepteerd worden.

Met inachtneming van een aantal door de onderwijsinstelling uit te voeren (en te controleren) acties, kan er op een veilige manier gebruik worden gemaakt van Visma.net HRM & Payroll.

Naast de risico's als gevolg van het niet geaccepteerd zijn van de nieuwe verwerkersovereenkomst is nog een aantal risico's geïdentificeerd die door de onderwijsinstelling zelf moet worden gemitigeerd. Deze dienen te worden meegenomen in de lokale DPIA. Het betreft:

1. Het risico dat er door het gebruik van de export en/of download functie mogelijk gevoelige persoonsgegevens buiten de applicatie terecht komen;
2. Het risico dat er te veel gegevens worden verwerkt en dat er onvoldoende invulling wordt gegeven aan het beginsel van dataminimalisatie;

3. Het risico dat er - als er door de school gebruik wordt gemaakt van Visma.net HRM & Payroll in een uitbesteed proces (administratiekantoor) – geen goede afspraken zijn gemaakt over de gegevensverwerking in Visma.net HRM & Payroll (als subverwerker) met de verwerker (het administratiekantoor);
4. Het risico dat er te veel gegevens worden uitgewisseld met derde partijen;
5. Het risico dat er bij accounts (met veel rechten) onregelmatigheden plaatsvinden doordat de toegang tot de applicatie onvoldoende is beveiligd omdat 2fa wordt uitgeschakeld;
6. Het risico dat gegevens te lang worden bewaard.
7. Het risico dat de school de autorisaties niet goed beheerd.

2. Introductie en achtergrond DPIA

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. Een onderdeel daarvan is het gebruik van veilige en verantwoorde ICT-middelen. Een Data Protection Impact Assessment (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 Assessment (DPIA). In de AVG wordt dit een gegevensbeschermingseffectbeoordeling (GEB) genoemd. Een DPIA wordt uitgevoerd op een applicatie of verwerking van persoonsgegevens door een leverancier (verwerker). De DPIA wordt uitgevoerd conform de eisen van artikel 35 lid 7 AVG. 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. Alleen indien de hoge risico's voldoende worden beheerst door mitigerende maatregelen, is een gegevensverwerking toegestaan.

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 de gehele onderwijssector zogenaamde **centrale DPIA's** uit. Deze DPIA worden door SIVON 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. Door samen op

te trekken staan schoolbesturen 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-schoolbesturen op weg om veilig en verantwoord gebruik te maken van persoonsgegevens en ICT.

Schoolbesturen moeten volgens de AVG zelf afwegen wat de risico's zijn voor de rechten en vrijheden van betrokkenen. Dat kan SIVON niet doen. Na de uitvoering van de centrale DPIA moeten daarom ieder schoolbestuur de uitkomsten uit de centrale DPIA op hun organisatie toepassen. 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 schoolbesturen 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 privacy toezichthouder Autoriteit Persoonsgegevens die een lijst gepubliceerd heeft bij welke verwerkingen het uitvoeren van aan DPIA verplicht is[1]. Het schoolbestuur voert door middel van een DPIA voorafgaand aan de verwerking van persoonsgegevens een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.

Het uitvoeren van een DPIA op het personeel administratiesysteem Visma.net HRM & Payroll is 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 de verbetering 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

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

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 persoonsgegevens 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 systeemniveau. Een centrale DPIA toetst of én wat de impact is van het gebruik (verwerking) van het systeem in relatie tot de bescherming van persoonsgegevens. Hoe kan het systeem veilig gebruikt worden en welke (extra) maatregelen en instellingen zijn daarvoor nodig?

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, een complete inventarisatie van de te verwerken persoonsgegevens, de verwerkingsdoeleinden en werking van het systeem,
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 (beveiligings)maatregelen 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 het systeem of dit voldoet aan de gemaakte afspraken;
3. Het maken van afspraken over maatregelen die nog niet zijn genomen maar op grond van de DPIA wel nodig zijn;
4. Een correcte implementatie van het systeem binnen 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 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 persoonsgegevens en 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 het systeem en aangevuld met een model lokale DPIA.

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.

[2] rapportagemodel-dpia-rijksdienst-v2-0-aangepast-cf-toegangscontrole.docx (live.com)
[3] https://aanpakibp.kennisnet.nl/app/uploads/Handreiking-DPIA-v1.0-1.pdf

VI. Scope van deze DPIA

De DPIA heeft betrekking op Visma.net HRM & Payroll (voor het onderwijs) van de leverancier Peple.

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 richt zich 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 Visma.net HRM & Payroll.

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.

Peple is bezig met een HRM Analytics applicatie (reporting oplossing), waarbij data uit het HRM product en het Payroll product samen wordt gevoegd voor rapportage doeleinden. Gelet op de fase waarin de ontwikkeling zich bevindt, is deze toepassing buiten scope.

VIII. Methodiek

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

- Beoordeling van de verwerkingen, (verwerkers)overeenkomsten, de te verwerken persoonsgegevens in relatie tot het doel, de rechtmatigheid, alsmede in hoeverre de verwerking van de persoonsgegevens voldoet aan de beginselen van de AVG, de risico's en de maatregelen;
- Beoordeling van de BIV-kwalificatie aan de hand van het ROSA certificeringsschema;
- 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 de wijze waarop het systeem voorziet in logging en de wijze waarop dit door de onderwijsinstelling gemonitord kan worden;
- Uitvoeren van test-script gevolgd door inzage verzoek bij leverancier;
- Opstellen rapportage;
- Overleg met leverancier over (aanvullende) maatregelen.

De centrale DPIA is uitgevoerd in de periode januari – december 2024 door het in de colofon genoemde DPIA-team.

IX. Definitie van verschillende gegevens

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.

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 servicegegevens genoemd.]

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[4] zwaardere eisen gesteld aan de beveiliging van de gegevens.

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

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.

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

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 persoon identificerende 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[5].

Privacyconvenant Onderwijs
Het Convenant digitale onderwijsmiddelen en privacy vertaalt de AVG naar de onderwijspraktijk. Het bevat afspraken over het omgaan met persoonsgegevens bij het gebruik van digitale leermiddelen en toetsen. Dankzij het convenant weten scholen en aanbieders wat ze over en weer van elkaar mogen verwachten, zijn de afspraken werkbaar in de praktijk en heeft iedereen dezelfde gemeenschappelijke uitleg bij deze afspraken. Het Convenant Digitale Onderwijsmiddelen en Privacy 4.0 en de bijbehorende documenten, zoals de Model Verwerkersovereenkomst en het Reglement, zijn terug te vinden op www.privacyconvenant.nl.

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

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

Visma.net HRM & Payroll wordt door schoolbesturen ingezet voor personeelsadministratie, verzuimregistratie, salarisverwerking en financiële administratie. 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.

2. Persoonsgegevens

In dit onderdeel wordt beschreven welke categorieën persoonsgegevens van welke betrokkenen worden verwerkt binnen het systeem.

De betrokkenen wiens persoonsgegevens worden verwerkt in Visma.net HRM & Payroll zijn onderverdeeld in de volgende categorieën:

- Werknemers, oud-werknemers en zelfstandigen;
- Stagiaires;
- Sollicitanten;
- Partner/kinderen van (oud)-werknemers;
- Noodcontactpersoon van (oud)-werknemers/stagiaires;
- Vrijwilligers;
- Werknemers (als gebruikers van het systeem).

Persoonsgegevens

De verwerkte persoonsgegevens per categorie betrokkenen, de categorieën persoonsgegevens en op hoofdlijnen de bron van de persoonsgegevens worden hieronder weergegeven:

Categorie betrokkene	**Categorie persoons gegevens**	**Persoonsgegeven** **(De aanduiding (N) of (H) staat voor de risicoclassificering Normaal (N) of Hoog (H). Rubricering door Peple).**	**Bron/verkrijging persoonsgegeven**
Werknemers, oud-werknemers en zelfstandigen	• Gewoon • Bijzonder • Gevoelig • Wettelijk identificatie-nummer	• Naam-, adres- en woonplaatsgegevens (N) • Opleidingsgegevens (N) • Burgerservicenummer (H) • Bezettings- en formatie informatie (N)	• Werknemer • Werkgever

		• Contactgegevens (o.a. telefoonnummers en e-mailadressen) (N) • Belonings-, uitkerings- en/of pensioengegevens en mutaties (N) • Kopieën van legitimatiebewijzen (H) • Verlofgegevens (N) • Toegangs- of identificatiegegevens (H) • Verzuimgegevens (H) • Bankrekeningnr. en financiële gegevens (N) • Functioneringsgegevens (N) • Aanstellings-/contract gegevens (N) • Uitstroommutaties / uitdienstdata (N) • Arbeidsverleden (N) • Geboortedatum (N) • Geboorteplaats (N) • Pasfoto (H) • Burgerlijke staat (N) • Nationaliteit (N) • Geslacht (N) • VOG (H) • Personeelsnummer (H) • Functietitel/-beschrijving (N) • Overige informatie met betrekking tot de arbeidsrelatie (H) • AOW-datum (N) • Overige gegevens (vrije invulvelden) (N/H)	
Stagiaires	• Gewoon • Bijzonder • Gevoelig • Wettelijk identificatie-nummer	• Naam-, adres- en woonplaatsgegevens (N) • Opleidingsgegevens (N) • Burgerservicenummer (H) • Bezettings- en formatie informatie (N) • Contactgegevens (o.a. telefoonnummers en e-mailadressen) (N) • Belonings-, uitkerings- en/of pensioengegevens en mutaties (N)	• Stagiaire • Werkgever

		• Kopieën van legitimatiebewijzen (H) • Verlofgegevens (N) • Toegangs- of identificatiegegevens (H) • Verzuimgegevens (H) • Bankrekeningnr. en financiële gegevens (N) • Functioneringsgegevens (N) • Aanstellings-/contract gegevens (N) • Uitstroommutaties / uitdienstdata (N) • Arbeidsverleden (N) • Geboortedatum (N) • Geboorteplaats N) • Pasfoto (H) • Burgerlijke staat (N) • Nationaliteit (N) • Geslacht (N) • VOG (H) • Personeelsnummer (H) • Functietitel/-beschrijving (N) • Overige informatie met betrekking tot de arbeidsrelatie (H) • AOW-datum (N) • Overige gegevens (vrije invulvelden) (N/H)	
Sollicitanten	• Gewoon • Bijzonder	• Naam-, adres- en woonplaatsgegevens (N) • Contactgegevens (o.a. telefoonnummers en e-mailadressen) (N) • Geboortedatum (N) • Geboorteplaats (N) • Pasfoto (H) • Burgerlijke staat (N) • Nationaliteit (N) • Geslacht (N) • VOG (H) • CV / motivatiebrief (H) • Salarisindicatie (H) • Overige gegevens (vrije invulvelden) (N/H)	• Sollicitant

Partner/kinderen van (oud)-werknemers	• Gewoon • Bijzonder (in potentie als de relatie iets zegt over de seksuele voorkeur van de betrokkene)	• Naam-, adres- en woonplaatsgegevens (N) • Contactgegevens (o.a. telefoonnummers en e-mailadressen) (N) • Geslacht (N) • Geboortedatum (N) • Burgerlijke staat (N) • Relatie tot werknemer (H)	• Werknemer
Noodcontactpersoon van (oud)-werknemers /stagiaires	• Gewoon • Bijzonder (in potentie als de relatie iets zegt over de seksuele voorkeur van de betrokkene)	• Naam-, adres- en woonplaatsgegevens (N) • Contactgegevens (o.a. telefoonnummers en e-mailadressen) (N) • Geslacht (N) • Relatie tot werknemer (H)	• Werknemer
Vrijwilligers	• Gewoon	• Naam-, adres- en woonplaatsgegevens (N) • Contactgegevens (o.a. telefoonnummers en e-mailadressen) (N)	• Vrijwilliger • Werkgever
Werknemers (als gebruikers van het systeem)	• Gewoon	• Accountgegevens (N) • 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 het systeem 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 Visma.net HRM & Payroll. 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

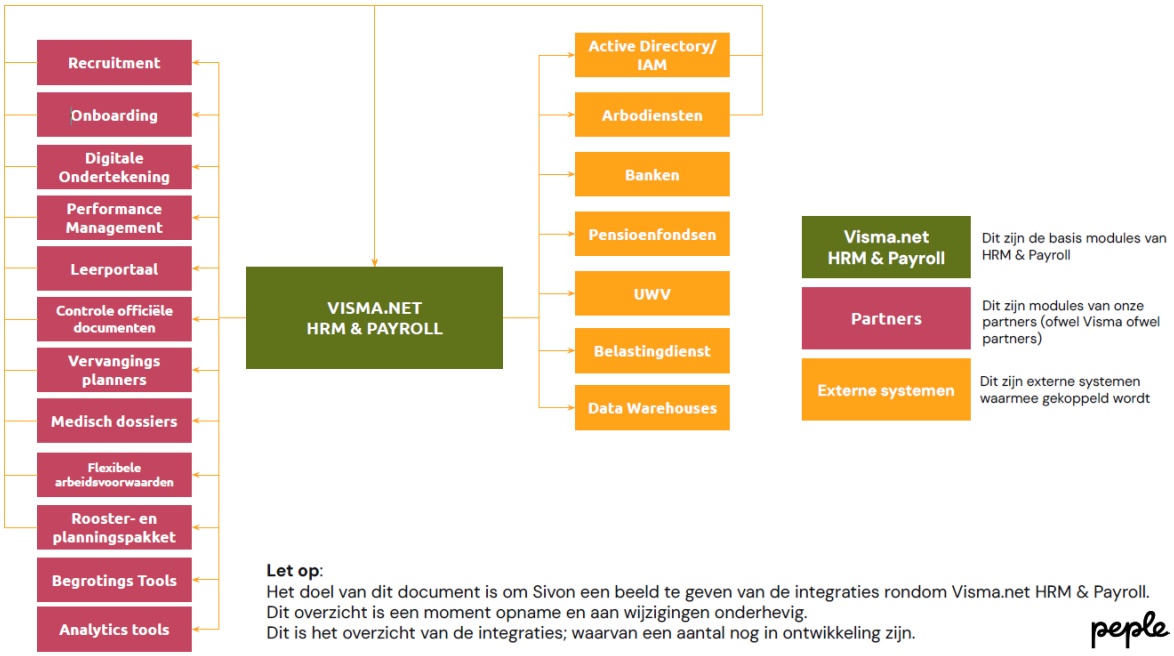
In het geval van de wettelijke koppelvlakken zoals belasting, UWV, Pensioen, Arbodienst (SIVI-koppelvlak) en DUO liggen de over te dragen gegevens vast per koppelvlakvereiste. Deze specifieke koppelvlakken worden door Visma.net HRM & Payroll aangestuurd.

Bij niet-juridische interfaces zijn de uit te wisselen gegevens afhankelijk van de aanvrager en wordt dit door de klant zelf aangestuurd (al dan niet met hulp van Visma.net HRM & Payroll consultants). In deze interfaces kan privacy-informatie verstuurd worden en moeten de onderwijsinstellingen een verwerkersovereenkomst hebben.

De gebruiker die deze koppelingen configureert moet de juiste autorisatie hebben en moet iemand zijn in de rol van Applicatie- / Functioneel Beheerder. Deze moet op ook de hoogte zijn van de wettelijke eisen en beperkingen.

Gegevensstromen/stroomschema

Omdat de gegevensverwerkingen gecompliceerd kunnen zijn en het niet altijd gemakkelijk is om het geheel van gegevensverwerkingen in woorden uit te drukken zijn de gegevensverwerkingen gevisualiseerd in onderstaand model.



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).

Gegevensverwerking	Doeleinde verwerking

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

(par.3 Gegevensverwerkingen)	(par.4. Verwerkingsdoeleinden)
Beheer personeelsgegevens	Opslaan, wijzigen, raadplegen, gebruiken, verwijderen gegevens van alle betrokkenen (werknemers/ zelfstandigen/ vrijwilligers/ oud-werknemers /stagiaires/ sollicitanten/ partner/ kinderen/ noodcontactpersoon)
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/ vrijwilligers)
Instroom personeel	Opslaan, wijzigen, raadplegen, gebruiken, verwijderen gegevens met betrekking tot sollicitaties (sollicitanten/ werknemers/ oud-werknemers/ zelfstandigen/ vrijwilligers/ 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)
Uitstroom personeel	Opslaan, wijzigen, raadplegen, gebruiken, verwijderen gegevens met betrekking tot arbeidsrelatie (werknemers/ oud-werknemers/ zelfstandigen/ vrijwilligers/ stagiaires)
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/ zelfstandigen/ stagiaires)
Salarisverwerking	Opslaan, wijzigen, raadplegen, gebruiken, verwijderen salarisgegevens, gegevens met betrekking tot arbeidsrelatie en bankrekeningnummer (werknemers/ oud-werknemers/ zelfstandigen/ stagiaires)

5. Betrokken partijen

De volgende partijen spelen een rol bij de verwerking van de persoonsgegevens in Visma.net HRM & Payroll en hebben toegang tot de persoonsgegevens.

In de verwerkersovereenkomst staat dat Peple andere in de EU/EER gevestigde bedrijven van de Visma-groep als subverwerker kan inschakelen zonder dat het Visma-bedrijf is vermeld en zonder voorafgaande goedkeuring of kennisgeving aan de Onderwijsinstelling. Dit gebeurt gewoonlijk met het oog op ontwikkeling, ondersteuning, activiteiten enz. Peple communiceert in deze gevallen wel over eventuele nieuwe subverwerkers, en de klant krijgt 30 dagen om bezwaar te maken.

Naam partij	AVG-rol	Functie/taak	Betrokken persoons gegevens	Verstrekker of ontvanger	De volgende personen/rollen hebben toegang deze pgg
Onderwijsinstelling (schoolbestuur)	Verwerkingsverantwoordelijke	Voert als werkgever personeels- en salarisadministratie uit	Gewoon, Bijzonder	Verstrekker en ontvanger	Geautoriseerde medewerkers van de onderwijsinstelling
Peple	Verwerker	Verwerkt persoonsgegevens in opdracht van de verwerkingsverantwoordelijke	Gewoon, Bijzonder	Ontvanger	Beheerder, Support medewerkers, consultants
Werknemer	Betrokkene	Kennisnemen, aanpassen gegevens en indienen declaraties	Gewoon, Bijzonder	Verstrekker en ontvanger	Eigen persoonsgegevens
Amazon Web Services	Subverwerker (verplicht)	Hosting en opslag Visma.Net systemen	Gewoon, Bijzonder	Ontvanger	Overeenkomstig de subverwerkersovereenkomst
Visma ITC	Subverwerker (verplicht)	Hosting en opslag Visma.Net systemen	Gewoon, Bijzonder	Ontvanger	Overeenkomstig de subverwerkersovereenkomst
Orca Security Ltd.	Subverwerker (verplicht)	Identificeert problemen met public cloudbeveiliging	Gewoon	Ontvanger	Overeenkomstig de subverwerk

					ersovereenkomst
Datadog	Subverwerker (verplicht)	Logging van resources en events	Gewoon	Ontvanger	Overeenkomstig de subverwerkersovereenkomst
Xurrent	Subverwerker (verplicht)	Ticketsysteem klanten	Gewoon	Ontvanger	Overeenkomstig de subverwerkersovereenkomst
Atlassian	Subverwerker (verplicht)	Ticketsysteem ontwikkelaars	Gewoon	Ontvanger	Overeenkomstig de subverwerkersovereenkomst
Hubspot	Subverwerker (verplicht)	CRM	Gewoon	Ontvanger	Overeenkomstig de subverwerkersovereenkomst
Visma Software AS	Subverwerker (verplicht)	Login portaal voor toegang tot software.	Gewoon	Ontvanger	Overeenkomstig de subverwerkersovereenkomst

Voor optionele verwerkingen zijn er tal van subverwerkers. Deze zijn gerelateerd aan de afgenomen diensten. Zie hiervoor ook de verwerkersovereenkomst.

Een actuele lijst met subverwerkers is daarnaast beschikbaar in het Visma Trust Centre en raadpleegbaar via: https://www.visma.com/trust-centre/product-search/

Een actueel overzicht inclusief salarisdienstverleners is beschikbaar op https://www.peple.nl/

6. Belangen bij de gegevensverwerking

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

Het inschakelen van een hostingpartij dient het bedrijfsbelang van Visma.net HRM & Payroll om betrouwbare opslag en beschikbaarheid van de gegevens te kunnen bieden.

7. Verwerkingslocaties

De persoonsgegevens die door de scholen in Visma.net HRM & Payroll worden geregistreerd, worden opgeslagen op servers van AWS en Visma. Visma gebruikt uitsluitend datacenters die zich binnen de EU/EER 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 Visma of Peple toegang hebben tot persoonsgegevens van het schoolbestuur, bijvoorbeeld voor ondersteuning op afstand, gebeurt dat binnen de EU.

Partijnaam	Statutaire vestigings-plaats (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
Amazon Web Services	US	Hosting en opslag Visma.Net systemen	EU/EER Doorgifte mechanisme: SCC
Visma ITC	EU	Hosting en opslag Visma.Net systemen	EU/EER
Orca Security Ltd.	Israël	Identificeert problemen met public cloudbeveiliging	EU/EER Doorgifte mechanisme: adequaatheidsbesluit en DPIA
Datadog	US	Logging van resources en events	EU/EER Doorgifte mechanisme: SCC
Xurrent	US	Ticketsysteem klanten	EU/EER Doorgifte mechanisme: SCC
Atlassian	AU	Ticketsysteem ontwikkelaars	EU/EER Doorgifte mechanisme: SCC
Hubspot	US	CRM	EU/EER Doorgifte mechanisme: SCC
Visma Software AS	EU/EER	Login portaal voor toegang tot software.	EU/EER

Voor optionele verwerkingen zijn er tal van subverwerkers. Deze zijn gerelateerd aan de afgenomen diensten. Zie hiervoor ook de verwerkersovereenkomst.

8. Technieken en methoden van gegevensverwerking

De applicatie Visma.net HRM & Payroll is een SaaS-applicatie. Dit houdt in dat Visma.net HRM & Payroll een op de cloud gebaseerd softwareleveringsmodel is waarin de aanbieder (Peple) cloudapplicatiesoftware ontwikkelt, onderhoudt en automatische software updates levert.

HRM en Payroll zijn verschillende onderdelen maar worden altijd in combinatie gebruikt. HRM bestaat uit zo'n 20 verschillende modules die naar gelang de behoefte van een onderwijsinstelling kunnen worden gebruikt.

Status van informatiebeveiliging

In Q1 2024 heeft een globaal onderzoek plaatsgevonden naar de status van informatiebeveiliging van de applicatie Visma.net HRM & Payroll. Dit onderzoek is gebaseerd op informatie welke door Peple is verstrekt. Omdat Peple het Privacy convenant niet heeft ondertekend is geen check op naleving van het ROSA uitgevoerd. Er is geen technisch onderzoek uitgevoerd naar het implementatieniveau van beveiliging.

Uit dit onderzoek is de volgende informatie verkregen:

- Visma.net HRM & Payroll is ISO27001 gecertificeerd sinds 2016, ISO9001 en ISAE3402. Visma.net HRM & Payroll valt in scope van het ISO27001 certificaat;
- In de VVT zijn alle vereisten relevant verklaard;
- Periodiek wordt de omgeving van Visma.net HRM & Payroll aan een pentest en security scan onderworpen. De meest recente pentest is van januari 2025. Alle constateringen worden in een ticket systeem opgeslagen en gemonitord;
- Peple (Visma) heeft een zeer professioneel risicomanagement methode.

Aanbevelingen

Uit het onderzoek volgen geen aanbevelingen.

2FA

Visma.net HRM & Payroll is standaard toegankelijk via User & Password en 2FA. SSO wordt ondersteund met SAML2. 2FA staat standaard aan. Het is mogelijk door de werkgever om dit uit te schakelen; er wordt echter via het systeem gewaarschuwd dat dit gevolgen kan hebben. Peple zal in 2025 wel onderzoeken of 2FA niet verplicht gemaakt kan worden.

Overige technische bevindingen

Bij de cookies op https://connect.visma.com/ is de default optie 'alle cookies accepteren'. En op het moment dat je op 'cookie instellingen' klikt zie je eigenlijk alleen weer 'alle toestaan'. De knop om de voorkeuren aan te geven is wat verborgen. Beter zou zijn de privacy by default optie 'noodzakelijke cookies accepteren' te laten zijn.

Logging

Er wordt op meerdere vlakken gelogd door Visma.net HRM & Payroll. Het betreft logging in het proces zelf en zichtbaar voor de gebruiker (bijvoorbeeld het uitvoeren van een taak). Er zijn ook overzichten die de mutaties tonen, wat er is gewijzigd en door wie (bijvoorbeeld bij salarisschaal of contract, arbeidsvoorwaarden etc.). Deze logging is te raadplegen door een geautoriseerde gebruiker. Het verwijderen van een werknemer, inzien van documenten, bewegingen in de applicatie etc. wordt ook gelogd, maar is niet direct bereikbaar voor de onderwijsinstelling (alleen op verzoek).

IAMA: mensenrechten in beeld bij algoritmes.

Visma.net HRM & Payroll maakt alleen gebruik van algoritmes bij berekeningen van salarissen en t.b.v. overboekingen naar de belastingdienst.

Er wordt ook gebruikgemaakt van machine learning bij de declaratiemodule. De werknemer kan daarvoor kiezen. Hierbij wordt d.m.v. objectherkenning uit de aangeboden declaratie de datum, bedrag en btw gehaald en vult het systeem dit voor de gebruiker in (SmartScan van Visma). Verdere verwerking vindt er niet plaats. Feitelijk kan iedere declaratie worden aangeboden door de werknemer, met of zonder gevoelige informatie. De techniek negeert deze informatie. Wel wordt de geüploade declaratie door de werknemer in de database van Visma.net HRM & Payroll opgeslagen.

Gelet op de aard van deze (technische) toepassingen is er verder geen nader onderzoek gedaan naar algoritmes, AI en mensenrechten.

10. 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

11. Bewaartermijnen

Per schoolbestuur dienen de bewaartermijnen voor een type dossieritem vastgelegd te worden. Daarbij dienen de wettelijke bewaartermijnen ook in acht genomen te worden[7].

Bewaartermijnen zijn standaard geconfigureerd in Visma.net HRM & Payroll. De Onderwijsinstelling kan hiervan afwijken, behalve voor de gegevens die een wettelijke bewaartermijn van 7 jaar kennen.

Er zijn geen technische en geautomatiseerde verwijderingsprocessen geïmplementeerd. Visma.net HRM & Payroll verwijdert alleen gegevens van werknemers die geen contract hebben.

De Onderwijsinstelling kan een rapport uitvoeren. In dit rapport worden de werknemers en de gegevens die worden verwijderd getoond. Die gegevens worden alleen verwijderd als de Onderwijsinstelling dit bevestigt.

Categorie betrokkene	Persoonsgegevens	Bewaartermijnen
Werknemers, oud-werknemers	Gegevens betreffende een werknemer, vereist voor de Uitvoeringsregeling loonbelasting.[8] 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, met uitzondering van de gegevens die noodzakelijk zijn om te voldoen aan de 7 jaar loonaangifte eis van de belastingdienst.
Werknemers, oud-werknemers	Gegevens betreffende een werknemer, verwerkt in het kader van de Wet verbetering poortwachter. [9]	2 jaar na uitdiensttreding en 5 jaar na uitdiensttreding voor WIA en eigen risicodragers.
Werknemers, oud-werknemers	Salarisadministratie inclusief afspraken betreffende salaris en arbeidsvoorwaarden.[10]	7 jaar na uitdiensttreding.

[7] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering/personeelsdossiers#hoe-langmag-ik-als-werkgever-de-gegevens-in-een-personeelsdossier-bewaren-8618
[8] Art. 7.9 Uitvoeringsregeling loonbelasting
[9] Wet verbetering poortwachter.
[10] Art. 52 Algemene wet inzake rijksbelastingen.

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, met uitzondering van die gegevens waarbij 7 jaar geldt in verband met de vereiste van de loonaangifte belastingdienst.
Werknemers, oud-werknemers	Verslagen in het kader van de Wet verbetering poortwachter	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 • Verslagen over functioneringsgesprekken • Alle overige informatie	Maximaal 2 jaar na uitdiensttreding.
Stagiaires	Alle gegevens	Maximaal 6 maanden na einde stage.
Sollicitanten	Alle gegevens	4 weken of 1 jaar (bij verkrijging toestemming)
Partner/kinderen van (oud)-werknemers	Alle gegevens	Maximaal 2 jaar na uitdiensttreding, met uitzondering van gegevens partner waarbij 7 jaar geldt in verband met de vereiste van de loonaangifte belastingdienst.
Noodcontactpersoon van (oud)-werknemers/stagiaires	Alle gegevens	Maximaal 6 maanden na uitdiensttreding.
Vrijwilligers	Alle gegevens	Maximaal 6 maanden na einde werkzaamheden.
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.

Klant data	•	6 maanden na beëindiging overeenkomst. Export beschikbaar voor klant.

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[11]
d) Vitaal belang van de betrokkene
e) Taak van algemeen belang[12] (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	Toestemming in geval CV langer dan 4 weken in portefeuille blijft.

[11] 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.
[12] 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.

	Artikel 6, eerste lid, sub a en f, AVG.	Gerechtvaardigd belang t.a.v. werving i.h.k.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

Onderbouwing gerechtvaardigd belang (indien van toepassing)

Bij het beoordelen van de rechtmatigheid van gegevensverwerking op basis van het gerechtvaardigd belang dient dit belang te worden onderbouwd.

Voorwaarden voor gerechtvaardigd belang	Beschrijving
Beoordeel of er een gerechtvaardigd belang achter de verwerking zit en of de verwerking noodzakelijk is voor het doel dat u hebt geïdentificeerd.	Een werkgever heeft er belang bij – en is daartoe vanuit goed werkgeverschap zelfs toe gehouden – om een zorgvuldig personeelsbeleid en –beheer te voeren. Voor het (veilig) uitvoeren van de gebruikelijke HR processen, zoals werving & selectie, competentiemanagement, planning, opleiden & ontwikkelen, beoordelen etc. moet een werkgever persoonsgegevens verwerken.
Beoordeel de impact op de belangen en rechten en vrijheden van de betrokkene	De verwerking van de persoonsgegevens maakt geen noemenswaardige impact op de rechten en vrijheden van betrokkene. De verwerking vindt plaats in een professioneel en veilig personeelsinformatiesysteem.

Beoordeel of de verwerking in overeenstemming is met de redelijke verwachtingen van de betrokkene.	Het grootste gedeelte van de gegevens komt tot stand in de samenwerking tussen werkgever en betrokkene (de medewerker). De medewerkers verwacht dat de werkgever deze verwerkt en gaat er daarbij vanuit dat de verwerking binnen een veilige professionele omgeving plaatsheeft.

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

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

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.

De Onderwijsinstelling is de eigenaar van de gegevens en Visma.net HRM & Payroll ondersteunt de Onderwijsinstelling om te voldoen aan de rechten van betrokkenen. Er zijn meerdere rapporten beschikbaar die helpen om de opgeslagen gegevens te rapporteren en op verzoek te delen met de werknemer of de Onderwijsinstelling kan zijn eigen rapporten maken. Er is een rapport optie beschikbaar om een rapport te maken van alle gegevens die over een werknemer zijn vastgelegd, inclusief historische gegevens (totaaloverzicht werknemer gegevens).

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 desgevraagd nadere toelichting kan geven over de gegevensverwerking. Informatie over de gegevensverwerking gaat buiten de applicatie om.	n.v.t.
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.	n.v.t.
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	n.v.t.

	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 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.*

17. Beoordeling verwerkersovereenkomst

Peple is geen deelnemer of medestander van het Convenant digitale onderwijsmiddelen en privacy 4.0 (ook wel: Privacyconvenant Onderwijs, hierna: Convenant). Voor leveranciers die geen deelnemer of medestander zijn, 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.

Uit de verwerkersovereenkomst volgen geen risico's. De door SIVON gesignaleerde punten zijn tijdens het DPIA proces opgelost en de laatste versie van de verwerkersovereenkomst voldoet aan de eisen die de AVG daaraan stelt.

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.

18. 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.
Negatieve gevolgen van de gegevensverwerking zijn bijvoorbeeld:

- 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).

De methodiek die wordt gevolgd, is beschreven door de Britse toezichthouder[13] 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:

[13] 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

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.

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 Kleine kans	Kans = gebeurtenis kan zich voordoen; meerdere malen per schooljaar Een redelijke kans	Kans = deze gebeurtenis zal zich bijna zeker voordoen; per maand, week of zelfs dag De kans dat het zich voordoet is groter, dan de kans dat het niet gebeurt

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

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 Visma.net HRM & Payroll 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:

- **M**ens – de mensen die nodig zijn om het informatiesysteem te beheren en gebruiken, denk aan: directe en indirecte gebruikers, en functioneel en technisch applicatiebeheer.
- **A**pparatuur – de apparatuur die nodig is om het informatiesysteem te laten functioneren, denk aan: webserver, applicatieserver, beheer van werkplekken en werkplekken van gebruikers.
- **P**rogrammatuur – de programmatuur waaruit het informatiesysteem bestaat, denk aan: de diverse applicaties die gebruikt worden.
- **G**egevens – de gegevens die door het systeem worden verwerkt, denk aan: basisregistraties, financiële verantwoording en vergunningen.
- **O**rganisatie – de organisatie die nodig is om het informatiesysteem te laten functioneren, denk aan: beheer-, gebruikers- en ontwikkelorganisatie.
- **O**mgeving – de omgeving waarbinnen het informatiesysteem functioneert, denk aan: locatie, serverruimte en werkplekken.
- **D**iensten – de externe diensten die nodig zijn om het systeem te laten functioneren, denk aan: technisch systeembeheer, netwerkinfrastructuur en onderhoudscontracten met externe dienstverleners.

Risicotabel:

Risico nr.	Mapgood	Risico-omschrijving	Oorzaak / toelichting	Kans	Impact	Risico	Proces en/of systeem-risico?
1	O	Het risico is dat er door het gebruik van de export en/of download functie mogelijk gevoelige persoonsgegevens buiten de applicatie terecht komen wat verlies van controle over deze data tot gevolg heeft.	Het maken van exports en downloads is een ongecontroleerd proces. Het is mogelijk dat onbevoegde gebruikers toegang krijgen tot persoonsgegevens en dat persoonsgegevens op allerlei plekken worden bewaard en niet tijdig worden vernietigd.	2	3	6	Proces (school)
2	O	Het risico is dat de verwerkingsverantwoordelijke geen toereikende afspraken met de verwerker heeft gemaakt over de verwerking van de persoonsgegevens.	De verwerkersovereenkomst voldoet niet aan alle eisen (Zie uitwerking paragraaf 18). Als er geen goede afspraken met de verwerker zijn gemaakt kan dat tot gevolg hebben dat de verwerking niet aan de vereisten van de AVG voldoet en dat de bescherming van de rechten van betrokkenen daardoor onvoldoende is gewaarborgd.	2	2	4	Proces (Peple en school)
3	O	Het risico is dat er teveel gegevens worden verwerkt en dat er onvoldoende invulling wordt gegeven aan het	Tijdens de inrichting (of daarna door de functioneel beheerder) zijn er teveel tekstvelden aangemaakt waardoor de mogelijkheid bestaat dat er teveel	2	3	6	Proces (school)

		beginsel van dataminimalisatie.	(onnodige) gegevens worden verwerkt (bijv. BSN partner). De onderwijsinstelling moet beleid hebben om te zorgen dat vrije invulvelden niet worden gevuld met informatie die niet strikt noodzakelijk is voor de vastgestelde doelen				
4	O	Het risico dat er - als er door de school gebruik wordt gemaakt van Visma.net HRM & Payroll in een uitbesteed proces (administratiekantoor) – geen goede afspraken zijn gemaakt over de gegevensverwerking in Visma.net HRM & Payroll (als subverwerker) met de verwerker (het administratiekantoor).	In de situatie dat de personeelsadministratie en/of salarisverwerking is uitbesteed aan een administratiekantoor (verwerker) kan het zijn dat VISMA.net HRM & Payroll subverwerker is. In dat geval moeten met de verwerker goede afspraken worden gemaakt over de verwerking van de medewerker gegevens bij de subverwerker. Belangrijke vraag daarbij is of alle klanten binnen 1 tenant staan of dat je als onderwijsinstelling een eigen tenant hebt.	3	3	9	Proces (school)
5	O	Het risico is dat er teveel gegevens worden uitgewisseld met derde partijen.	• Bij niet-juridische interfaces zijn de uit te wisselen gegevens afhankelijk van de aanvrager en wordt dit door de Onderwijsinstelling zelf aangestuurd (al dan niet met hulp van Visma.net HRM & Payroll consultants). In deze interfaces kan privacy-informatie verstuurd worden en moeten de onderwijsinstellingen een verwerkersovereenkomst hebben.	2	3	6	Proces (school)

			• De gebruiker die deze koppelingen configureert moet de juiste autorisatie hebben en moet iemand zijn in de rol van Applicatie- / Functioneel Beheerder. Deze moet op ook de hoogte zijn van de wettelijke eisen en beperkingen.				
6	O	Het risico is dat medewerkers over teveel rechten beschikken.	• Rollen en rechten zijn default ingericht. Hier kan de school zelf van afwijken. • Indien de werknemer de juiste autorisaties heeft kan hij/zij BSN autorisaties aanpassen. • De superuser van de school kan ook zelf andere superusers toevoegen.	2	3	6	Proces (school)
7	O	Het risico is dat er bij accounts (met veel rechten) onregelmatigheden plaatsvinden doordat de toegang tot de applicatie onvoldoende is beveiligd omdat 2fa wordt uitgeschakeld.	2FA staat standaard aan. Het is mogelijk door de werkgever om dit uit te schakelen; er wordt echter via het systeem gewaarschuwd dat dit gevolgen kan hebben	3	3	9	Proces (school)
8	O	Het risico is dat gegevens te lang worden bewaard.	Standaard zijn bewaartermijnen ingesteld. Gegevens moeten wel periodiek door de onderwijsinstelling worden verwijderd.	2	3	6	Proces (school)

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. 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.

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.

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:

Risico nr.	Omschrijving risico (steekwoord)	Risico	Maatregel(en) (Org/Techn/Jur)	Maatregel voor (naam applicatie/school)	Restrisico (cijfer)	Toelichting aanvaardbaarheid restrisico	(datum)maatregel geïmplementeerd?
1	Export en download van medewerkergegevens	6	Onderwijsinstelling maakt afspraken over het gebruiken van exports, richt de autorisaties goed in en oefent hier controle op uit.	School	3		
2	Verwerker gebruikt het model in de verwerkersovereenkomst niet (goed).	4	1. Peple brengt de verwerkersovereenkomst in overeenstemming met de eisen uit de AVG. 2. Onderwijsinstelling sluit een up-to-date verwerkersovereenkomst met Peple.	Peple en school	2		
	Onvoldoende invulling aan het beginsel van	6	Onderwijsinstelling voert (periodiek) een lokale DPIA uit en controleert overbodige velden.	School	3		

	dataminimalisatie.						
4	Uitbesteed proces (Administratie Kantoor) niet goed in geregeld (met de verwerker).	9	Onderwijsinstelling sluit een adequate verwerkersovereenkomst met de verwerker en controleert de door de verwerker uitgevoerde DPIA.	School	3		
5	Teveel gegevens uitgewisseld met derde partijen.	6	1. Onderwijsinstelling sluit een adequate verwerkersovereenkomst met koppelpartijen; 2. Onderwijsinstelling heeft een opgeleide functioneel beheerder die regelmatig wordt bijgeschoold.	School	3		
6	Medewerkers beschikken over teveel rechten	6	• Onderwijsinstelling controleert periodiek de autorisaties; • Onderwijsinstelling maakt bij het aanmaken van een superuser altijd het 4 ogen principe toe	School	3		
7	2fa is uitgeschakeld	9	Onderwijsinstelling verbiedt het uitschakelen van 2FA in Visma.net HRM & Payroll.	School	2		
8	Gegevens worden te lang bewaard	6	Onderwijsinstelling neemt het periodiek verwijderen van	School	2		

			gegevens op in een proces.				

7. 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 privacy coördinator 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 Visma.net HRM & Payroll minimaal eens per drie jaar her beoordelen.		
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 (optionele)		

	toepassingen van Visma.net HRM & Payroll .		
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 getraind in het gebruik ervan.		
12	Persoonsgegevens worden niet op verkeerde plekken opgeslagen omdat regels en/of bekendheid met Visma.net HRM & Payroll 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 Visma.net HRM & Payroll en dit is tevens gedocumenteerd.		
14	De onderwijsinstelling neemt verantwoordelijkheid voor het veilig koppelen van het Visma.net HRM & Payroll met een ander systeem zoals een leerlingadministratiesysteem.		

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

Risico	**Te nemen maatregel**	**Uitgevoerd?**	**Opmerking/toelichting**
Het risico is dat er door het gebruik van de export en/of download functie mogelijk gevoelige persoonsgegevens buiten de applicatie terecht komen wat verlies van controle over deze data tot gevolg heeft.	Onderwijsinstelling maakt afspraken over het gebruiken van exports, richt de autorisaties goed in en oefent hier controle op uit.		
Het risico is dat de verwerkingsverantwo	Onderwijsinstelling sluit een up-to-date		

ordelijke geen toereikende afspraken met de verwerker heeft gemaakt over de verwerking van de persoonsgegevens.	verwerkersovereenkomst met Peple.		
Het risico is dat er teveel gegevens worden verwerkt en dat er onvoldoende invulling wordt gegeven aan het beginsel van dataminimalisatie.	Onderwijsinstelling voert (periodiek) een lokale DPIA uit en controleert overbodige velden.		
Het risico dat er - als er door de school gebruik wordt gemaakt van Visma.net HRM & Payroll in een uitbesteed proces (administratiekantoor) – geen goede afspraken zijn gemaakt over de gegevensverwerking in Visma.net HRM & Payroll (als subverwerker) met de verwerker (het administratiekantoor).	Onderwijsinstelling sluit een adequate verwerkersovereenkomst met de verwerker en controleert de door de verwerker uitgevoerde DPIA.		
Het risico is dat er teveel gegevens worden uitgewisseld met derde partijen.	1. Onderwijsinstelling sluit een adequate verwerkersovereenkomst met koppelpartijen; 2. Onderwijsinstelling heeft een opgeleide functioneel beheerder die regelmatig wordt bijgeschoold.		
Het risico is dat medewerkers over teveel rechten beschikken.	1. Onderwijsinstelling controleert periodiek de autorisaties; 2. Onderwijsinstelling maakt bij het aanmaken van een superuser altijd het 4 ogen principe toe.		
Het risico is dat er bij accounts (met veel rechten) onregelmatigheden	Onderwijsinstelling verbiedt het uitschakelen van 2FA in Visma.net HRM & Payroll.		

plaatsvinden doordat de toegang tot de applicatie onvoldoende is beveiligd omdat 2fa wordt uitgeschakeld.			
Het risico is dat gegevens te lang worden bewaard.	Onderwijsinstelling neemt het periodiek verwijderen van gegevens op in een proces.		

[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]					
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]

D. 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 […].

E. 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.

F. 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.

G. 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.

H. 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 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