CENTRALE DPIA
Jamf School

Versie 2.0 (Maart 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	Ashley Hoogendoorn Ferdy IJsselmuiden (DPIA-projectmanager) Hans-Peter Ligthart (portfoliomanager IBP)
Met dank aan	Medewerkers van Jamf

Inhoudsopgave

1. Samenvatting

Mobile Device Management van Jamf is veilig te gebruiken

Deze DPIA heeft betrekking tot Jamf School, een Mobile Device Management systeem.

Uitvoering van de DPIA

SIVON heeft deze DPIA uitgevoerd in ongeveer een periode van twee jaar. Jamf is in de gesprekken transparant geweest en heeft duidelijke inzichten gegeven in het systeem. Jamf heeft verder geluisterd naar de suggesties van SIVON om onder andere de SLASA aan te passen.

Conclusie

Jamf School is een veelgebruikte cloud-applicatie die door scholen gebruikt wordt om Apple apparaten te beheren vanuit een centrale omgeving. Vanuit deze omgeving kunnen uitgebreide beheermogelijkheden worden vormgegeven voor apparaten zoals Macbooks, iPads, smartphones, hun gebruikers en klassen als ook de gewenste apps. Uit de DPIA is gebleken dat er qua informatiebeveiliging geen grote risico's verbonden zijn aan het gebruik van Jamf school, en er zijn slechts een aantal risico's waar scholen zelf maatregelen voor moeten treffen. Deze zullen moeten worden meegenomen in de 'lokale DPIA', het gaat dan om de volgende:

3. Onbevoegde toegang tot het admin-account, shut down onderwijs met Apple Apparaten.

4. Adminrollen moeten zelf worden ingericht.

6. Te brede beheerrechten toekennen aan gebruikers.

7. Issues met betrekking tot support tickets (via de support desk).

8. Verlies van controle toegang tot de Apple store.

De volgende risico's zijn in het kader van de DPIA door Jamf zelf gemitigeerd:

1. Een akkoord sluiten op de Jamf voorwaarden door een ongeautoriseerde gebruiker.

2. Gebrek aan transparantie eigen verwerkingsdoeleinden Jamf.

5. Risico's die zijn op de verwerkersovereenkomst.

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 uit (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 n 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 privacytoezichthouder 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.

Beoordeling noodzaak DPIA Jamf

Bij het gebruik van het Mobile Device Management systeem van Jamf School worden op een grote schaal en op dagelijkse basis (gevoelige) persoonsgegevens verwerkt van minderjarige leerlingen. Deze minderjarige leerlingen zijn aan te merken als een kwetsbare groep waarbij hogere eisen gesteld worden aan de bescherming van hun persoonsgegevens. Ook de aard van deze gegevens, onder andere locatiegegevens, vereist de verankering van zorgvuldige waarborgen op het gebied van privacy en informatiebeveiliging. Omdat er bij deze verwerking wordt voldaan aan een tweetal criteria uit zowel het DPIA besluit[2] als de EDPB-richtsnoeren[3], betekent dit dat er een DPIA-verplichting geldt op basis van artikel 35 van de AVG.

[1] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf
[2] wetten.nl - Regeling - Besluit lijst verwerkingen persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens - BWBR0042812 (overheid.nl)
[3] JUSTICE AND CONSUMERS ARTICLE 29 - Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) (europa.eu)

De verwerkingen binnen Jamf School voldoen aan de volgende twee criteria welke nader worden uitgewerkt:

1.De Verwerking vindt plaats op grote schaal

en

2. De verwerking van de gegevens heeft betrekking op een kwetsbare doelgroep.

De Europese toezichthouder European Data Protection Board (EDPB) omschrijft in de Richtsnoeren DPIA negen criteria die relevant zijn bij beoordeling of de verwerking "waarschijnlijk een hoog risico inhoudt".

In de meeste gevallen kan een verwerkingsverantwoordelijke ervan uitgaan dat voor een verwerking die aan twee van deze criteria voldoet een DPIA moet worden uitgevoerd. Hoe groter het aantal criteria waaraan een verwerking voldoet, hoe waarschijnlijker het is dat ze een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen, en dus een DPIA vereist is, ongeacht de maatregelen die de verwerkingsverantwoordelijke voornemens is te nemen. In sommige gevallen kan een verwerkingsverantwoordelijke echter oordelen dat een verwerking die aan slechts één van deze criteria voldoet een DPIA vereist.

Toelichting criteria:
1.*op grote schaal*

Een aantal van de criteria is enkel van toepassing bij verwerking op grote schaal. In de AVG wordt niet gedefinieerd wat grootschalig is. De AP en de EDPB geven aan dat met name de volgende factoren in aanmerking moeten worden genomen bij het bepalen of een verwerking op grote schaal wordt uitgevoerd:

- het aantal betrokkenen, hetzij als een specifiek aantal hetzij als een deel van de relevante populatie;
- het volume van gegevens en/of het bereik van verschillende gegevensitems die worden verwerkt;
- de duur, of het permanente karakter, van de gegevensverwerkingsactiviteit;
- de geografische omvang van de verwerkingsactiviteit.

De meeste scholen die gebruikmaken van Apple apparaten gebruiken Jamf voor het beheer daarop. Dit betekent dat alle leerlingen van die betreffende scholen onderworpen zijn aan het management wat op die apparaten plaatsvindt via Jamf. Hierdoor is er sprake van een verwerking op ‘grote schaal’.

2.Gegevens met betrekking tot kwetsbare betrokkenen

De verwerking van gegevens met betrekking tot kwetsbare betrokkenen is een criterium vanwege de machtsongelijkheid tussen de betrokkenen en de verwerkingsverantwoordelijke, wat betekent dat de natuurlijke personen mogelijk niet in staat zijn om gemakkelijk in te stemmen met of bezwaar te maken tegen de verwerking van hun gegevens, of om hun rechten uit te oefenen. Kwetsbare betrokkenen kunnen kinderen omvatten (kinderen kunnen worden geacht niet in staat te zijn om bewust en bedachtzaam in te stemmen met of bezwaar te maken tegen de verwerking van hun gegevens), werknemers, kwetsbaardere segmenten van de bevolking die speciale bescherming behoeven (geesteszieken, asielzoekers, bejaarden, patiënten enz.), en in elk geval waarin een onevenwichtigheid in de relatie tussen de positie van de betrokkene en de verwerkingsverantwoordelijke kan worden vastgesteld.

De Autoriteit Persoonsgegevens (hierna: AP) heeft veelvuldig aangegeven dat de gegevens van minderjarige leerlingen kwalificeren als gevoelig. Zie in dit kader bijvoorbeeld de volgende passage uit de brief van de AP aan het Ministerie van Onderwijs, Cultuur en Wetenschappen: “Kinderen hebben recht op een passende invulling van hun grondwettelijke recht op bescherming van persoonsgegevens en dienen te worden beschermd tegen schendingen van dat grondrecht. Een juiste borging van dat grondrecht vergt extra aandacht bij kinderen. Zij hebben volgens de AVG, het Handvest en het Verdrag inzake de rechten van het kind recht op specifieke bescherming. De AP stelt daarom voorop dat bij het inschatten van de risico’s aangaande de verwerking van persoonsgegevens in voldoende mate de specifieke risico’s voor kinderen moeten worden geïdentificeerd en onderzocht. Dit vergt een nauwkeurige analyse van de specifieke risico’s voor kinderen en de uitwerking die deze risico’s hebben op kinderen van verschillende leeftijden. Daarbij is het onvoldoende om kinderen te positioneren als betrokkenen met alleen een lagere leeftijd, aangezien kinderen zich minder bewust zijn van de betrokken risico’s en gevolgen van de verwerking van hun persoonsgegevens. Daarbij kunnen risico’s een andere impact en uitwerking hebben op kinderen dan op volwassenen. Het stelselmatig vastleggen van gegevens over het gedrag en de ontwikkeling van kinderen kan leiden tot risico’s zoals discriminatie en uitsluiting. Bovenstaande leidt tot de conclusie dat er bij de verwerking van persoonsgegevens van kinderen extra zorgvuldig zal moeten worden onderzocht welke risico’s er spelen en welke waarborgen passend zijn.”

De combinatie van het grootschalige karakter van de verwerking en de betrokkenheid van kwetsbare leerlingen voldoet aan criteria die een DPIA-verplichting rechtvaardigen volgens zowel het DPIA-besluit als de richtlijnen van de European Data Protection Board.

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 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 geregistreerd 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 en 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. 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 het systeem op scholen.

V. Gebruik model

De centrale DPIA volgt het model van de Rijksoverheid[4], aangevuld met onderwijs-specifieke informatie uit de *Handleiding uitvoeren data protection impact assessment (DPIA) voor het po en vo (versie 1.0)*[5]. 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:

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

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

VI. Scope van deze DPIA

Jamf kent meerdere management platforms (zoals Jamf Pro en Jamf Now) waar organisaties, afhankelijk van hun behoefte, gebruik van kunnen maken. Schoolinstellingen zullen bij Jamf voornamelijk de dienst Jamf School afnemen en daar ligt binnen deze DPIA de focus op. Jamf School is een veelgebruikte cloud-applicatie die door scholen gebruikt wordt om Apple apparaten te beheren vanuit een centrale omgeving. Vanuit deze omgeving kunnen uitgebreide beheermogelijkheden worden vormgegeven voor apparaten zoals Macbooks, iPads, smartphones, hun gebruikers en klassen als ook de gewenste apps.

Om het beheer over de door school uitgegeven Apple apparaten vorm te geven zijn er een aantal stappen nodig. Jamf krijgt controle over de Apple omgeving via een API (Application Programming Interface). Deze API wordt geactiveerd door het uitwisselen van certificaten die gekoppeld zijn aan Apple School Manager. Jamf integreert dus met Apple School Manager om een koppeling mogelijk te maken voor scholen om Apple apparaten te beheren binnen een bredere IT-structuur. Deze uitwisseling van certificaten vindt onder meer plaats op de volgende vlakken.

- Algemene koppeling
- User management
- Device enrollment en management
- App management

Deze DPIA gaat over Jamf School device management wat scholen dus in staat stelt om beleid op apparaten door te voeren. Jamf School biedt gebruikers een veilige omgeving door de mogelijkheid om het gebruik van "onveilige" digitale middelen te beperken, wat de veiligheid van gebruikers waarborgt.

Door school uitgegeven Apple apparaten

Jamf School biedt een uitgebreide reeks instellingsmogelijkheden voor het beheer van apps op apparaten die worden gebruikt binnen onderwijsinstellingen. Deze instellingen variëren van het toestaan van een grote mate van vrijheid voor gebruikers om apps te downloaden tot aan strikte beheersmaatregelen waarbij het downloaden van apps alleen vanuit het beheer mogelijk is.

Deze DPIA is geschreven vanuit het perspectief dat de Apple apparaten die onder beheer zijn bij Jamf School enkel voor schoolgerelateerde doeleinden gebruikt zullen worden. Dit brengt met zich mee dat het aan de school is om zowel de te gebruiken apps als de functionaliteiten vorm te geven. Het zelf downloaden van apps is voor de leerling dus geen

mogelijkheid. Dit voorkomt de mogelijkheid voor de leerling om potentieel schadelijke of ongeschikte apps te downloaden als ook afleiding van het leerproces. Onveilige apps kunnen mogelijk toegang krijgen tot gevoelige gegevens op het apparaat zoals contacten, locatiegegevens en foto's en deze gegevens verder delen.

Een ongewenst bijeffect van vrij gebruik van het apparaat is de vergroting van het risico op cyberpesten en online intimidatie waarbij leerlingen kwetsbaar kunnen zijn voor misbruik door medeleerlingen of externe partijen[6]. Het onmogelijk maken van het gebruik van social media op de Apple apparaten verkleind, in ieder geval tijdens schooltijd, de mogelijkheid om digitaal te pesten of gepest te worden.

Deze DPIA gaat dus uit van de situatie waarbij het voor de leerling onmogelijk is om zelf apps te downloaden en de functionaliteiten beperkt zijn tot wat is toegestaan door de IT-beheerders van de school.

Verschil Jamf School en Apple School manager
Jamf School is een uitgebreid beheerplatform dat specifiek is gericht op IT-beheer van Apple-apparaten in het onderwijs. Zo is het voor scholen via Jamf School o.a. mogelijk om op basis van de gedetailleerde beheermogelijkheden centraal de configuratie, updates, app-distributie, beveiligingsinstellingen en monitoring van Apple-apparaten uit te voeren. Dit betekent dat er nooit toegang is tot de inhoudelijke content of andere verwerkingen die binnen Apple School manager plaatsvinden of welke applicaties op de Apple apparaten dan ook. Jamf School integreert met Apple School Manager waardoor je apps kunt toewijzen aan apparaten zonder dat er toegang tot de app store nodig is..

Apple School Manager is een oplossing voor het beheren van Apple-apparaten, het toewijzen van apparaten aan gebruikers en klassen en het faciliteren van de aankoop en distributie van apps en boeken in het onderwijs. Het aanschaffen van educatieve apps is dus mogelijk via Apple School Manager. Jamf School en Apple School Manager kunnen samenwerken en integreren om een uitgebreide effectieve beheeromgeving te bieden van Apple-apparaten in het onderwijs.
NB Zie Apple school manager als de TV en Jamf School als de afstandsbediening. Met Jamf school kan de beheerder bepalen wat er in de Apple omgeving gebeurt.

[6] Nederlands Jeugdinstituut en haar uitleg over Online pesten. https://www.nji.nl/pesten/online-pesten-wat-is-het#:~:text=Online%20pesten%20gebeurt%20op%20verschillende,het%20anders%20dan%20offline%20pesten.

VII. Buiten scope

De volgende management oplossingen van Jamf vallen buiten de scope van deze DPIA:

Jamf Pro, Jamf Now, Jamf protect, Jamf Connect en Jamf Safe Internet.

Binnen de Jamf School omgeving kan ook gebruik gemaakt worden van de apps Jamf School parent, Jamf School student, Jamf School assessment en Jamf School teacher. Deze zijn echter buiten scope van de DPIA. Op deze apps kan op een later moment een DPIA worden uitgevoerd.

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 (mitigerende) maatregelen.

De centrale DPIA is uitgevoerd in de periode 2023-maart 2025.

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[7] 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.

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

- Burgerservicenummer (BSN)
- BIG-nummer (beroepen in de individuele gezondheidszorg),

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

• 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[8].

[8] 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

Jamf school biedt met haar Mobile Device Management-systeem (MDM) een softwareoplossing die scholen helpt bij het beheren en beveiligen van mobiele Apple apparaten zoals Macbooks en Ipads. Het stelt hiermee onder meer de IT-beheerders in staat om verschillende aspecten van deze apparaten op afstand te beheren, zoals het installeren van apps, het configureren van instellingen en het monitoren van gebruik. Jamf school slaat dus geen user/content data op en heeft hier evenmin toegang toe.

Scholen hebben baat bij het gebruik van een MDM-systeem zoals Jamf School omdat deze de IT-beheerders een centraal platform biedt waarmee ze meerdere apparaten centraal kunnen beheren, zoals de beveiliging van mobiele apparaten, het afdwingen van sterke wachtwoordbeleidsregels, gegevens op afstand te wissen in geval van verlies of diefstal, en zelfs apparaten te vergrendelen of te lokaliseren. Dit helpt bij het beschermen van (gevoelige) gegevens en voorkomt ongeoorloofde toegang.

Jamf is vooral een beheerstool. Jamf slaat maar beperkt persoonsgegevens op, wel meta data maar geen content data. Zie Jamf als een soort remote control van de Apple omgeving. Content data staat dus bij Apple (of elders).

Jamf School biedt diverse functies waarmee de apparaten van Apple vormgegeven kunnen[9]. De belangrijkste functionaliteiten om deze apparaten effectief te kunnen beheren zijn op een rijtje gezet in onderstaande tabel.

Functionaliteit	**Verwerkingen**
Dashboard	Monitor beheerde devices, gebruikers en apps. Bekijk snel de status van devices en signaleer problemen.
Klaslokaalbeheer	Apps, inhoud en beperkingen configureren.

[9] Jamf School Apple MDM voor scholen, onderwijs en het klaslokaal

IBeacon-profieltoewijzing	Leerlingen krijgen automatische toegang tot onderwerpspecifieke materialen, terwijl niet-gerelateerde inhoud wordt verborgen.
Incidentensysteem	Schade aan devices of andere problemen bijhouden.
Locaties	Elke locatie en de devices, gebruikers en groepen afzonderlijk beheren door vanuit één locatie profielen en apps te pushen.
Content caching	Download bestanden die door meerdere leerlingen worden gebruikt naar één toegewijd device dat vanaf daar verder werkt om anderen te bedienen. (b.v. voor App updates)
App Request	Leerkrachten kunnen apps aanvragen, die vervolgens worden gedeeld met IT-beheerders. Organisaties kunnen apps beoordelen op informatie beveiliging en privacy aspecten alvorens deze de authoriseren en te distribueren

Met MDM voldoen schoolbesturen aan norm 11.3 uit het normenkader IBP[10].

Koppelen Apple apparaten

In deze DPIA wordt aandacht besteed aan de verschillende manieren van aanmelden van het apparaat en de effecten daarvan op de verwerkingen door Jamf School. Onder beheer brengen van Apple apparaten bij Jamf School kan plaatsvinden via de school. Dit gebeurt doorgaans wanneer de apparaten door de scholen worden uitgegeven. Apple apparaten gekocht door een school bij een Apple reseller worden via Apple School Manager automatisch gekoppeld aan de managed omgeving van de school. Onbevoegden kunnen het apparaat nooit onder eigen naam registreren. Na factory reset zal het apparaat altijd op basis van serienummer weer aan de school gekoppeld worden. Dit is de meest veilige optie. Daarnaast bestaat ook de zogenaamde gebruikersinschrijving om Apple devices van ouders/leerling in beheer te nemen.

Toegang

Alleen beheerders rollen hebben toegang tot Jamf school. Inloggen is standaard met twee-factorauthenticatie (2FA) wee-factorauthenticatie (2FA[1112]Jamf School ondersteunt

[10] Het Normenkader informatiebeveiliging en privacy voor het Funderend Onderwijs biedt praktische handvatten voor de inrichting van sterkere informatiebeveiliging en wordt op termijn wettelijk verankerd, Digitaal Funderend Onderwijs 2023 (kennisnet.nl)

[12] https://learn.jamf.com/nl-NL/bundle/jamf-pro-documentation-current/page/Jamf_Pro_User_Accounts_and_Groups.html

rolgebaseerde toegangscontrole met gedetailleerde CRUD (create, read, update, delete) privileges voor verschillende functies binnen het systeem. De rollen met bijbehorende rechten kunnen schoolbesturen zelf inrichten.

Deze maatregelen waarborgen een gecontroleerde toegang tot het systeem, beveiliging via 2FA/MFA, en een minimaal vereiste toegangsrechten op basis van de principes van 'least privilege'

Jamf School integraties
Jamf School kent de onderstaande veel voorkomende integraties van waaruit synchronisatie kan plaatsvinden om gebruikers, klassen en locaties te importeren in Jamf School. Daarnaast kan er handmatig worden gesynchroniseerd vanuit het Jamf School-dashboard en met een LDAP-adreslijstvoorziening.

Apple School Manager
Somtoday
Microsoft Azure
Google Sign-In

2. Persoonsgegevens

In dit hoofdstuk van de DPIA wordt een analyse uitgevoerd van de verwerking van persoonsgegevens binnen Jamf School, met specifieke aandacht voor verschillende soorten persoonsgegevens en de definities daarvan. Het hoofdstuk richt zich op het begrijpen van de aard en het gebruik van persoonsgegevens binnen Jamf School en het identificeren van mogelijke privacyrisico's en mitigatiemaatregelen. Zie ook de definitiebepalingen onder IX.

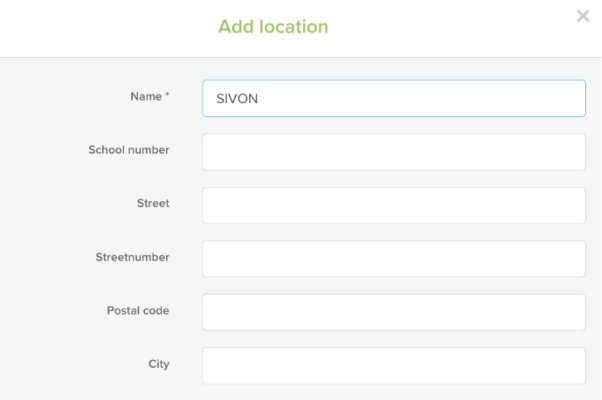
Betrokkenen

De AVG biedt specifieke bescherming aan kwetsbare betrokkenen zoals kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader. In Jamf School worden persoonsgegevens verwerkt van leerlingen van de onderwijsinstelling en van medewerkers (beheerders en docenten) van de onderwijsinstelling. Dit betekent dat aan de verwerking van deze persoonsgegevens strengere waarborgen worden gesteld.
In de onderstaande uitwerking zal aan de hand van printscreens en duiding worden geschetst welke persoonsgegevens binnen Jamf School worden verwerkt.

Het gebruik van Jamf School vereist niet dat vertrouwelijke of gevoelige persoonlijke gegevens verstrekt moeten worden. Jamf School maakt kenbaar tijdens het DPIA-onderzoek alleen de minimale gegevens te verzamelen die nodig zijn om de software te laten functioneren. Jamf controleert of reguleert geen aanvullende gegevens die klanten invoeren in de gehoste services.

Accountgegevens

Accountgegevens zijn algemene gegevens van de school en schoollocaties.



Administrator account gegevens

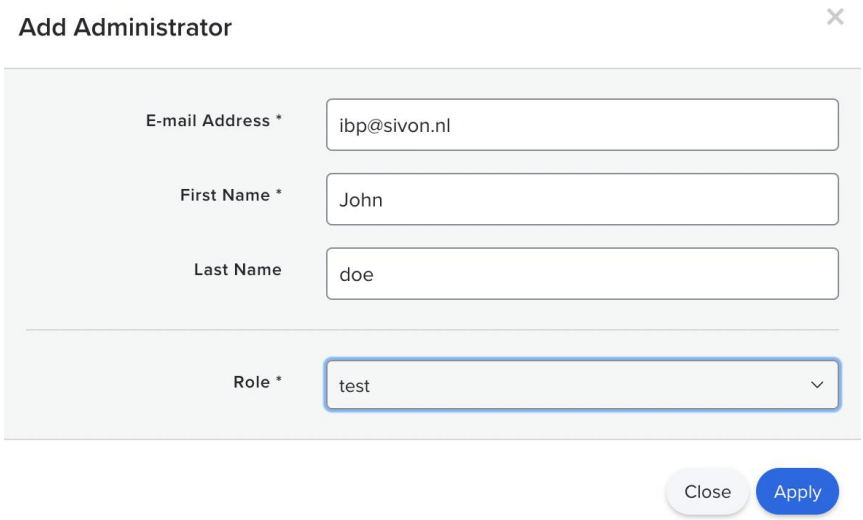
Dit zijn typisch de beheerders van de Jamf School omgeving. Het top-level account is de system administrator. Dit account heeft alle rechten. 2 factor authenticatie is verplicht voor dit type account. Er kan vanuit deze rol geen export gemaakt worden van de gebruikershistorie van de users of anderszins gedetailleerde inzichten worden verworven. Het is bijvoorbeeld niet mogelijk om te zien wanneer er voor het laatst gebruik is gemaakt van welke apps. Wel is in deze rol informatie te zien welke betrekking heeft op de hardware, de versie van het besturingssysteem, opslag, de apps en waar het apparaat zich (bij benadering) bevindt[13].

De beschreven inzichten door de system administrator beperkt de toegang tot gevoelige gebruikersgegevens en vermindert het risico op misbruik van persoonlijke informatie door het beheerdersaccount, wat de privacy van de gebruikers van de Jamf School beschermt. Bovendien zorgt de verplichte tweefactorauthenticatie voor een extra beveiligingslaag, waardoor ongeautoriseerde toegang tot het account wordt voorkomen.
De system administrator kan verschillende beheerdersrollen aanmaken voor de verschillende verantwoordelijkheden binnen de school, zoals materiaalmanager, apparaatmanager of helpdeskmedewerker.
Voordat een beheerdersrol wordt ingesteld, is het verstandig de specifieke functies en verantwoordelijkheden te bepalen die voor die rol moeten gelden. Hiermee bepaal je welke toegangsrechten en bevoegdheden voor die rol nodig zijn.

Verplichte persoonsgegevens: voornaam, email, rol

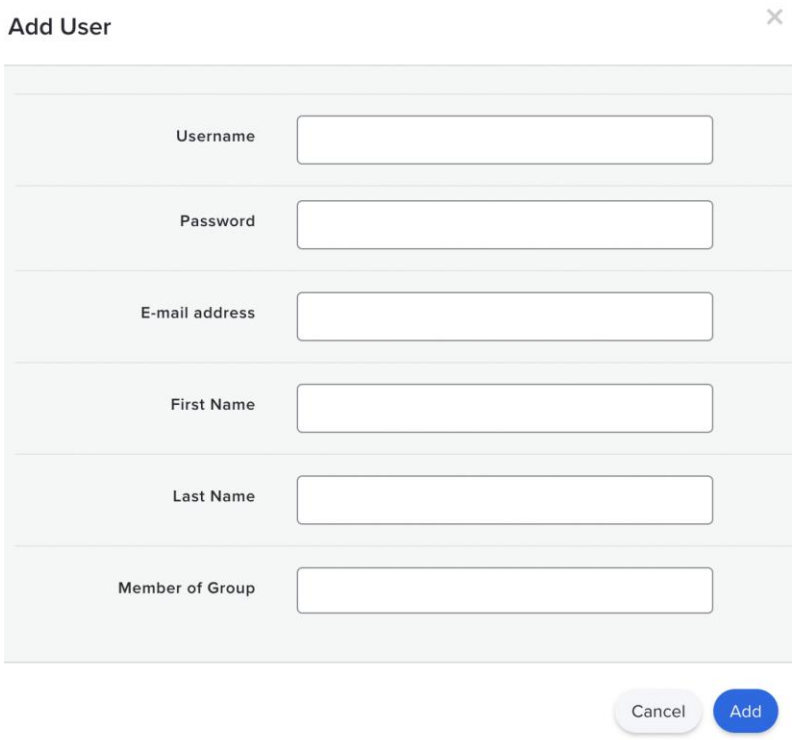
Optionele gegevens: achternaam, foto, telefoonnummer

[13] https://learn.jamf.com/nl-NL/bundle/jamf-school-documentation/page/Viewing_and_Editing_Device_Inventory_Information_in_Jamf_School.html



Gebruikersgegevens

Gebruikers in Jamf zijn typisch de gegevens van leerlingen en medewerkers.



Bij het aanmaken van een user worden de onderstaande gegevens gevraagd. Deze gegevens kunnen ook via een Active Directory, import of Apple School Manager koppeling in Jamf School opgenomen worden.

- Username
- Password
- E-mail adres
- First Name
- Last Name

- Member of Group

Verder registreert Jamf School

- Gekoppelde device (computer naam)
- Rol (Teacher/Student/Staff)
- IP adres en locatie gegevens (optioneel / default aan)
- Apps
- Klas

Locatie
Wanneer een Apple apparaat gestolen of verloren is kan via Jamf School op afstand het apparaat gewist worden zodat onbevoegden geen toegang meer kunnen verkrijgen tot de inhoud. Evengoed kan op deze manier de locatie worden vastgesteld. Dit kan helpen bij het traceren van het verloren apparaat. De locatie wordt in een dergelijk geval verkregen op basis van een IP-adres, het gaat dus niet om GPS-tracking hetgeen in de regel een stuk nauwkeuriger en betrouwbaarder is. Voor het vinden van het apparaat moet het dus verbonden zijn met het internet.

Het verkrijgen van een locatie op basis van een IP-adres kan verschillende niveaus van precisie hebben afhankelijk van factoren zoals de beschikbare netwerkgegevens en de nauwkeurigheid van de IP-geolocatietechnologie.
Bij het technisch onderzoek tijdens deze DPIA bleek de geteste bijvoorbeeld regelmatig in een grote stadsplas te liggen volgens locatievoorziening in de beheeromgeving. Het betrof echter wel een stadsplas in de buurt van de woning van de bezitter van de Ipad hetgeen contextueel beredeneerd wel de veronderstelling rechtvaardigt dat de Ipad zich in het huis van de eigenaar bevindt. Volgens de AVG wordt een locatie die een individu identificeert of identificeerbaar maakt beschouwd als een persoonsgegeven. Dit geldt ook voor locatiegegevens die worden verkregen via een IP-adres. Zelfs als het IP-adres niet rechtstreeks naar een specifieke persoon verwijst, kan het nog steeds worden beschouwd als persoonsgegevens omdat het, wanneer het wordt gecombineerd met andere informatie of context, kan leiden tot de identificatie van een individu. Daarom moeten locatiegegevens die via IP-adressen worden verkregen worden behandeld in overeenstemming met de AVG en de relevante gegevensbeschermingsprincipes, zoals het beginsel van doelbinding en gegevensminimalisatie.

Prestatie- en gebruikersgegevens
Uit artikel 19c van de SLASA[14] (Software License and Service Agreement) blijkt dat Jamf School in beginsel statistische, gebruiks-, configuratie- en prestatiegegevens van de diensten ten behoeve van het bewaken van de prestaties, integriteit en stabiliteit van de diensten verzamelt. Jamf heeft tijdens dit DPIA onderzoek toegezegd om de verzameling hiervan voor de gebruikers binnen de onderwijssector te staken met ingang van 28 februari 2024. Hoewel dit een stap in de goede richting is geeft Jamf tevens aan dat de verwerkingen zoals bedoeld in artikel 19 a en b indien door Jamf dit noodzakelijk acht, zullen plaatsvinden.

[14] Deze is hier integraal te vinden.

Naar aanleiding hiervan dient er evengoed nader inzicht te worden gegeven naar de precieze betekenis van deze verwerkingsdoeleinden gezien het mogelijke gebrek aan transparantie, doelbinding en juridische grondslag voor de gebruikers binnen het onderwijs een risico inhoudt.

In het verbeterplan zijn specifieke afspraken gemaakt over de randvoorwaarden van de gedane toezegging door Jamf. Nederlands educatieve instellingen worden door Jamf gecategoriseerd als ”custom contract”. Bij custom contract vervallen de verwerking zoals onder 19.c vermeld.

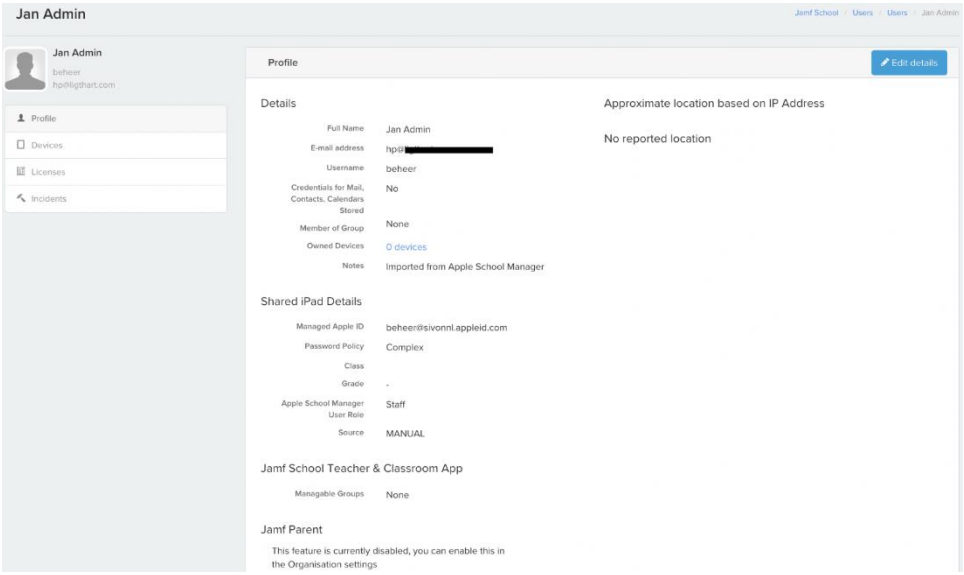
Artikel 19 SLASA, Data Collection and Use 19. a) Jamf may collect and use Performance and Usage Data and Customer Content to check compliance with contractual Software usage limits; monitor the performance, integrity and stability of the Hosted Services; address or prevent technical or security issues; provide support Services; and improve the Hosted Services and/or Software. We will not otherwise access, use or process Customer Content except as necessary to provide the Services. b) Jamf may use de-identified, anonymized and aggregated Performance and Usage Data to analyze, improve and develop the Software and/or Hosted Services, such as the detection of new security threats. c) Jamf and its service providers may use de-identified, anonymized and aggregated Performance and Usage Data and Customer Content during and after the term of this Agreement for any purpose so long as the data or content does not identify Customer or any individual, including Users.

Jamf presenteert zich als verwerker

Jamf is helder in haar communicatie ten aanzien van de rol die zij vervult als verwerker versus de rol van het schoolbestuur als verwerkingsverantwoordelijke. In de Q&A[15] maakt Jamf kenbaar geen onafhankelijke besluiten te nemen ten aanzien van de verwerking van persoonsgegevens en dit enkel te doen in opdracht van de verwerkingsverantwoordelijk (het schoolbestuur). Echter blijkt uit artikel 19 in de SLASA dat Jamf wel eigen verwerkingsdoeleinden heeft die buiten de reikwijdte vallen die binnen de reguliere verwerkersrol behoren. Ook voor verschillende support rollen[16] verricht Jamf verwerkingen in de rol van verwerkingsverantwoordelijke. Nu er op onderdelen een verschuiving plaatsvindt in het bepalen van het doel en de middelen van de verwerking is het aan Jamf om hier transparant over te zijn en de nodige passende juridische grondslagen gemotiveerd kenbaar te maken.

Who is the controller and who is the processor? With respect to Personal Data provided to Jamf in relation to Customer’s use of Jamf’s Services, the Customer is the controller and Jamf is the processor. As the processor, Jamf does not make independent decisions about the Personal Data and only processes it upon Customer’s instructions and in accordance with our SLASA, DPA and Data Protection Laws.

[15] https://www.jamf.com/resources/product-documentation/data-processing-agreement-for-jamf-customers-faqs/
[16] jamf-support.pdf



Telemetrie gegevens in de audit log van Jamf

5-7-2022 11:56:11	[redacted]@sivon.nl	Synchronize content purchased in volume	86.90.6.189	sivon.jamfcloud.com	SIVON
5-7-2022 11:50:11	[redacted]@sivon.nl	Save 'appearance' settings	86.90.6.189	sivon.jamfcloud.com	SIVON
5-7-2022 11:48:23	[redacted]@sivon.nl	Assign device C02H57G7Q6L4 to a user 'test2'	86.90.6.189	sivon.jamfcloud.com	SIVON
5-7-2022 11:47:39	[redacted]@sivon.nl	Assign device GG7H80X4Q16N to a user 'test1'	86.90.6.189	sivon.jamfcloud.com	SIVON
5-7-2022 11:43:43	[redacted]@sivon.nl	Install media 'Jamf test doc' on device GG7H80X4Q16N by user	86.90.6.189	sivon.jamfcloud.com	SIVON
5-7-2022 11:43:14	[redacted]@sivon.nl	Create wallpaper 'SIVON.png'	86.90.6.189	sivon.jamfcloud.com	SIVON
5-7-2022 11:40:58	[redacted]@sivon.nl	Create group 'alle devices'	86.90.6.189	sivon.jamfcloud.com	SIVON
5-7-2022 11:39:25	[redacted]@sivon.nl	Add in-house app	86.90.6.189	sivon.jamfcloud.com	SIVON
5-7-2022 11:38:37	[redacted]@sivon.nl	Synchronize content purchased in volume	86.90.6.189	sivon.jamfcloud.com	SIVON
5-7-2022 11:38:07	[redacted]@sivon.nl	Synchronize ASM	86.90.6.189	sivon.jamfcloud.com	SIVON
5-7-2022 11:37:22	[redacted]@sivon.nl	Refresh backend	86.90.6.189	sivon.jamfcloud.com	SIVON
5-7-2022 11:31:19	[redacted]@sivon.nl	Login success	86.90.6.189	sivon.jamfcloud.com	SIVON
1-7-2022 16:18:30	C02H57G7Q6L4	Enroll new device C02H57G7Q6L4	86.90.6.189	sivon.jamfcloud.com	SIVON

Overzicht geheel van verwerkte persoonsgegevens

Tabel 3.1: Overzicht verwerking van persoonsgegevens

Persoonsgegevens	**Medewerker schoolbestuur**	**Leerling**
Voor- en achternaam	X	X
Beroepsnaam en functie	X	
IP-adres, naam computer, gebruikersnaam en wachtwoord, groepsnaam	X	X
Mailadres	X	X
Locatie	X	X
Foto	X	X

De hiervoor genoemde informatie wordt samengebracht in één tabel:

Tabel 3.2: Overzicht verwerking van persoonsgegevens

Categorie betrokkene	Categorie persoonsgegevens	Persoonsgegeven	Bron/verkrijging persoonsgegeven
Medewerker schoolbestuur	Algemeen Locatiegegevens	Voor- en achternaam; Gebruikersnaam Wachtwoord E-mailadres Lid van de groep Foto (optioneel) Gekoppeld apparaat (naam computer) *Functietitel en rollen/taken* *IP adres en locatie gegevens (optional / default aan)* *Apps op apparaat* *Klas*	Schoolbestuur
Leerling	Algemeen Locatiegegevens	Voor- en achternaam; Gebruikersnaam Wachtwoord E-mailadres Lid van de groep Foto (optioneel) Gekoppeld apparaat (naam computer) *Apps op apparaat* *Klas* *IP adres en locatie gegevens (optional / default aan)*	Schoolbestuur

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 het schoolbestuur. Het gaat er hier vooral om een beeld te schetsen van de scope van de gegevensverwerkingsanalyse.

Het doel van Jamf is het helpen bij het beheren en beveiligen van gebruikers van Apple apparaten.
De verwerking van persoonsgegevens met behulp van Jamf School vindt plaats met het oog op apparaat-beheer en configuratie ter ondersteuning van leerkrachten en leerlingen in het onderwijs. Jamf School stelt een school in staat om geconfigureerde Apple apparaten te leveren en te beheren die scholen kunnen gebruiken voor het aanbieden van een digitale leeromgeving.
Jamf School heeft geen toegang tot de gegevensverwerkingen (bijvoorbeeld contentdata zoals mappen, documenten en leeroefeningen binnen educatieve apps) die plaatsvinden binnen deze leeromgeving. Via Jamf School kunnen wel de binnen de leeromgeving gewenste applicaties worden gedownload en geconfigureerd.

Duiding ten aanzien van de verwerkingen van persoonsgegevens
Jamf School fungeert als interface waarmee IT-beheerders van scholen instellingen kunnen activeren en configureren op de gemanagede Apple apparaten. Jamf heeft schriftelijk bevestigd geen toegang te hebben tot de functies ten aanzien van:
• Allow Dictionary Lookup Supervised only
• Allow QuickType Predictive Keyboard Supervised only
• Allow AutoCorrection Supervised only
• Allow Spell Check Supervised only

Met Jamf kan een beheerder deze functies aan of uit zetten, maar de verwerking vindt plaats bij Apple.

Het beperkte bereik van de verwerkingsactiviteiten binnen Jamf School wordt dus verklaard doordat het voornamelijk fungeert als een platform voor het beheren van instellingen en functionaliteiten van Apple apparaten.

De-facto worden binnen Jamf School de aan/uit knoppen van Apple bediend. Dit verklaart dan ook de beperkte verwerkingsactiviteiten en gegevensverwerkingen binnen Jamf School.

Verwerkingsactiviteiten
Voor de opsomming van de verwerkingen van persoonsgegevens die binnen Jamf school plaatsvinden is aansluiting gezocht bij de functionaliteiten van Jamf, de uitlatingen van Jamf over de werking van Jamf School, de verwerkersovereenkomst en de SLASA.

De gegevensverwerkingen die binnen Jamf School plaatsvinden zijn:

- App distributie Setup, configuratie en beheer van apparaten en omgeving
- Beveiligingsbeheer
- Monitoring en rapportage
- Ondersteuning en klantenservice
- Mobiel apparaat beheer

Duiding gegevensverwerkingen De voornaamste gegevensverwerkingen op de Apple apparaten vinden plaats binnen de apps die gepusht worden vanuit Jamf School. Er is dus geen (technische) mogelijkheid vanuit Jamf School om de content/core data van enige app te lezen of onderscheppen. De verwerkingsactiviteiten, zoals het maken van een opdracht binnen een educatieve applicatie, of het koppelen en aanmaken van leerlingaccounts binnen Apple school manager, vindt plaats binnen afgeschermde virtuele omgevingen, ook bekend als 'sandboxes'. Deze sandboxes zijn geïsoleerde omgevingen waarin applicaties kunnen worden uitgevoerd zonder directe toegang tot het onderliggende systeem of andere applicaties.

Mailmogelijkheden
Jamf School kent geen interne mailmogelijkheden. In dit kader is er dus geen sprake van privacygerelateerde aandacht op dit gebied.

Jamf School technische ondersteuning (support)

In het geval van de behoefte aan technische ondersteuning bestaat er de mogelijkheid om het voorliggende probleem voor te leggen aan de supportafdeling[17]. Eindgebruikers zoals leerlingen en leerkrachten hebben geen mogelijkheid om een ticket in te schieten. De administrator kan instellen of een aangemaakte beheerdersrol wel of geen tickets kan inschieten. In de praktijk zal een dergelijke melding dus door de applicatiebeheerder/administrator worden ingediend.

Het verwerken van persoonsgegevens is onvermijdelijk bij deze activiteit. Minimaal zullen gegevens worden verwerkt om de melding op te volgen en contact te onderhouden met de indiener, waaronder e-mailadres en telefoonnummer. Jamf School neemt de rol van verwerkingsverantwoordelijke op zich voor deze verwerkingen. Dit betekent dat scholen geen controle meer hebben over deze gegevens, wat relevant is bij het indienen van tickets en de mee te sturen gegevens.

Binnen de digitale omgeving van Jamf School kan een ticket worden aangemaakt waar onderwerp en beschrijving van het probleem ingevoerd kunnen worden als ook eventuele logbestanden, schermafbeeldingen of video's kunnen worden geupload.

Als je een probleem hebt in Jamf School en geen oplossing kunt vinden in de documentatie, kun je een supportticket maken om hulp bij de supportafdeling te vragen. Bij het opstellen

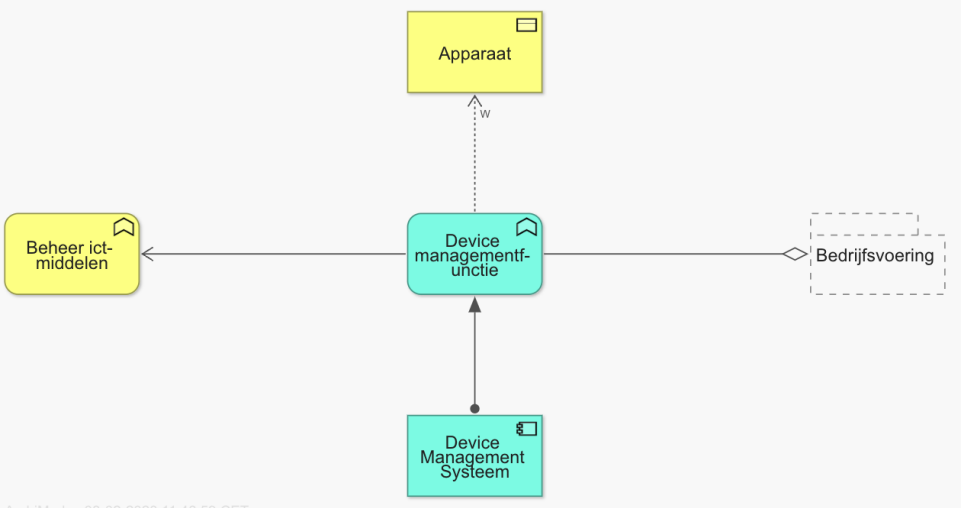
[17] https://learn.jamf.com/nl-NL/bundle/jamf-school-documentation/page/Creating_a_Support_Ticket.html

van een supportticket wordt geadviseerd gedetailleerde informatie over het probleem op te nemen[18].

Applicatielandschap

In termen van FORA referentie component kan Jamf School worden geduid als 'Device Management Systeem'. Een systeem ter ondersteuning van het beheer van devices / apparatuur, zoals laptops, smartphones, tablets e.d. Het Context diagram geeft inzicht in mogelijke koppelingen en gegevensuitwisselingen.

. https://fora.wikixl.nl/index.php/FORA/id-00804949-6a40-41978-d6d4-d43c7bc8c98

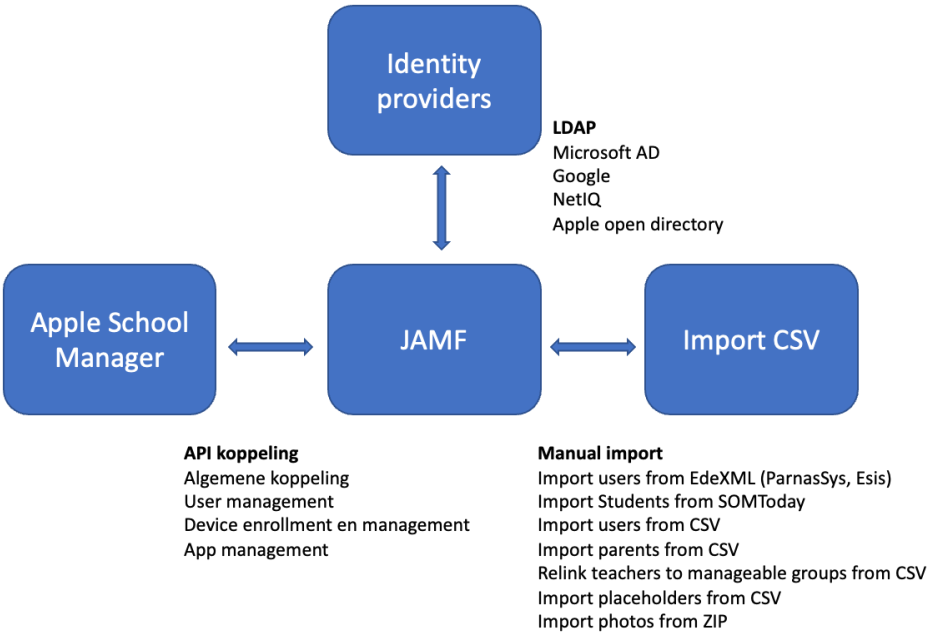


Koppelingen

Het onderstaande schema geeft een overzicht van de koppelingen die met Jamf School gemaakt kunnen worden. De koppelingen komen tot stand via webservices, uploads via SSL verbindingen of uitwisseling van certificaten/tokens. Allen volgens geldende (beveiligings) standaarden.
Gegevensoverdrachten voor integraties maken gebruik van veilige communicatieprotocollen. Gegevens worden versleuteld tijdens transport met behulp van TLS 1.2 en worden opgeslagen met AES-256-versleuteling

De DPIA ziet toe op privacy aspecten van Jamf School. Door het schoolbestuur moet beoordeeld worden of gekoppelde systemen ook aan DPIA's onderworpen moeten worden.

[18] Een supportticket maken - Jamf School-documentatie | Jamf

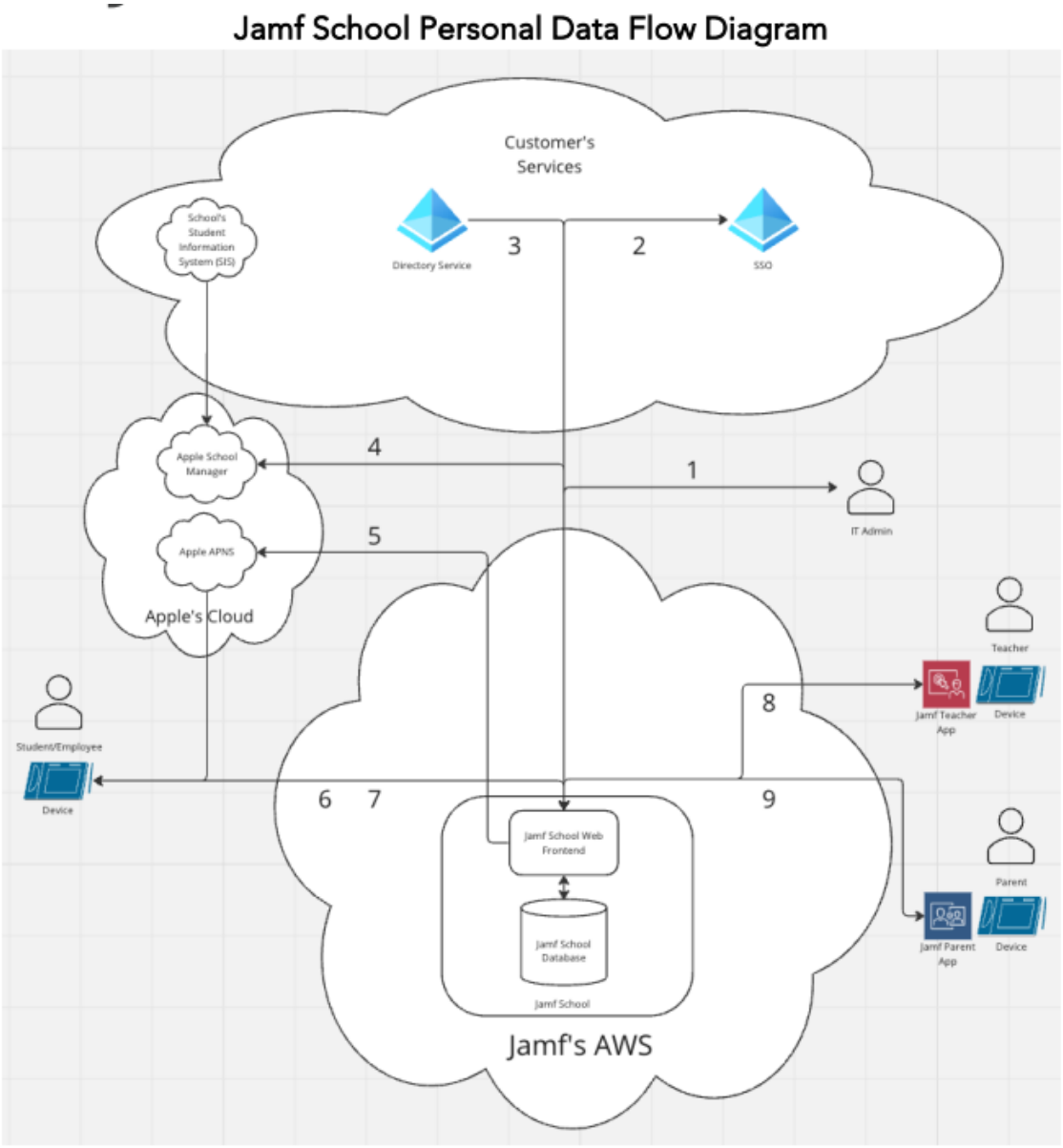


Tabel 3.3: Jamf School help pagina's over de diverse koppelingen

App volume purchase	https://learn.jamf.com/nl-NL/bundle/jamf-school-documentation/page/Volume_Purchasing_Integration.html#concept-206
MDM koppeling device enrollment	https://learn.jamf.com/nl-NL/bundle/jamf-school-documentation/page/Automated_Device_Enrollment_Integration.html#concept-1116
Synchronisatie gebruikers, klassen en locaties uit Apple School Manager	https://learn.jamf.com/nl-NL/bundle/jamf-school-documentation/page/Syncing_with_Apple_School_Manager.html#concept-4469
Somtoday sync	https://learn.jamf.com/nl-NL/bundle/jamf-school-documentation/page/Syncing_with_Somtoday.html
Active Directory	https://learn.jamf.com/nl-NL/bundle/jamf-school-documentation/page/Syncing_with_an_LDAP_Directory_Service.html

Gegevensstromen/stroomschema

Onderstaande dataflow schema van de binnen het ecosysteem te verwerken persoonsgegevens is door Jamf aangeleverd en biedt een visualisatie en toelichting op de verwerkingen van de soort persoonsgegevens alsmede de doeleinden daarvan.



1) IT Admin management of Jamf School Sends: user ids, name, email, phone, office location, position, device ids Reads: user ids, name, email, phone, office location, department, position, device ids, geolocation (lost mode only), IP address
Purpose: Setup, configuration, and management of devices and environment
2) Jamf School integration with a Customer's Single Sign On (SSO)
Sends: N/A (redirects)
Reads: user ids, name, email
Purpose: Enable customer authentication to Jamf services
3) Jamf School integration with a Customer's Directory Service
Sends: N/A

Reads: user ids, name, email, phone, office location, department, position
Purpose: Enable assignment of users to devices enabling dynamic, custom configurations
4) Jamf School integration with a Customer's Apple School Manager
Sends: user names, email
Reads: user ids, name, email, phone, office location, department, position, device ids, IP address, classes, teachers
Purpose: Import of a school's classes, students, and teachers for dynamic management of classroom devices
5) Jamf Pro integration with Apple's Push Notification Service (out of scope for this DPIA)
Sends: device id
Reads: N/A
Purpose: Standard feature of Apple MDM, enabling Jamf management products to notify a device it needs to check in to the server
6) Device check-in to Jamf Pro (out of scope for this DPIA)
Sends: device id, IP address, other device inventory
Reads: configuration information
Purpose: Inventory and configuration of the device
7) Jamf School communication with Jamf Student
Sends: username, classes, teacher Reads: username, device ids
Purpose: Classroom management of devices for the learning environment
8) Jamf School communication with Jamf Teacher, Apple Classroom (out of scope for this DPIA)
Sends: device id, IP address, usernames, classes
Reads: usernames, device ids, student photo
Purpose: Classroom management of devices for the learning environment
9) Jamf School communication with Jamf Parent (out of scope for this DPIA)
Sends: username, registered student device id, boolean for in geofence
Reads: parent device id, IP address, parent username, location of geofence
Purpose: Configuration of student-assigned devices by parents outside of the school day

4. Verwerkingsdoeleinden

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

De verwerking moet gebonden zijn aan specifieke verzameldoelen en de verwerkingsverantwoordelijke mag ze alleen ten behoeve hiervan gebruiken. In het geval van Jamf School mag bijvoorbeeld de mogelijkheid om de vindplaats van de I-pad te tracken niet worden ingezet om als bewijs te dienen dat een leerling spijbelt. Hierbij zou het gaan om een onverenigbare verwerking.

Het is daarom aan de school om geen scheve schaats te rijden ten aanzien van de inzet van de mogelijke inzichten die Jamf School biedt.

Afwijken van het primaire doel waarvoor de gegevens zijn verzameld kan enkel wanneer er eerst wordt bekeken of dat nieuwe doel past bij het oorspronkelijke doel waarvoor we de gegevens hebben verzameld. Dit wordt een verenigbaarheidstoets genoemd[19].

De bedrijfsfunctie beheer ICT-middelen binnen de FORA[20] is omschreven als:

Het beheer van diverse soorten ict-middelen (hard- en softwarecomponenten), zoals:
- servers - netwerken - PC's, en daarop draaiende software - devices / apparatuur, zoals laptops, smartphones, tablets e.d. - werkplekken - storage- en backupsystemen - print- / kopieersystemen - telefonienetwerk - applicaties
Dit omvat ook monitoring en signalering van de juiste werking, de beschikbaarheid, de veiligheid, de capaciteit, het gebruik en de performance van de ict-middelen.

De verwerkingsdoeleinden zijn schematisch weergegeven en gekoppeld aan de verwerking

Tabel 4.1: Gegevensverwerkingen en doeleinden

Gegevensverwerking (par.3 Gegevensverwerkingen)	**Doeleinde verwerking (par.4. Verwerkingsdoeleinden)**	**Toelichting**
App-distributie setup, configuratie en beheer van apparaten en omgeving	Bij het distribueren van apps naar Apple apparaten via Jamf, kunnen persoonsgegevens zoals gebruikersnamen en e-mailadressen worden gebruikt om de juiste apps aan specifieke gebruikers toe te wijzen.	Apps, inhoud en beperkingen configureren. Dit omvat ook het instellen van beperkingen en controles om de toegang tot bepaalde apps of inhoud te beperken en het configureren van instellingen.
Beveiligingsbeheer	Een efficiënt beheer van apparaten in een educatieve omgeving mogelijk maken, zoals het managen van toegang tot (educatieve) apps, het beheren van apparaatinstellingen en het beschermen van de veiligheid en privacy van de apparaten. Uitvoering van beveiligingsbeleid zoals het afdwingen van	

[19] Artikel 6, vierde lid, AVG.
[20] Beheer ict-middelen - Funderend Onderwijs Referentie Architectuur (wikixl.nl)

	wachtwoordvereisten en het instellen van apparaatvergrendelingen.	
Monitoring en rapportage	Persoonsgegevens kunnen worden verwerkt voor monitoring- en rapportagedoeleinden, zoals het bijhouden van apparaatgebruik, het genereren van rapporten over apparaatstatus en -prestaties, en het identificeren van potentiële beveiligingsrisico's.	
Ondersteuning en klantenservice	Bij het verlenen van ondersteuning en klantenservice aan gebruikers kunnen persoonsgegevens worden verwerkt om technische problemen op te lossen, vragen te beantwoorden en algemene assistentie te bieden met betrekking tot het gebruik van Jamf en Apple apparaten	Jamf is verwerkingsverantwoordelijke voor deze verwerkingen.
Mobile device management	Op afstand kunnen apparaten van Apple worden geblokkeerd en/of gewist. Dit betekent ook dat de locatie (bij benadering) van het apparaat vastgesteld kan worden.	

5. Betrokken partijen

De hieronder genoemde organisaties zijn betrokken bij de gegevensverwerkingen.

Tabel 5.1: Betrokken partijen gegevensverwerkingen en doeleinden

Naam partij	AVG-rol	Functie/taak	Betrokken persoonsgegevens	Verstrekker of ontvanger
Jamf	Verwerker	Uitvoeren dienst	Alle binnen Jamf School verwerkte	Ontvanger

			persoonsgegevens	
Jamf	Verwerkingsverantwoordelijke	Support (technische ondersteuning)	Alle met de ticket meegestuurde gegevens maar in ieder geval mail, naam en achternaam.	Ontvanger
School	Verwerwerkingsverantwoordelijke	Faciliteren lesprogramma		Verstrekker
Amazon Web Services, Inc.	Sub-verwerker	Cloud hosting	Alle binnen Jamf School verwerkte persoonsgegevens	Ontvanger
OneSignal Inc.	Sub-verwerker	Push notificaties		Ontvanger

6. Belangen bij de gegevensverwerking

Hieronder staat de toelichting op de belangen die de genoemde betrokken partijen hebben bij de gegevensverwerkingen. Dit benoemen van belangen is relevant om de noodzaak van de verwerking te beoordelen.

Jamf, bedrijfsbelang te weten het zorgdragen van een soepele werking van de diensten en oplossingen (klanttevredenheid). Het oplossen van technische storingen en bieden van ondersteuning (support).

School, beheren en beveiligen van uitgegeven apparaten en applicaties binnen het schooldomein om zo een ononderbroken leerproces te waarborgen.

Amazon Web Services Inc, bedrijfsbelang te weten de cloud opslag waarbij alle binnen Jamf School verwerkte persoonsgegevens worden gehost.

OneSignal Inc. Bedrijfsbelang te weten de cloud opslag voor verstrekken pushnotificaties binnen Jamf School.

7. Verwerkingslocaties

De gegevensverwerking vindt plaats in de volgende landen.

Tabel 7.1: Verwerkingslocaties

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 Inc.	Verenigde staten	Cloud Hosting	Duitsland
OneSignal Inc.	Verenigde staten	Push notificaties	Nederland

Jamf als verwerkingsverantwoordelijke
Jamf is verwerkingsverantwoordelijke voor wat betreft de afhandeling van de ingediende rechten van betrokkenen en ingeschoten tickets bij de support afdeling ten behoeve van (technische) ondersteuning. Omdat hier geen controle is over de verwerkte persoonsgegevens het advies om in de communicatie met Jamf geen persoonsgegevens, anders dan de noodzakelijke t.b.v. de afhandeling van het verzoek, mee te sturen.

Jamf maakt gebruik van de volgende verwerkers21 ten behoeve van de taken waarvoor zij zichzelf als verwerkingsverantwoordelijke aanmerkt:

> Jamf may engage vendors to provide services on our behalf. Any vendor who may process Customer Content, as defined in Jamf's Software License and Services Agreement (SLASA), are considered sub-processors and are disclosed below. As set forth in Jamf's Data Processing Agreement (DPA), Jamf has adequate data transfer mechanisms in place with each sub-processor.

Sub-processor	Location(s) of processing	Purpose of processing
Dropbox	United States	Secure data sharing
Microsoft Corporation	United States	Email communication
Salesforce	Ireland*, United States	Customer relationship management
ServiceNow	United States	Customer support case management
Zoom Video Communications	United States	Online meetings

8. Beoordeling uitvoeren Data Transfer Impact Assessment (DTIA)

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

[21] https://resources.jamf.com/images/corporate-responsibility/Sub-processors-support.pdf

Jamf verwerkt als verwerker de persoonsgegevens in het Duitse datacenter van het Amerikaanse bedrijf AWS. Als verwerkingsverantwoordelijke verwerkt Jamf buiten Europa persoonsgegevens ten behoeve van het bieden van ondersteuning op het gebied van rechten van betrokkenen, support en mailcontact in het kader van relatiemanagement en verkoop.

Op 10 juli 2023 heeft de EC (Europese Commissie) het adequaatheidsbesluit voor het nieuwe Data Privacy Framework (DPF) tussen de EU en Verenigde Staten (VS) aangenomen. Het Framework is de opvolger van het eerdere EU-VS Privacy Shield dat door het Europese Hof van Justitie met haar Schrems II-uitspraak in 2020 ongeldig werd verklaard, omdat de rechten van Europese burgers onvoldoende beschermd waren. De Europese Commissie heeft bepaald dat dit met het nieuwe Framework is opgelost. Dat betekent dat organisaties binnen de EER op basis van het nieuwe besluit veilig persoonsgegevens kunnen doorgeven aan bedrijven in de VS die deelnemen aan het nieuwe Framework.

Amazon Webservices en Onesignal, hoewel de datacenters in Duitsland en Nederland staan, zijn aangesloten bij het nieuwe DPF. Zie: https://www.dataprivacyframework.gov/s/participant-search.

De verwerkers die Jamf gebruikt ten behoeve van hun rol als verwerkingsverantwoordelijke zijn eveneens bij gecertificeerd bij het DPF.

Geen DTIA nodig
Op basis van het recente adequaatheidsbesluit van de Europese Commissie met betrekking tot het DPF tussen de EU en de Verenigde Staten en gezien het feit dat Jamf gegevens verwerkt binnen de EU via dienstverleners die gecertificeerd zijn onder het nieuwe DPF, waaronder Amazon Web Services en OneSignal, die bovendien hun datacenters hebben in Duitsland en Nederland, is een DTIA niet noodzakelijk geacht. Ook het ontbreken van de verwerking van gevoelige of bijzondere persoonsgegevens draagt bij aan de veronderstelling dat voornoemde mechanisme voldoende is om de overdracht op te kunnen baseren en er geen aanvullende verplichtingen gesteld hoeven te worden.

Er wordt voldoende gewaarborgd dat de algemene persoonsgegevens veilig kunnen worden overgedragen aan bedrijven in de Verenigde Staten die deelnemen aan het nieuwe Framework, waardoor wordt voldaan aan de vereisten voor gegevensoverdracht buiten de EER onder de AVG.

9. Technieken en methoden van gegevensverwerking

Artikel 32 van de AVG[22] schrijft voor dat er passende technische en organisatorische maatregelen genomen moeten worden om een op het risico afgestemd beveiligingsniveau te waarborgen. Om inzicht te krijgen in welke mate er vorm wordt gegeven aan deze abstracte formulering wordt gebruik gemaakt van de voor de verwerkers opgestelde standaard DPIA-vragenlijst. Deze vragenlijst wordt door de verwerker gevuld en zal voor een

[22] Artikel 32 EU algemene verordening gegevensbescherming (EU-AVG). Privacy/Privazy according to plan. (privacy-regulation.eu)

belangrijk deel inzicht geven in o.a. de genomen technische beheersmaatregelen en informatiebeveiliging.

Beveiligingsadvies

In september 2023 heeft een globaal onderzoek plaatsgevonden naar de status van informatiebeveiliging van de applicatie Jamf. Dit onderzoek is gebaseerd op informatie door Jamf via hun website verstrekt en de aangeleverde vragenlijst. Het betreft geen technisch onderzoek naar het implementatieniveau van beveiliging. Daarnaast heeft dit onderzoek focus naar veiligheid van de applicatie en niet op veiligheid van de beherende organisatie.

Onderzoek

Voor dit onderzoek is de volgende informatie verkregen:

- Jamf is ISO27001 gecertificeerd.
  - Scope: “The certificate scope comprises the Information Security Management System (ISMS) and Privacy Information Management System (PIMS) supporting the operations underlying the infrastructure, management, and administration of the Jamf Now, Jamf Pro, Jamf School, Jamf Protect, Jamf Private Access, Jamf Data Policy, and Jamf Threat Defense product offerings. These activities are governed by the Statement of Applicability based on ISO/IEC 27001:2013 as extended by the Controller and Processor controls described within ISO/IEC 27701:2019. This organizational scope includes the Information Security, Corporate Information Technology, Software Development, Cloud and Delivery, Technical Support, and Legal and Compliance teams affecting the ISMS and PIMS.”
  - Oorspronkelijke registratie 4 mei 2020, meest recente audit 2 mei 2023
  - Looptijd certificaat tot 4 mei 2026
  - Verklaring van toepassing v1.8 van 13-03-2023. Alle punten zijn van toepassing verklaard muv 14.2.7 “Outsourced Development”. Argumentatie is dat alle software ontwikkeling intern plaats vindt en niets extern: “Jamf does not outsource the development of sourcecode to external parties. All code is developed in-house.”

- Jamf is SOC 2 gecertificeerd. SOC 2 is een assurance verklaring vergelijkbaar met ISAE 3402, alleen is deze niet gebonden aan de financiële verslaggeving van de klant. De inhoud van SOC 2 wordt bepaald door de Trust Services Criteria, een verplichte set aan beheersdoelstellingen. Door deze verplichte set gaat SOC 2 een stap verder dan ISAE 3000. Deze ISAE 3000 wordt in Nederland veel gehanteerd voor het verlenen van assurance over uitbestede IT / data processen.

  Het audit onderzoek heeft plaats gevonden over de periode 1-10-2021 tot 30-09-2022. Het audit verslag is beschikbaar.

- Jamf voert jaarlijks een pentest uit door een externe security bedrijf.
    - Scope van de pentest is de Web Application for JamfPro. “The goal of the assessment was to determine if attackers could gain unauthorized access to sensitive data, and to ensure that Jamf developers follow security industry best practices in order to prevent common vulnerabilities such as the OWASP Top 10 2021.”
    - Geen severe vulnerabilities geconstateerd. Wel een hoog risico en een medium risico welke direct na de constatering zijn verholpen.
    - Naast de jaarlijkse pen test worden ook voor vrijgave van een nieuwe release een geautomatiseerde pentest en kwetsbaarheden scan uitgevoerd.

- Jamf conformeert zich aan de CSA (Cloud Security Alliance) vereisten (Level 1).

  De CSA STAR-certificering is een externe onafhankelijke beoordeling van de beveiliging van een cloud serviceprovider. De certificering maakt gebruik van de vereisten van het ISO/ IEC 27001-beheersysteemstandaard samen met de CSA Cloud Controls Matrix, een specifieke reeks van bijna 200 criteria die de volwassenheidsniveaus van de cloudservice meet.

  Het betreft een level 1 verklaring waarbij in de vorm van een self assessment aangegeven is dat ze aan de vereisten voldoen. De eerste registratie is van 6 mei 2021 en de meest recente update is van 29 april 2022. Bij level 2 is een externe accountant verklaring nodig en kan een certificaat verkregen worden.

Conclusies

Jamf is al sinds mei 2020 ISO27001 gecertificeerd. Hierbij is zowel het hoofdkantoor van Jamf inclusief andere vestigingen in scope. Alhoewel een onderdeel van de VVT niet van toepassing is verklaard is dit verklaarbaar en doet geen afbreuk aan het certificaat. Het certificaat is onlangs verlengt tot mei 2026.

Naast ISO27001 certificaat is het bedrijf SOC 2 geaccrediteerd en conformeert zich aan de CSA Start vereisten.

Door het voldoen aan diverse internationale beveiligingsvereisten kan de conclusie getrokken worden dat beveiliging serieus wordt toegepast door Jamf en aan diverse internationale normen voldoet.

Aanbevelingen

Gezien het hoge volwassenheidsniveau zijn er geen risico’s of aanbevelingen voor Jamf geïdentificeerd.

Overview Jamf School security https://security.jamf.com/

Configuratie

Jamf School kent oneindig veel instellingen om Apple appraten te beheren. We adviseren een configuratie en security baseline vast te stellen voor devices voor gebruik binnen de school en erop toe te zien dat deze gehandhaafd wordt. Hiervoor kunnen scholen bijvoorbeeld de CIS security benchmark[23] gebruiken. Norm 11.1 van het normenkader IBP schrijft bovendien voor dat scholen een security baseline vaststellen.

De Jamf compliance editor is een tools om dit beheer automatisch te doen. Voor meer informatie zie -> https://cdn.document360.io/e5d71abd-07b9-46d0-8876-03cc9073df6b/Images/Documentation/Jamf%20Compliance%20Editor%20-%20User%20Guide%2811%29.pdf?sv=2019-07-07&sig=aGTfS1xrZJsxU%2FNLp8GUsRpaEWExO48wYeHDzOJq2qM%3D&spr=https%2Chttp&st=2023-11-21T14%3A43%3A09Z&se=2023-11-21T14%3A53%3A09Z&srt=o&ss=b&sp=r

Met Jamf School kunnen beheerders auditlogbestanden bekijken voor de 500 meest recente commando's die zijn verstuurd naar computers en mobiele apparaten

10. Juridisch en beleidsmatig kader

Onderstaande tabel geeft vorm aan de juridische en beleidsmatige fundamenten ten aanzien van het gebruik van een mobiele device management (MDM) oplossing binnen het onderwijs. De hieruit voortkomende verwerking van persoonsgegevens zijn inherent aan het doel van de verwerking, namelijk het beheren van door de school uitgegeven apparaten. Vervolgens is het gebruik van Jamf School weer faciliterend aan de meer algemene onderwijsdoelen waaronder het doorlopen van ononderbroken onderwijs respectievelijk ontwikkelproces.
Het Normenkader[24] wordt op termijn een verplichting voor schoolbesturen om aan te voldoen. De relevante waarborgen die de MDM-oplossing raken zijn daarom ook opgenomen in dit overzicht.

Tabel 10.1: Juridisch en/of beleidsmatig kader

Gegevensverwerkingen	Juridisch en/of beleidsmatig kader	Wetsartikelen
Faciliteren toegang tot aanbod leermateriaal	Wet op het primair onderwijs t.b.v. doorlopen ononderbroken onderwijs	o.a. Artikel 8 en 182, lid 12
Faciliteren toegang tot aanbod leermateriaal	Wet voortgezet onderwijs 2020 t.b.v. doorlopen ononderbroken ontwikkelproces.	o.a. Artikel 1.4, lid 2 en 8.17, lid 10
Faciliteren toegang tot aanbod leermateriaal	Normenkader IBP	Hoofdstuk 10, Identity & Access Management
Logging	Normenkader IBP	Hoofdstuk 11.4 Security Management

[23] https://www.cisecurity.org/benchmark/apple_os
[24] https://aanpakibp.kennisnet.nl/app/uploads/Normenkader-IBP.pdf

11. Bewaartermijnen

De bewaartermijn van de binnen Jamf School te verwerken data is door de gebruiker te bepalen. Het is dus aan de scholen om termijnen in te regelen die in overeenstemming zijn met de AVG. Voor wat betreft de back-ups worden deze na 30 dagen verwijderd uit de database.

Een veel voorkomende situatie is de voormalig leerling of leerkracht die niet langer gebruik maakt van de diensten van Jamf. De verwerkingen die gedurende het gebruik hebben plaatsgevonden zullen in het geval van de standaard instellingen automatisch verwijderd worden. Zolang een gebruiker is aangemaakt is er data. Wanneer het wenselijk wordt geacht om userdata te verwijderen dan kan deze rol worden uitgeschreven uit het Jamf platform.
De data die gedurende het gebruik van bijvoorbeeld een leerling of leerkracht binnen Jamf School aanwezig zijn hebben voornamelijk betrekking op: Naam, mailadres, soort apparaat, welke apps erop staan en hoe de configuratie is vormgegeven. De gevoeligheid van de gegevens en de aard van de verwerking is derhalve laag te noemen.

Uitschrijven
Het volledig loskoppelen van het apparaat aan het beheer onder Jamf School kan door middel van het uitschrijven van het apparaat[25]. Bij dit uitschrijfproces worden het MDM-profiel en alle geïnstalleerde profielen verwijderd. Apps die ”onder beheer” zijn geïnstalleerd zullen in dat geval bij het uitschrijven ook worden verwijderd. Wanneer het apparaat niet langer beheerd wordt kan deze volledig uit Jamf School worden verwijderd. Er kunnen vervolgens geen beheertaken meer worden uitgevoerd totdat het apparaat weer is ingeschreven.

Loggegevens worden standaard 12 maanden bewaard.

Back-up beleid uitgelegd door Jamf
Jamf voert regelmatig geplande back-ups uit van de gehoste services (elke 24 uur) en bewaart de back-ups op basis van dertig (30) dagen, maar garandeert niet de beschikbaarheid van back-ups na de dertig (30) dagen waarvoor ze worden bewaard, en onderhoudt geen historische back-upkopieën van de gehoste services voor het doel van herstel van gegevens op een specifiek tijdstip of archivering.

Na beëindiging van het contract met Jamf zal de afdeling Jamf Customer Succes de customer's data verwijderen binnen 30 dagen.

Jamf geeft in het Privacybeleid[26] op haar beurt aan persoonsgegeven zo lang als nodig te

[25] Apparaten verwijderen uit Jamf School - Jamf School-documentatie | Jamf
[26] https://www.jamf.com/nl/privacybeleid/

bewaren in het licht van de doeleinden waarvoor ze zijn verzameld. Criteria hiervoor zijn onder meer:

- De duur van de doorlopende relatie;
- De aanwezigheid van een wettelijke verplichting;
- De juridische positie van Jamf (zoals verjaringstermijnen, rechtszaken of onderzoeken van regelgevende instanties).

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

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

Artikel 6 AVG lid

a) Toestemming van de betrokkene
b) Uitvoering van een overeenkomst
c) Wettelijke verplichting[27]
d) Vitaal belang van de betrokkene
e) Taak van algemeen belang[28] (of openbaar gezag)
f) Gerechtvaardigd belang

Jamf School kwalificeert zichzelf voor de verwerkingen die binnen de applicatie plaatsvinden hoofdzakelijk als verwerker. Uitzondering hierop is de rol die zij vervullen tijdens het verlenen van, klantbeheer, verkoop, technische ondersteuning en uitvoering rechten van betrokkenen. Meer hierover in hoofdstuk 3.

De scholen zijn verwerkingsverantwoordelijke voor de overige verwerkingen die binnen Jamf School plaatsvinden. Hiervoor is een grondslag als bedoeld in artikel 6 van de AVG een noodzakelijke voorwaarde. Er kan aansluiting gevonden worden bij de grondslag onder artikel 6, eerste lid, sub e, te weten de uitvoering van een taak van algemeen belang die de scholen uitvoeren in het geven van onderwijs.
Dit betekent dat de verwerkingen van persoonsgegevens ten behoeve van het doel waarvoor Jamf School wordt ingezet gerechtvaardigd is omdat dit deel uitmaakt van de essentiële taken van onderwijsinstellingen om onderwijs te geven.
Het gebruik maken van oplossingen die ondersteunend zijn aan het primaire onderwijsproces van onderwijsinstellingen vinden plaats onder diezelfde verwerkingsgrondslag.

[27] 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.
[28] 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.

Voor wat betreft de verwerking van persoonsgegevens binnen Jamf School, wordt in het onderstaande uiteengezet wat de regels zijn omtrent het aanbieden van leermiddelen in het primair onderwijs (hierna: po) en het voortgezet onderwijs (hierna: vo), de juridische basis hiervoor en in het verlengde daarvan de verwerking van persoonsgegevens.

Uitgangspunten en doelstelling onderwijs

Zowel binnen de Wet op het primair (WPO) onderwijs als de Wet op het voortgezet onderwijs (WVO) staat het volgende centraal:

Het onderwijs wordt zodanig ingericht dat de leerlingen een ononderbroken ontwikkelingsproces kunnen doorlopen. Het wordt afgestemd op de voortgang in de ontwikkeling van de leerlingen.

Naast de in de WPO genoemde inhoud en de WVO genoemde kerndoelen waar het onderwijs aan moet voldoen hebben scholen een ruime vrijheid om te voorzien in het bieden van de hierbij passende leermiddelen die hieraan ondersteunend zijn. Dit kunnen bijvoorbeeld fysieke boeken zijn, digitale applicaties en alles daartussenin. Vanuit zowel de WPO als de WVO is het scholen verplicht om de voortgang van de leerlingen op verschillende onderdelen bij te houden. Deze vorm van monitoring vindt niet zelden digitaal plaats en ook leerlingen zelf krijgen hier regelmatig toegang tot hun vorderingen.

Verwerking van persoonsgegevens met behulp van (digitale) onderwijsmiddelen door onderwijsinstellingen vindt plaats ten behoeve van het verzorgen van onderwijs, waaronder het voorbereiden, uitvoeren, evalueren en ondersteunen van het onderwijs(proces) en het begeleiden en volgen van onderwijsdeelnemers (in hun leerproces). Dit is een (wettelijke) kernactiviteit van scholen in het po en vo.

Artikel 182 lid 12 van de Wet op het primair onderwijs (hierna: WPO) geeft aan dat:

Het bevoegd gezag kan het pseudoniem, bedoeld in het elfde lid, gebruiken voor het genereren van een ander pseudoniem voor een leerling in het kader van de toegang tot en het gebruik van digitale leermiddelen of het digitaal afnemen van toetsen, waarbij het bevoegd gezag er zorg voor draagt dat dit andere pseudoniem wordt bewaard in de systemen waarin de leerlingen zijn geregistreerd. Dit andere pseudoniem wordt uitsluitend verstrekt aan een leverancier die een digitaal product of een digitale dienst aanbiedt bestaande uit leerstof of toetsen en de daarmee samenhangende digitale diensten.

Artikel 8.17, lid 10 van de Wet Voortgezet onderwijs 2020 (hierna: WVO) geeft bijna identiek aan dat:

Het bevoegd gezag kan het pseudoniem gebruiken voor het genereren van een ander pseudoniem voor een leerling in het kader van de toegang tot en het gebruik van digitale leermiddelen of het digitaal afnemen van toetsen en examens, waarbij het bevoegd gezag er zorg voor draagt dat dit andere pseudoniem wordt bewaard in de systemen waarin de leerlingen zijn geregistreerd. Dit andere pseudoniem wordt uitsluitend verstrekt aan een leverancier die een digitaal product of een digitale dienst aanbiedt bestaande uit leerstof of toetsen en de daarmee samenhangende digitale diensten.

Dit geeft (indirect) aan dat een onderwijsinstelling in het kader van haar taken zoals bedoeld in de WPO en WVO, namelijk het geven van onderwijs, digitale leermiddelen mag inzetten en daarbij gebruik kan maken van ondersteunende digitale diensten (zoals Jamf School).

Het behoort tot de verantwoordelijkheid van de school om er voor zorg te dragen dat de leerlingen een ononderbroken ontwikkelingsproces kunnen doorlopen. Ondersteunend aan dit proces is het in gebruik nemen van een mobile device management oplossing zoals Jamf School.

Passende maatregelen

De AVG schrijft voor dat de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen moeten nemen om de gegevensverwerking op een veilige manier te laten plaatsvinden.

Jamf School levert een veilige MDM-oplossing waardoor leerlingen (en medewerkers) op een veilige en uniforme manier toegang krijgen tot de aanbieders van digitale (leer)middelen. Op deze manier wordt ten aanzien van het uitgeven van Apple apparaten vormgegeven aan de vereisten van artikel 32 AVG.

Tabel 12.1: Grondslag AVG

Verwerking/doeleinde (zie hiervoor 4. Verwerkingsdoeleinden)	**Grondslag AVG**	**Toelichting**
Het in gebruik nemen van een MDM-oplossing ten behoeve van het beheer van uitgegeven Apple apparaten.	Artikel 6, eerste lid, onder e Taak van algemeen belang jo Artikel 8 en 182, lid 2 Wet op het primair onderwijs en artikel 8.17, lid 10 Wet op het voortgezet onderwijs 2020	De onderwijssector mag zich voor de uitvoering van uiteenlopende taken beroepen op het algemeen belang als verwerkingsgrondslag t.b.v. de noodzakelijke verwerkingen

13. Bijzondere persoonsgegevens

Binnen het gebruik van Jamf School worden geen bijzondere, strafrechtelijke of gevoelige persoonsgegevens verwerkt.
De scope van de DPIA ziet op door de school uitgegeven en beheerde Apple apparaten die enkel voor onderwijsdoeleinden beschikbaar worden gesteld en hierdoor niet kunnen worden gebruikt voor het downloaden van andere apps dan die vanuit de schoolinstelling worden geïnstalleerd. Het installeren van privé apps waaruit bijvoorbeeld geloofsovertuiging, seksuele gezindheid of politieke voorkeur blijkt is simpelweg niet mogelijk wanneer de instellingen dat niet toelaten. In dit geval doen zich geen risico's voor die verband houden met de verwerking van deze als bijzondere persoonsgegevens aan te merken applicaties, vanuit de rollen die daar toegang toe hebben zoals een applicatiebeheerder.

14. Kinderrechten-afweging (Best Interests Assessment Children)

Artikel 3 van het Verdrag inzake de rechten van het kind, schrijft voor dat bij alle maatregelen betreffende kinderen - ongeacht of deze worden genomen door openbare of particuliere instellingen, rechterlijke instanties, bestuurlijke autoriteiten of wetgevende lichamen - de belangen van het kind de eerste overweging (moeten) vormen. Deze belangenafweging gaat verder dan een veilige gegevensverwerking maar ziet ook op de mogelijke gevolgen van de verwerking. Met schoolbesturen als leden van SIVON in het primair en voortgezet onderwijs, betekent dit dat SIVON in haar DPIA's rekening houdt met o.a. gebruikers (betrokkenen) in de leeftijd van 4 tot 18 jaar (of ouder). Kinderen hebben recht op specifieke bescherming van hun persoonsgegevens. Dit volgt uit het feit dat zij zich minder bewust zijn van de risico's, gevolgen en waarborgen en van hun rechten in verband met de verwerking van hun persoonsgegevens. SIVON geeft hier in deze DPIA invulling aan door af te wegen of het gebruik van het Jamf School en de gegevensverwerking(en) die daarmee samenhangen, in het belang zijn van de betrokkenen (kind/leerling als betrokkene). SIVON maakt hierbij gebruik van de systematiek van de best interests assessment children van de Britse ICO[29]. De afweging bestaat uit 4 stappen:

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

Hieronder wordt beschreven welke rechten[i30] van en voor kinderen relevant zijn in het kader van deze DPIA. Van belang is de leeftijd van de kinderen (leeftijdsadequaat). Hierbij wordt nagegaan of de gegevensverwerking (negatieve) gevolgen heeft voor de ondersteuning en van de behoeften van het kind op het gebied van veiligheid, gezondheid, welzijn, familierelaties, fysieke, psychologische en emotionele ontwikkeling, identiteit, vrijwaring van economische commerciële en/of fysieke uitbuiting, vrijheid van meningsuiting, privacy en de mogelijkheid om een eigen mening te vormen en deze te laten horen, het belang van toegang tot informatie, omgang met anderen en spel (buiten spelen) om de ontwikkeling van het kind te ondersteunen. Het gaat erom dat het kind in overeenstemming met zijn of haar ontwikkelende capaciteiten, een stem heeft (kan hebben) in zaken die hem of haar aangaan.

Jamf School wordt gebruikt om Apple apparaten van kinderen te kunnen beheren. In potentie kan een commerciële goudmijn aan data geoogst worden indien aan het gebruik van Jamf School in het geheel geen beperkingen zouden zijn gesteld. In een dergelijk geval zouden er allerhande kinderrechten worden geschonden hetgeen deze MDM-oplossing als inherent onrechtmatig zou classificeren. We leggen deze verwerking tegen de lat van relevante kinderrechten criteria. Hierbij kijken we onder meer naar of het gebruik van de applicatie leeftijdsadequaat en dus past bij de leeftijd van de leerlingen. De leeftijdscategorie en de verschillende behoeften van kinderen van verschillende leeftijden

[29] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/best-interests-self-assessment/
[30] https://wetten.overheid.nl/BWBV0002508/2002-11-18#Verdrag_2

en ontwikkelingsstadia moeten centraal staan bij het gebruik van Jamf School en de daarmee samenhangende gegevensverwerkingen.

Naast dat de waarborging van de privacy van zowel de leerlingen als leerkrachten van groot belang is zijn er de volgende rechten die voor dergelijk kwetsbare doelgroepen getoetst worden.

De onderstaande rechten komen terug in regelgeving en in het Verdrag inzake de Rechten van het Kind (IVRK) en zijn van toepassing op Jamf School:

- Het recht op privacy wordt geëerbiedigd;
- Persoonlijke gegevens worden beschermd;
- Kinderen worden niet onderworpen aan willekeurige of onrechtmatige inmenging in hun privéleven;
- Kinderen worden beschermd tegen beslissingen op basis van automatische verwerking van gegevens, als die hun kansen of vrijheden significant kunnen beïnvloeden;
- Er moet een mogelijkheid zijn voor menselijk ingrijpen, waarbij kinderen of hun voogden de kans krijgen om hun standpunt te uiten en de beslissing aan te vechten.

Het gaat erom dat de gegevensverwerkingen uiteindelijk niet onverenigbaar mogen zijn met een van de hierboven te beschermen belangen.

2. Identificeer het effect van de gegevensverwerking en gebruik van Jamf School op deze rechten

De toepassing van Jamf School lijkt geen (negatieve) gevolgen te hebben voor de ondersteuning en van de behoeften van het kind op het gebied van veiligheid, gezondheid, welzijn, familierelaties, fysieke, psychologische en emotionele ontwikkeling, identiteit, vrijwaring van economische commerciële en/of fysieke uitbuiting, vrijheid van meningsuiting, privacy en de mogelijkheid om een eigen mening te vormen en deze te laten horen, het belang van toegang tot informatie, omgang met anderen en spel (buiten spelen) om de ontwikkeling van het kind te ondersteunen.

Het gebruik van Jamf School, waarbij het mogelijk is voor de applicatiebeheerder om de locatie van een apparaat te zien, kan een risico met zich meebrengen met betrekking tot geolocatie-tracking, zoals beschreven in de Children's Code Geolocation-standaard[31]. Geolocatie-tracking houdt in hoe online diensten de geolocatiegegevens van kinderen monitoren en gebruiken, meestal afkomstig van het apparaat van de gebruiker en aangeeft waar dat apparaat zich geografisch bevindt. Dit omvat in het geval van Jamf School IP-adresgegevens. Een belangrijk aspect van deze technische trackingmogelijkheid is wie hiervoor ten behoeve van welke doeleinden gebruik kan maken. Ten eerste kan geolocatie-

[31] Code standards | ICO **10 Geolocation**: Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child). Provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to 'off' at the end of each session.

tracking de rechten van kinderen beïnvloeden met betrekking tot artikel 6 van het VN-Verdrag inzake de Rechten van het Kind, dat het recht op leven, overleven en ontwikkeling beschermt[32]. Het delen van deze gegevens met andere gebruikers, vooral als dit standaard ingeschakeld is, niet duidelijk is voor het kind wanneer het wordt gebruikt, of niet automatisch weer wordt uitgeschakeld na gebruik, kan kinderen blootstellen aan risico's van fysieke of emotionele schade, zoals stalking, pesten of intimidatie. Aan de andere kant kan geolocatie-tracking dit recht ondersteunen wanneer het wordt gebruikt voor bescherming en ouderlijk toezicht.

Ten tweede kan geolocatie-tracking de vrijheid van vereniging van kinderen beïnvloeden, zoals beschreven in artikel 15 van het VN-Verdrag inzake de Rechten van het Kind. Het gebruik van ouderlijke controle voor het volgen van de bewegingen van kinderen zonder voldoende transparantie voor het kind kan dit recht schenden.

Ten derde kan geolocatie-tracking het recht van kinderen op bescherming tegen geweld, misbruik en verwaarlozing beïnvloeden, zoals beschreven in artikel 19 van het VN-Verdrag inzake de Rechten van het Kind. Opnieuw kan het delen van deze gegevens met andere gebruikers, vooral als dit standaard ingeschakeld is, niet duidelijk is voor het kind wanneer het wordt gebruikt, of niet automatisch weer wordt uitgeschakeld na gebruik, kinderen blootstellen aan risico's van geweld of misbruik, zoals stalking, pesten of intimidatie. Maar geolocatie-tracking kan dit recht ook ondersteunen wanneer het wordt gebruikt voor bescherming en ouderlijk toezicht.

Om deze risico's te minimaliseren, moeten online diensten zoals Jamf School zich houden aan de verwachtingen en normen zoals uiteengezet in de Children's Code Geolocation-standaard. Dit omvat het bieden van duidelijke opties en transparantie aan gebruikers, met name kinderen, over het gebruik van geolocatiegegevens en het implementeren van veiligheidsmaatregelen om de privacy en veiligheid van kinderen te waarborgen.

3. Beoordeel of dit effect wenselijk is

Hoewel het gebruik van Jamf School over het algemeen geen negatieve gevolgen lijkt te hebben voor de ondersteuning en behoeften van het kind, moeten we ons bewust zijn van het risico van geolocatie-tracking. Dit kan het recht van kinderen op privacy, bescherming tegen geweld en misbruik, en vrijheid van vereniging beïnvloeden. Om deze risico's te minimaliseren moet gekeken worden naar de toegangsmogelijkheden tot deze data en het eventuele gebruik daarvan. In de praktijk blijkt dit mee te vallen gezien toegang hiertoe beperkt is tot de enkel de door de school aangewezen rollen.
Wanneer de hypothetische situaties van ongewenste en onbevoegde toegang tot de

32 https://www.kinderrechten.nl/verdragstekst/#:~:text=Artikel%206%3A%20Leven%20en%20ontwikkeling&text=De%20Staten%20die%20partij%20zijn%2C%20erkennen%20dat%20ieder%20kind%20het,de%20ontwikkeling%20van%20het%20kind.
Artikel 6: Leven en ontwikkeling 1. De Staten die partij zijn, erkennen dat ieder kind het inherente recht op leven heeft. 2. De Staten die partij zijn, waarborgen in de ruimst mogelijke mate de mogelijkheden tot overleven en de ontwikkeling van het kind.

geolocatie van de eindgebruikers worden afgezet tegen de kans, waarschijnlijkheid, impact en ernst van mogelijke gevolgen van de rechten van het kind dan is de kans eenvoudig laag te noemen.

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

Er is geen noodzaak om aanvullende maatregelen te nemen om de rechten van het kind te beschermen. De effecten die de gegevensverwerkingen binnen Jamf School hebben op de kinderrechten zijn over een brede linie tegen het licht gehouden en lijken hier niet een niet te rechtvaardigen inbreuk op te maken. Met betrekking tot het enige potentiële risico, namelijk toegang tot de locatie van het Apple apparaat, vermeldt Jamf School dat zij hier geen toegang toe heeft. Bovendien wordt in hun privacybeleid expliciet vermeld dat deze gegevens niet worden gedeeld met derden. Het is dus hoofdzakelijk aan de school zelf om beleid op te stellen ten aanzien van het verkrijgen van toegang tot deze informatie. Een stukje uitgeschreven doelbinding zou daarbij kaders kunnen bieden in welke gevallen de locatiegegevens van de apparaten opgevraagd kunnen worden. Bijvoorbeeld wanneer een apparaat kwijt, verloren of gestolen is.

Jamf school ter voorkoming online pesten
Jamf School kan effectief bijdragen aan het voorkomen van online pesten door verschillende functionaliteiten en beveiligingsmaatregelen te bieden die een veilige digitale omgeving bevorderen. Allereerst stelt Jamf School beheerders in staat om controle uit te oefenen over de applicaties die op de apparaten van leerlingen worden geïnstalleerd, waardoor de kans op het gebruik van potentieel schadelijke of ongepaste apps kan worden verminderd.

15. Doelbinding

Doelbinding als uitgangspunt opgenomen in de AVG houdt in dat data alleen verzamelt mag worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en niet verder mag worden verwerkt op een manier die onverenigbaar is met die doelen[33].
De facto betekent dit dat de schoolinstelling de doelen waarvoor persoonsgegevens worden verzameld specificeert en deze persoonsgegevens enkel voor dat specifieke doel mag gebruiken. In het geval van Jamf School ligt het zwaartepunt op het beheren van de uitgegeven Apple apparaten en ervoor zorgen dat de leerlingen en leerkrachten de juiste digitale (leer) middelen kunnen gebruiken. Het kunnen volgen van apparaten is handig voor de situatie wanneer een leerling zijn/haar Ipad kwijt is maar het is zeer onwenselijk om buiten die situaties de vindplaats van de Ipad te tracken. Het is daarom aan de schoolinstellingen om beleid op te stellen ten aanzien van het gebruik van het opvragen van locatiedata van de beheerde apparaten. Daar waar de Ipad is, is niet zelden ook de leerling. Er moeten derhalve grenzen worden gesteld aan deze specifieke “vind het apparaat” functie en die moet ook transparant zijn zodat wordt voorkomen dat er een situatie ontstaat van een niet te rechtvaardigen aantasting van de privacy.

[33] Artikel 5, eerste lid, onder b, AVG.

De gedetailleerdheid van de inzichten van het gebruik van de apparaten is van beperkte aard hetgeen niet snel zal leiden tot het risico op een *chilling effect* op leerlingen. Een dergelijk effect zal zijn intrede doen wanneer een leerling zijn gedrag gaat aanpassen vanwege het sterk ontstane gevoel in de gaten gehouden te worden.

Het meekijken met de leerling of leerkracht zonder dat deze dat weet of het verkrijgen van gedetailleerde informatie ten aanzien van de online tijd op een (leer)applicatie is niet inzichtelijk voor een leerkracht of applicatiebeheerder.

Monitoring medewerkers
Het is van groot belang om informatievoorziening te bieden aan medewerkers van scholen die gebruik maken van beheerde Apple apparaten ten aanzien van de eventuele tracking en gegevensverwerkingen die plaatsvinden. Ook wanneer er geen gebruik wordt gemaakt van potentiële monitoringsmogelijkheden dient hier over te worden gecommuniceerd.

Kijkende naar de mate van gebruikersinformatie die de rol met de meeste rechten kan verwerven is het risico op onrechtmatige monitoring klein te noemen. Om concreet te gaan is de volgende informatie beschikbaar voor een administrator:

- Alle informatie over de hardware
- Datum en tijd laatst ingelogd
- Batterijlevel
- Geïnstalleerde applicaties
- Mac/IP-adres
- Locatie op basis van IP-adres

Gelet op het DPIA-onderzoek, de aard en het doel van de gegevensverwerking zijn er geen aanknopingspunten om te veronderstellen dat er voor scholen veel mogelijkheden zijn om de gegevens voor andere doeleinden te gebruiken. De MDM-oplossing verzamelt, verwerkt en deelt persoonsgegevens alleen met als doel om het beheer op de apparaten op de juiste manier vorm te geven. Wanneer de gegevens uitsluitend worden gebruikt voor het doel waarvoor ze oorspronkelijk waren verzameld en de gegevens niet worden gebruikt voor andere toepassingen dan het oorspronkelijke doel hoeven scholen geen afzonderlijke onderzoeken uit te voeren ten aanzien van de rechtmatigheid van de verdere verwerking. Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld dient beoordeeld te worden of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. Het is aan de school zelf om een dergelijke afweging te maken.

16 a. Noodzakelijkheid

Persoonsgegevens mogen worden verwerkt als dit noodzakelijk is voor de vervulling van een taak in het algemeen belang. De verwerking moet in deze gevallen altijd een grondslag hebben in het recht van de EU of in Nederlands recht. Jamf School is ondersteunend aan het door schoolbesturen uit te voeren primaire proces. Dit bestaat uit het inrichten van het onderwijs op een manier dat de leerlingen een ononderbroken ontwikkelingsproces kunnen

doorlopen[34]. Of de gegevensverwerking die ten behoeve van dit proces binnen Jamf School plaatsvindt noodzakelijk is dient mede beantwoord te worden aan de hand van de vraag of het de toets van de proportionaliteit en subsidiariteit kan doorstaan.

16. b. Proportionaliteit en subsidiariteit

In dit hoofdstuk zal de afweging worden gemaakt tussen de inbreuk op de persoonlijke levenssfeer en de bescherming van persoonsgegevens enerzijds, en de evenredigheid ten opzichte van de verwerkingsdoeleinden anderzijds.

Proportionaliteit

De binnen Jamf School gebruikte persoonsgegevens sluiten aan bij het uitgangspunt van dataminimalisatie. Er worden niet meer gegevens gebruikt ten behoeve van het doel dan nodig. Dit is voor een belangrijk deel ingegeven door de toezegging van Jamf om voor de educatieve sector specifieke afspraken overeen te komen ten aanzien van de beperking van de verwerkingen voor eigen onduidelijke doeleinden zoals bedoeld in artikel 19 a en b van de Software License and Software Agreement (SLASA)[35].
Er is vanuit Jamf School geen toegang tot de content data die binnen de verschillende beheerde applicaties wordt verwerkt en de gebruikte gegevens om de Apple apparaten zijn nodig gebleken om de gewenste beheermogelijkheden te verkrijgen. Met de verwerking wordt dus het beoogde doel bereikt.

Kijkende naar de evenredigheid van de verwerking ligt de vraag voor of het beoogde rechtmatige doel in verhouding staat tot de noodzaak om persoonsgegevens te verwerken. Met de gemaakte afspraken over het buiten toepassing stellen van bepalingen uit de SLASA wordt geen inbreuk gemaakt op dit principe.

Verder is het van belang om vast te stellen dat het detailniveau van de adminstrators en andere beheerdersrollen ten aanzien van het gebruik van de Apple apparaten door zowel de leerlingen als medewerkers van een beperkt niveau is. Er is dus geen sprake van een mogelijkheid tot onaanvaardbare en/of minutieuze monitoring van gebruikers van Apple apparaten.

Het tweede element van de proportionaliteitstoets betreft de evenredigheid. Het rechtmatige doel dat wordt nagestreefd moet in verhouding staan tot het feit dat daarvoor persoonsgegevens moeten worden verwerkt. De verwerking moet niet verder gaan dan noodzakelijk is voor het beoogde doel. Voor wat deze afweging betreft is, geredeneerd vanuit het perspectief van de school, het gebruik van Jamf School als MDM-oplossing een geschikte en proportionele methode gebleken.

Subsidiariteit

[34] Artikel 2 Wet op het voortgezet onderwijs, wetten.nl - Regeling - Wet op het voortgezet onderwijs - BWBR0002399 (overheid.nl)
[35] jamf-SLASA.pdf

Subsidiariteit betref de vraag of het genoemde doel niet op een andere, minder ingrijpende wijze (bijvoorbeeld door géén of minder persoonsgegevens te verwerken) kan worden bereikt. Deze DPIA voorziet niet in een vergelijkend warenonderzoek, de alternatieven op de markt zijn niet betrokken in dit assessment. Het op afstand beheren van de Apple apparaten is echter ook gedeeltelijk mogelijk via andere MDM-oplossingen. De vraag is of er bij andere MDM-oplossingen mogelijk minder persoonsgegevens nodig zijn voor de beschreven doelen, waardoor de hoeveelheid persoonsgegevens die nodig is kan worden verminderd. Voor nu lijkt dit onwaarschijnlijk gezien duidelijk naar voren is gekomen dat de verwerkingsdoelen niet zonder de geïnventariseerde persoonsgegevens bereikt kunnen worden.

Dit geldt echter in mindere mate voor de verwerkingen die Jamf op eigen conto doet zoals genoemd in artikel 19 van de SLASA. Hierover zullen verbetermaatregelen overeengekomen worden.

SLASA Software License and Services Agreement
Gebruikers van Jamf School zijn verplicht in te stemmen met de door Jamf opgestelde SLASA, deze versie V10082021 is de huidige en is beoordeeld in deze DPIA. De SLASA regelt de voorwaarden waaronder de schoolinstelling toegang krijgt tot de software en diensten van Jamf. De overeenkomst omvat definities van belangrijke termen, zoals "Affiliate", "Confidential Information" en "Personal Data", en beschrijvingen van de aangeboden diensten, waaronder de geboden technische ondersteuning, gehoste services en optionele diensten. Daarnaast behandelt het document aspecten zoals licentieverlening, gebruikslimieten, betalingsvoorwaarden en klantverplichtingen, inclusief de verantwoordelijkheid voor de benodigde infrastructuur en het naleven van vereisten gesteld door derden, zoals Apple. De SLASA is het belangrijkste contract tussen Jamf en haar klanten, waarin de voorwaarden worden vastgelegd voor het licenseren van Jamf's software en het verkrijgen van diensten. In het kader van deze DPIA is het van belang om aandacht te bieden aan artikel 19 van de SLASA. Hierin biedt Jamf zichzelf de ruimt om als verwerkingsverantwoordelijke verschillende verwerkingen te verrichten. Welke grondslag Jamf daarvoor gebruikt wordt niet vermeld en gemotiveerd. De onder artikel 19 a genoemde verwerkingen acht SIVON mogelijk deels passend bij de rol van verwerker echter is niet op alle onderdelen duidelijk welke gegevens op welke manier worden gebruikt. Het betreft: het monitoren van prestaties, integriteit en stabiliteit van de gehoste services, verhelpen en voorkomen van technische of beveiligingsproblemen, bieden van ondersteunende diensten en het verbeteren van de gehoste services en/of software.
Het beginsel dat de verwerking van persoonsgegevens transparant moet zijn, is een essentieel aspect van artikel 5 van de AVG. Een gebrek hieraan ondermijnt de legitimiteit van de verwerking. Het is daarom van belang dat in de SLASA meer duidelijkheid wordt geboden over de rol van Jamf School ten aanzien van deze verwerkingen als ook de verwerkingsdoeleinden. Ter bevordering van de transparantie zou ook in de verwerkersovereenkomst een verbinding gemaakt moeten worden met de SLASA ten aanzien van de verwerkingen die voor verantwoordelijkheid van Jamf komen en de grondslag die daarvoor wordt gebruikt.

Dit geldt niet voor de in artikel 19 b en c opgenomen verwerkingen. Hierover zijn privacybezwaren nu onvoldoende transparantie is over welke gegevens worden verzameld, hoe ze worden geanonimiseerd en hoe ze worden gebruikt. Na de bezwaren ten aanzien van deze verwerkingen voorgelegd te hebben aan Jamf zijn er afspraken gemaakt voor de educatieve sector. Deze behelzen dat Jamf een aparte SLASA ontwikkelt voor de educatieve sector binnen Nederland. Zie voor verdere informatie de maatregelentabel.

Jamf SLASA V10082021
19. Data Collection and Use.
a) Jamf may collect and use Performance and Usage Data and Customer Content to check compliance with contractual Software usage limits; monitor the performance, integrity and stability of the Hosted Services; address or prevent technical or security issues; provide support Services; and improve the Hosted Services and/or Software. We will not otherwise access, use or process Customer Content except as necessary to provide the Services.

b) Jamf may use de-identified, anonymized and aggregated Performance and Usage Data to analyze, improve and develop the Software and/or Hosted Services, such as the detection of new security threats.

c) Jamf and its service providers may use de-identified, anonymized and aggregated Performance and Usage Data and Customer Content during and after the term of this Agreement for any purpose so long as the data or content does not identify Customer or any individual, including Users.

Een transparante verwerking door de verwerker, juist als deze plaatsvindt voor eigen doeleinden, is essentieel om te waarborgen dat de belangen van de betrokkenen worden gerespecteerd en dat de verwerking proportioneel is aan het beoogde doel.

17. Rechten van de betrokkenen

In het volgende overzicht wordt weer gegeven hoe betrokkenen hun rechten kunnen uitoefenen.

Jamf als verwerker

Jamf School stelt de rol van IT-beheerder in staat om zijn verplichtingen als gegevensbeheerder te vervullen. Persoonlijke gegevens binnen het systeem kunnen rechtstreeks in de beheerinterface worden bekeken, bijgewerkt en verwijderd. Aangezien gedurende het proces van deze DPIA, Jamf binnen de Nederlandse educatieve sector niet meer gezien kan worden als verwerker en geen van deze taken op zich neemt, is het niet noodzakelijk extra rechten aan betrokkene te geven. Deze taak ligt bij het schoolbestuur zelf.

Jamf als verwerkingverantwoordelijke

Daarnaast heeft SIVON zelf een inzageverzoek ingediend welke via een one-trust omgeving[36] Kan worden ingediend. In dit geval betreft het een inzage verzoek voor verwerkingen waarbij Jamf de verantwoordelijke is.

Jamf heeft voorafgaand aan de afhandeling wel onderzoek naar de context van de indiener gedaan door te controleren of de indiener een eindgebruiker betrof of de direct verwerkingsverantwoordelijke. In het geval van het eerste zou zijn verwezen naar het proces van SIVON. Vertaald naar de onderwijssector wordt een eindgebruiker (leerling of leerkracht) die een verzoek indient bij Jamf dus verwezen naar de school om zijn rechten uit te oefenen.
De tijdige afhandeling van het verzoek bood vervolgens een volledig overzicht om tegemoet te komen in de te garanderen rechten. Het inzageverzoek wordt door Jamf afgehandeld via Onetrust. Er kan worden vastgesteld dat Jamf voorziet over een werkend systeem welke volledig voorziet in het uitgevraagde inzageverzoek. Zo voldeed het verzoek aan het bieden van een gedetailleerd overzicht van alle contacten die er met Jamf zijn geweest waaronder;

- Mails
- Registratie in CRM
- Jira ticket
- Gegevens als Jamf administrator contactpersoon (bedrijf/school gegevens)

Voor de afhandeling van de ingediende rechten van betrokkenen is Jamf verwerkingsverantwoordelijke. De verzameling van persoonsgegevens ten behoeve van dit proces vindt plaats buiten de controle van de school om. Dit betekent dat er geen invloed is op hoe en voor welke doeleinden deze gegevens gebruikt gaan worden en voor hoe lang deze worden bewaard. Jamf heeft echter wel inzicht geboden in de verwerkers die zij ten behoeve van deze verwerkingen hebben ingeschakeld en dat met deze partijen door de Europese Commissie goedgekeurde modelcontracten voor doorgifte zijn overeengekomen[37].

Tabel 17.1: Rechten van betrokkenen

Recht van betrokkene	**Toelichting procedure**	**Evt. beperking verwerking***
Het recht op informatie (het is aan de scholen om in dit recht te voorzien)	Bijvoorbeeld: • School verwijst naar gepubliceerde privacyverklaring van Jamf School; • Intern gepubliceerde privacyverklaring; • Versturen van een digitale brief naar e-mailadres betrokkenen;	n.v.t.

[36] https://privacyportal.onetrust.com/webform/d94b466b-3228-4486-adf9-a106deb779b6/94c8a983-6a6a-498b-ab5d-3584c3804b62

[37] Het is niet verplicht om een modelcontract te gebruiken, maar een leverancier kan hiermee laten zien u aan de privacywetgeving te voldoen.
https://www.autoriteitpersoonsgegevens.nl/themas/internationaal/doorgifte-binnen-en-buiten-de-eer/modelcontract-voor-doorgifte

Het recht van inzage	Jamf product voorziet scholen in de mogelijkheid om dit recht te kunnen uitoefenen en heeft hiervoor een werkende procedure.	n.v.t.
Het recht op rectificatie	Jamf School voorziet scholen in de mogelijkheid om dit recht te kunnen uitoefenen en heeft hiervoor een werkende procedure.	n.v.t.
Het recht op gegevenswissing	Jamf School voorziet scholen in de mogelijkheid om dit recht te kunnen uitoefenen en heeft hiervoor een werkende procedure.	n.v.t.
Het recht op beperking van de verwerking	Jamf School voorziet scholen in de mogelijkheid om dit recht te kunnen uitoefenen en heeft hiervoor een werkende procedure.	n.v.t.
Een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens	Jamf School voorziet scholen in de mogelijkheid om dit recht te kunnen uitoefenen en heeft hiervoor een werkende procedure.	n.v.t.
Het recht op overdraagbaarheid van gegevens	Jamf School voorziet scholen in de mogelijkheid om dit recht te kunnen uitoefenen en heeft hiervoor een werkende procedure.	n.v.t.
Het recht van bezwaar	Jamf School voorziet scholen in de mogelijkheid om dit recht te kunnen uitoefenen en heeft hiervoor een werkende procedure.	n.v.t.
Het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit	Is niet aan de orde bij het gebruik van Jamf (School)	n.v.t.

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

18. Beoordeling verwerkersovereenkomst

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

Convenant) en daarbij gebruik maken van het daarbij horende model verwerkersovereenkomst vindt een toetsing plaats welke wordt afgezet tegen de vereisten van het convenant. Dit wordt de theoretische toets genoemd. Voor leveranciers, waaronder Jamf, die geen deelnemer of medestander zijn van het convenant is de verwerkersovereenkomst getoetst aan de vereisten van de AVG.

Afnemers van de diensten van Jamf kunnen gebruikmaken van de door Jamf aangeboden verwerkersovereenkomst genaamd "Jamf Customer DPA V08142023" (DPA=Data Processing Agreement). Hierin staat onder meer opgenomen dat Jamf een Privacy Officer heeft aangesteld en voorziet tevens in het mailadres van deze persoon. Verder is invulling gegeven aan de rangorde van de DPA in die zin dat deze voor gaat op alle andere overeenkomsten waaronder de hoofdovereenkomst (SLASA). In geval van een conflict gelden dus de voorwaarden van de verwerkersovereenkomst. Echter wanneer er een bepaling in conflict is met de Standaard Contractuele Clausules zullen de toepasselijke Clausules gelden.

Tabel 18.1: Verwerkersovereenkomst

TOETSRAPPORT	**Toelichting**
Toets - Verwerkersovereenkomst	
• Artikel 6) Data Subject Requests	Er wordt een waarschuwing gegeven voor wat betreft de de kosten die gepaard gaan met de afhandeling van verzoeken van rechten van betrokkenen die de scope van Jamf's "commercieel redelijke" medewerking te boven gaan. Het is van belang dat Jamf zich houdt aan de wettelijke vereisten een de hiermee behorende verplichtingen. Jamf zal contact met het schoolbestuur opnemen indien Jamf vermoedt dat er kosten gemaakt zullen worden die verband houden met de afhandeling van de rechten van betrokkenen.
• Artikel 9) Personal Data Breach Management and Notification	Er zijn geen duidelijke afspraken opgenomen die zien op de inhoud en werkwijze in het geval van een datalek. Jamf geeft aan het schoolbestuur te verwittigen en te voorzien in assistentie voor zover gegevensbeschermingswetten dit vereisen. De suggestie wordt gedaan om gebruik te maken van een extra bijlage waarin wordt gespecificeerd welke stappen gezet moeten worden. Jamf heeft een contactlijst waarin de namen van de Primary Technical Contact and Decision Makers voor het account. Deze worden opgegeven door het schoolbestuur.
• Artikel 14a) Governing Law,	Deze passage betekent dat, afgezien van de bepalingen in de EEA Standaard Contractuele Clausules, het Zwitserse Addendum en het VK Addendum die betrekking hebben op welke wet hen regeert, de

	Verwerkersovereenkomst zal worden beheerst door en geïnterpreteerd in overeenstemming met de in de hoofdovereenkomst (SLASA) overeengekomen locatie en procedure voor geschillenbeslechting te weten Minnesota in de Verenigde Staten.
Toets - Bijlage 1: Details of Processing, B. Description of Transfer • Betreft gebrek aan transparantie **Bijlage 2: Approved Sub-processors** • Betreft gebrek aan transparantie	Binnen Jamf School kunnen ook foto's (in het profiel) worden verwerkt. Dit staat echter niet opgenomen in de bijlage. In het kader van de MDM is het ook mogelijk om de locatie (o.b.v. IP adres) van het apparaat vast te stellen. Dit staat niet opgenomen in de bijlage. Er staat niet in de verwerkersovereenkomst opgenomen welke verwerkingen in het kader van artikel 19 van de SLASA plaatsvinden. Bijlage of VWO voorziet niet in de naam van de af te nemen diensten/producten. Jamf heeft hier een grote verscheidenheid aan en de daarbij komende verwerkingen hangen samen met de betreffende dienst/product. In de VWO staat nergens dat de verwerkingen specifiek zien op het gebruik van Jamf School. De ingeschakelde subverwerkers ten tijde van het aangaan van de verwerkersovereenkomst staan niet in bijlage 2 opgenomen maar er wordt verwezen naar een dynamische link naar een website waar de namen van de subverwerkers staan.

Geen bijlage met afspraken inbreuk in verband met gegevensverwerkingen	Er is niet voorzien in een specifiek protocol op het gebied van informatievoorzieningen in het geval zich een inbreuk in verband met persoonsgegevens voordoet. Hierdoor is het lastig om in het geval de informatievoorziening gebrekkig is, dit af te dwingen en op die manier de betrokkenen de juiste mate van bescherming en informatievoorziening te voorzien.
Toets - Bijlage 3: Security Measures	Geen opmerkingen, bijlage is voorzien van uitvoerige opsomming van en inzicht in de door Jamf genomen technische en organisatorische maatregelen.

Subverwerkers

Ten aanzien van de gebruikte subverwerkers het volgende. Jamf zal het schoolbestuur op de hoogte stellen van elke wijziging in subverwerkers, inclusief toevoegingen of vervangingen van subverwerkers, waardoor het schoolbestuur de mogelijkheid heeft om bezwaar te maken tegen dergelijke wijzigingen. Als het schoolbestuur niet binnen 30 werkdagen na ontvangst van deze kennisgeving bezwaar heeft gemaakt tegen de voorgenomen wijziging, wordt het schoolbestuur geacht de voorgenomen wijziging te hebben goedgekeurd.

De verwerkersovereenkomst was niet in het Nederlands beschikbaar. Omdat schoolbesturen gebruik maken van een product in Nederland welke in een Nederlandse taal wordt aangeboden is het evengoed wenselijk in het kader van de transparantie en duidelijkheid om de verwerkersovereenkomst die ten grondslag ligt aan de voorwaarden waaronder gegevensverwerkingen (mogen) plaatsvinden in het Nederlands aan te bieden. Bovendien schrijft de AVG voor dat de verwerkersovereeenkomst in een taal moet worden aangeboden die begrijpelijk is.

<u>Verduidelijking subverwerkers</u>

In de lijst met door Jamf School ingeschakelde subverwerkers wordt kenbaar gemaakt dat de locaties van de gegevensverwerkingen door Amazone Web Services, Inc. in Duitsland, Japan of de Verenigde Staten kan plaatsvinden.

The countries listed are the sub-processor's locations from which this Jamf product is made available. Customers may choose the specific location in which they would like the product hosted.

Na uitvraag is gebleken dat bij de aanschaf van Jamf School automatisch de dichts bij zijnde hosting optie voor het product wordt aangeboden. Een andere locatie kan op verzoek, standaard wordt de data dus in Duitsland opgeslagen.

<u>Inbreuk in verband met persoonsgegevens</u>

Voorgestelde bijlage die handelingsperspectief biedt aan Jamf in het geval van een inbreuk in verband met persoonsgegevens.

Artikel 9 bijlage data breach

Afspraken over het informeren over beveiligingsincidenten en/of Datalekken

Verwerker heeft een procedure voor de monitoring en identificatie van incidenten en het informeren in geval van Datalekken en/of incidenten met betrekking tot beveiliging. In zo'n geval zal Verwerker de Verwerkingsverantwoordelijke de volgende informatie ter hand stellen:

· de kenmerken van de inbreuk, zoals: datum en tijdstip ontdekken en duur inbreuk; samenvatting van de inbreuk, waaronder de aard van de inbreuk en de aard en beschrijving van het beveiligingsincident (op welk onderdeel van de beveiliging heeft het betrekking, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van Persoonsgegevens);

· de oorzaak van de inbreuk;

· hoe de inbreuk is ontdekt;

· de maatregelen die getroffen zijn om de inbreuk aan te pakken en eventuele (verdere en toekomstige) schade te voorkomen;

· of de bij de inbreuk betrokken Persoonsgegevens versleuteld, gehasht etc. waren;

· de groep(en) Betrokkenen die gevolgen kunnen ondervinden van het incident, en de aantallen en omvang van de groep(en) Betrokkenen;

· wat de mogelijke gevolgen zijn van de inbreuk voor de Onderwijsinstelling en de groep(en) Betrokkene(n), waaronder indien mogelijk een inschatting van het risico van de gevolgen voor de groep(en) Betrokkene(n);

· de hoeveelheid en soort Persoonsgegevens betrokken bij de inbreuk (met name bijzondere Persoonsgegevens zoals gegevens over gezondheid of godsdienst, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

In geval van een (vermoeden van een) beveiligingsincident en/of Datalek, kunnen Onderwijsinstelling en Verwerker in beginsel per e-mail contact met elkaar opnemen via onderstaande contactgegevens.

	Naam en functie contactpersoon bij beveiligingsincidenten/Datalekken	**Contactgegevens (e-mail en telefoonnummer)**
Verwerker	[naam en functie contactpersoon Verwerker]	[contactgegevens Verwerker]
Onderwijsinstelling	[idem voor Onderwijsinstelling]	

Verder heeft Jamf de volgende aanvullende informatie geleverd:

'Zoals vermeld in de Data Processing Agreement (DPA), zal Jamf klanten zonder onnodige vertraging op de hoogte stellen van een inbreuk op persoonsgegevens en verdere hulp bieden indien vereist door de relevante wetgeving inzake gegevensbescherming. Jamf heeft interne beleidsregels en processen gedocumenteerd waarin richtlijnen en verantwoordelijkheden zijn vastgelegd voor het reageren op een inbreuk op persoonsgegevens. Dit omvat (i) processen voor het opsporen en onderzoeken van

inbreuken en interne meldingsprocedures, (ii) processen om het waarschijnlijke risico voor personen als gevolg van een inbreuk te beoordelen, (iii) processen voor het informeren van klanten en relevante toezichthoudende autoriteiten, inclusief de timing van meldingen en welke informatie we aan elke respectieve groep moeten verstrekken, en (iv) processen voor het documenteren van alle inbreuken, Ook als ze niet gemeld hoeven te worden.

Als Jamf vaststelt dat een melding noodzakelijk is, wordt de volgende informatie aan klanten verstrekt:

Een beschrijving van de aard van de inbreuk in verband met persoonsgegevens,

Een beschrijving van de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens,

een beschrijving van de maatregelen die zijn genomen of voorgesteld om de inbreuk in verband met persoonsgegevens aan te pakken en, in voorkomend geval, de maatregelen die zijn genomen om eventuele nadelige gevolgen te beperken;

De naam en contactgegevens van de functionaris voor gegevensbescherming en/of een ander contactpunt waar meer informatie kan worden verkregen.'

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

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

Beoordelingskader risico's

Alle mogelijke risico's van de gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen worden beschreven en afgewogen. Het gaat hierbij om de negatieve gevolgen die de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, de oorsprong van deze gevolgen, de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden en de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden: kans (waarschijnlijkheid) X impact (ernst) = risico.
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[38] om risico's te classificeren. Hierbij wordt een objectieve inschatting gemaakt van de kans en impact van negatieve gevolgen (eventuele fysieke, emotionele of materiële schade).

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

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

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

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

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)	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een of meerdere dagen brengt merkbare schade toe.	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een werkdag brengt merkbare schade toe. Juistheid

[38] 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

schade toe. Blijvende juistheid van informatie (vanaf de bron tot het laatste gebruik) is gewenst, maar hoeft niet gegarandeerd te zijn.	Sommige afwijkingen in data zijn toelaatbaar, juistheid data is belangrijk maar niet kritisch.	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 Jamf School 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.

Tabel 19.1: Risicotabel

Nummer	Mapgood	Risico-omschrijving	Oorzaak	Gevolgen	Kans	Impact	Risico	Proces en/of systeem-risico?
1		Onbevoegde/ongeautoriseerde Jamf gebruiker gaat akkoord met aangepaste voorwaarden.	Accepteren aangepaste Jamf voorwaarden SLASA wordt voorgelegd aan eerste gebruiker met beheerrechten die inlogt na de wijziging. Tekst Jamf School na update SLASA: *Agreements, Jamf has updated its Software License and Services Agreement ("SLASA"). The first user to sign in after the SLASA has been updated will be prompted to review and agree to the updated SLASA. For more information about Jamf's customer agreements, please visit Legal on Jamf's website.* *To continue using Jamf School, you must accept the updated Jamf School Agreements by Mon Aug 01 2022*	Aangepaste voorwaarden worden goedgekeurd door de eerste Jamf gebruiker zonder dat de schoolinstelling op de hoogte is van de gevolgen en aanpassingen.	3	2	6	
2			In artikel 19 van de SLASA geeft Jamf aan voor verschillende doeleinden persoonsgegevens te verwerken. De verwerking lijkt op onderdelen	Gebrek aan transparantie en controle over de data die Jamf gebruikt voor haar eigen doeleinden.	2	3	6	

			verder te gaan dan die van een reguliere verwerker. Hierdoor onstaat gebrek aan duidelijke afspraken over welke specifieke gegevens worden verzameld, voor welk doeleinde en onder welke grondslag.					
3		Onbevoegde toegang tot het admin-account, shut down onderwijs met Apple Apparaten. Wanneer de Adminrol wordt gehackt is er een groot probleem gezien alles gelockt en verwijderd kan worden. Het waarborgen van de integriteit en beschikbaarheid zijn van zeer grote urgentie.	De oorzaak van dit risico is de mogelijkheid dat een adminrol wordt gehackt, waardoor een kwaadwillende toegang kan krijgen tot het beheerdersaccount van Jamf School.	Als gevolg hiervan kan de hacker alle apparaten die onder het beheer vallen, vergrendelen of verwijderen. Dit kan leiden tot ernstige verstoringen van de integriteit en beschikbaarheid van de gegevens en systemen die binnen Jamf School worden beheerd.	1	3	3	
4		Standaardrollen van de users maar van de admins moet je ze zelf definiëren. Incorrect definiëren van adminrollen System ad kan alles, of andere zelf aan te	Terwijl standaardgebruikersrollen vooraf zijn gedefinieerd met specifieke bevoegdheden en toegangsrechten, vereisen administratorrollen handmatige configuratie en definitie door de beheerder. Als gevolg hiervan kan het voorkomen dat bepaalde administratorrollen niet correct worden geconfigureerd, wat kan leiden tot inconsistente of onbedoelde bevoegdheden voor bepaalde gebruikers.	Gebrek aan adequate controle over de toegang en autorisaties ingericht binnen het platform met ruimere bevoegdheden dan nodig is voor hun taken.	2	2	6	

		maken rol, by default alles uit.						
5a		Verwerkersovereenkomst (tabel 18.1) Obstakel uitoefenen rechten van betrokkenen.	In artikel 6 van de DPA wekt Jamf de suggestie dat het kosten in rekening kan brengen aan het schoolbestuur wanneer deze ondersteuning van Jamf nodig heeft voor de uitoefening van de rechten van betrokkenen indien het verzoek Jamf's norm van het “commercieel redelijke” overstijgt.	Het schoolbestuur kan kosten in rekening worden gebracht door Jamf voor het faciliteren van de rechten van betrokkenen van leerlingen en medewerkers.			3	
5b		Verwerkersovereenkomst (tabel 18.1) Onvoldoende respons en beheer in geval van inbreuk in verband met persoonsgegevens	Er zijn geen duidelijke afspraken opgenomen die zien op de inhoud en werkwijze in het geval van inbreuk in verband met persoonsgegevens. Jamf geeft aan het schoolbestuur te verwittigen en te voorzien in assistentie voor zover gegevensbeschermingswetten dit vereisen.	Het schoolbestuur kan in het geval zich een incident heeft voorgedaan bij Jamf geen beroep doen op concrete in de verwerkersovereenkomst toegezegde informatievoorziening die kan helpen bij het beheersen van het incident als ook informeren aan de toezichthouder en/of betrokkenen.	2	3	6	
5c		Verwerkersovereenkomst (tabel 18.1) Onvoldoende rechtsbescherming in geval van (juridisch) conflict of geschil	De hoofdovereenkomst (SLASA) schrijft de wetten en geschillenbeslechtingsprocedures van een ander rechtsgebied voor (Verenigde Staten), waardoor het schoolbestuur mogelijk niet kan profiteren van de bescherming die de Nederlandse wetgeving biedt in geval van een geschil met Jamf.	Als de regels voor geschillen tussen het schoolbestuur en Jamf niet duidelijk zijn, kan het lastiger zijn om snel problemen op te lossen. Dit kan betekenen dat het schoolbestuur niet goed kan zorgen voor de bescherming van de gegevens van leerlingen en dat leerlingen hun rechten misschien niet volledig kunnen gebruiken. Een geschil wordt bovendien complex en juridisch ingewikkeld en duur omdat de wetten van de Verenigde			6	

				Staten gelden en hiervoor dus ook specifieke juridische kennis nodig is. Het schoolbestuur kan dus te maken krijgen met onzekerheid, complexiteit en mogelijk een gebrek aan effectieve juridische bescherming bij het oplossen van geschillen met Jamf.				
5d		Verwerkersovereenkomst (tabel 18.1) Gebrek aan transparantie	De ingeschakelde subverwerkers ten tijde van het aangaan van de verwerkersovereenkomst staan niet in bijlage 2 opgenomen maar er wordt verwezen naar een dynamische link naar een website waar de namen van de subverwerkers staan.	Het is niet of lastig controleerbaar met welke subverwerkers akkoord is gegaan en welke aanpassingen er op een later moment hebben plaatsgevonden. Zo kan de informatie op de subverwerkers-website zijn aangepast in de tijd tussen aangaan verwerkersovereenkomst en moment van bekijken van de website. Het is dan niet vast te stellen of er wisselingen in subverwerkers hebben plaatsgevonden.	2	2	4	
5e		Verwerkersovereenkomst (tabel 18.1) Gebrek aan transparantie p.20	Zowel de verwerking van een optionele (profiel)foto als de locatie van het apparaat (o.b.v. IP-adres) staat niet opgenomen in de verwerkersovereenkomst. Dit geldt ook voor de (diagnostische) gegevens die in het kader van artikel 19 SLASA worden verwerkt.	Dit kan leiden tot niet-naleving van de transparantieverplichting, waarbij betrokkenen mogelijk niet volledig op de hoogte zijn van de verwerking van hun gegevens. Dit kan resulteren in potentiële inbreuken op de privacyrechten van betrokkenen.	3	2	6	

			Uit de Jamf DPA: Details of processing: Categories of Personal Data transferred: Names, IP addresses, telephone numbers, computer names, job titles and functions, and email addresses.					
5f		Verwerkersovereenkomst (tabel 18.1) Gebrek aan transparantie p.20	De DPA voorziet niet in de naam van de af te nemen diensten/producten. Jamf heeft hier een grote verscheidenheid aan en de daarbij komende verwerkingen hangen samen met het betreffende dienst/product.	Dit kan leiden tot niet-naleving van de transparantieverplichting, waarbij betrokkenen mogelijk niet volledig op de hoogte zijn van de verwerking van hun gegevens. Dit kan resulteren in potentiële inbreuken op de privacyrechten van betrokkenen.				
6		Te brede beheerrechten	De system administrator kan verschillende beheerdersrollen aanmaken voor verschillende verantwoordelijkheden binnen de school. Zo kan de rol van materiaalmanager, apparaatmanager of helpdeskmedewerker worden aangemaakt. Deze rollen kunnen vergaande autorisaties met zich meebrengen welke sterk afwijken van die van de leerling of leerkracht.	De bevoegdheden, die de door de system administrator uitgegeven beheerdersrollen, met zich meebrengen kunnen tot ongewenst gevolg met zich meebrengen dat standaard instellingen en functionaliteiten worden aangepast en gewijzigd door onbekwame gebruikers waardoor er een gebrek is aan eenduidig beheer binnen de Jamf School omgeving. Dit kan resulteren in inconsistenties, verwarring en verminderde efficiëntie bij het beheren van apparaten.	2	2	4	

7		Support p.26	Jamf is verwerkingsverantwoordelijke voor wat betreft de afhandeling van support tickets. Risico: Jamf is controller t.a.v. de tickets, wees terughouden met het meesturen van persoonsgegevens via de inhoud van de melding of meegestuurde bijlagen zoals pdf, video etc.	(gevoelige) gegevens die ten behoeve van een supportvraag worden gedeeld met Jamf vallen buiten de controle van de school omdat Jamf deze supporttickets in de rol van verwerkingsverantwoordelijke afhandelt.				
8		Verlies van controle Toegang tot Apple store	De systeembeheerder heeft de mogelijkheid om gebruikers vrij toegang te geven tot de Apple Store of strikte controle uit te oefenen over het pushen van (educatieve) apps. Om controle over de digitale leeromgeving en de hiervoor in te zetten educatieve middelen te behouden dient de App store afgesloten te worden voor gebruikers van de in beheer uitgegeven Apple apparaten.	Het voor gebruikers openstellen van de App store kan leiden een gebrek aan controle over de digitale (leer)omgeving en het ontstaan van potentiële veiligheidsrisico's, zoals blootstelling aan ongepaste inhoud of privacyproblemen. Bovendien kan het beheer van de apparaten complexer worden en kan het moeilijker zijn om een consistente leeromgeving te handhaven.	3	2	6	

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.

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.**

19. 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.

Tabel 19: 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	Akkoord Jamf voorwaarden door ongeautoriseerde gebruiker	6	Jamf creert een herziene versie van de SLASA en DPA specifiek gericht op Nederlandse scholen (een zogenaamde 'special contract'). Deze overeenkomst zal ter vervanging dienen van de click-through overeenkomst die eerder gebruikt werd. Deze nieuwe versie vermijdt de clickthrough en zal in plaats daarvan getekend kunnen worden door scholen voor akkoord.	Jamf	0	Er is na het doorvoeren van de maatregelen geen restrisico	Afspraak gemaakt 17 juli, 4 december bevestiging van implementatie
2	Gebrek aan transparantie eigen verwerkingsdoeleinden Jamf	6	Jamf zal in dezelfde herziene versie van de SLASA, artikel 19 sectie c verwijderen. Jamf zal hierdoor geen rol van verwerkingsverantwoordelijke meer op haar nemen. Jamf heeft bevestigd alleen verwerkingen uit te voeren in het kader van productverbetering. Doordat Jamf slechts verwerker is van de scholen, is het niet langer noodzakelijk om doeleinden van haar eigen verwerkingen toe te lichten.	Jamf	0	Er is na het doorvoeren van de maatregelen geen restrisico.	4 december bevestiging
3	Onbevoegde toegang tot het admin-account, shut down onderwijs	4	Beperk het aantal rollen met de hoogste autoriteit binnen Jamf zodat de kans op onbevoegde toegang en ongewenste wijzigingen wordt verkleind. Dit kan aan de hand van een strikt	School	0	Er is na het doorvoeren van de maatregelen geen	Direct door schoolbestuur in te richten

	met Apple Apparaten.		rolgebaseerde autorisatiematrix.			restrisico .	
4	Adminrollen moeten zelf worden ingericht	6	Ga zorgvuldig te werk bij het definiëren van adminrollen en stem deze af op de door de medewerkers/gebruikers benodigde autorisaties. Controleer en werk deze rollen met enige regelmaat bij.	School	0	Er is na het doorvoeren van de maatregelen geen restrisico .	Direct door schoolbestuur in te richten
5a	Verwerkersovereenkomst, rechten van betrokkenen	3	Jamf geeft aan dat deze beperking alleen toepasbaar is op situaties waarin zij verwerkingsverantwoordelijke zijn. Aangezien het contract zo aangepast is dat Jamf effectief geen verwerkingsverantwoordelijke meer is binnen contracten met Nederlandse scholen, is deze maatregel niet meer noodzakelijk en het probleem verholpen.	Jamf	0	Er is na het doorvoeren van de maatregelen geen restrisico .	4 december bevestiging
5b	Verwerkersovereenkomst, procedure inbreuk persoonsgegevens.	6	Jamf vat haar procedure voor inbreuk op persoonsgegevens samen zodat deze toegevoegd kan worden aan deze DPIA. (zie pagina 55-56)	Jamf	0	Er is na het doorvoeren van de maatregelen geen restrisico .	17 juli opgeleverd
5c	Verwerkersovereenkomst, jurisdictie	6	Jamf verklaart, ten behoeve van de duidelijkheid en het bieden van een vertrouwde juridische omgeving voor het oplossen van geschillen, de jurisdictie van de verwerkingsverantwoordelijke in de herziene versie van de	Jamf	0	Er is na het doorvoeren van de maatregelen geen	Bevestiging 4 december

			SLASA en DPA van toepassing. Deze aanpassing zal plaatsvinden in artikel 14. Van de SLASA. De geschillen zullen worden beslecht volgens de wetten en geschillenbeslechtingsprocedures van Nederland conform Nederlandse wetgeving.			restrisico.	
5d	Verwerkersovereenkomst, gebrek aan transparantie	4	Jamf stuurt bestaande klanten notificaties in het geval van updates binnen de lijst met sub-verwerkers. Dit gebeurt via de e-mail alsmede de 'Jamf Nation', het usergroup portal van Jamf. Scholen wordt geadviseerd deze notificaties zorgvuldig bij te houden om op de hoogte te blijven van veranderingen.	Jamf/school	0	Er is na het doorvoeren van de maatregelen geen restrisico.	Bestaande alternatieve maatregel
5e/f	Verwerkersovereenkomst, onduidelijkheid afgenomen product en te verwerken persoonsgegevens	6	Jamf zal voorzien in duidelijkheid in de verwerkersovereenkomst ten aanzien van zowel de afgenomen producten waar de verwerkingen op zien als ook de persoonsgegevens die daarbij worden gebruikt waaronder locatiegegevens, diagnostische gegevens en foto's. Jamf voegt dit toe in de eerstvolgende versie van de DPA.	Jamf	0	Er is na het doorvoeren van de maatregelen geen restrisico.	Zal worden doorgevoerd in Q1 2025
6	Te brede beheerrechten aan gebruikers	4	Implementeer een gestructureerd rollen- en autorisatiebeleid binnen het Jamf-School beheersysteem. Door deze rollen te definiëren met duidelijk omschreven autorisaties die aansluiten bij de taken van de gebruikers, wordt het risico verminderd dat	School	1	Na implementatie wordt het risico verminderd, maar het kan niet geheel	Direct door schoolbestuur in te richten

			onbekwame gebruikers onbedoelde aanpassingen maken aan instellingen en functionaliteiten.			verholpen worden.	
7	Support Jamf	4	Wees voorzichtig en terughoudend bij het delen van (gevoelige) informatie, zoals printscreens en documenten, voor technische ondersteuning vanuit de supportomgeving van Jamf. Deel enkel die informatie die strikt nodig is bij het oplossen van de supportvraag. Houd er rekening mee dat Jamf deze ondersteunende gegevens verwerkt als verwerkingsverantwoordelijke.	School	1	Na implementatie wordt het risico verminderd, maar het kan niet geheel verholpen worden	Direct door schoolbestuur toe te passen
8	Inrichting Jamf/toegang Apple store	4	Beperk de toegang tot de Apple Store voor gebruikers van de in beheer uitgegeven Apple apparaten ten behoeve van het behouden van controle over de digitale (leer)omgeving van de school. Dit voorkomt tevens dat de school kan zien welke apps de leerling/medewerker zelf op zijn apparaat heeft gedownload.	School	0	Er is na het doorvoeren van de maatregelen geen restrisico.	Direct door schoolbestuur in te richten

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

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

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

- onvermogen om rechten uit te oefenen (inclusief maar niet beperkt tot privacyrechten);
- onvermogen om toegang te krijgen tot diensten of kansen;

- verlies van controle over het gebruik van persoonsgegevens;
- discriminatie;
- identiteitsdiefstal of fraude;
- financieel verlies;
- reputatieschade;
- verlies van vertrouwelijkheid;
- heridentificatie van gepseudonimiseerde gegevens; of
- elk ander significant economisch of sociaal nadeel
- gevolgen en risico's voor de beveiliging van [SYSTEEM].]

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

kans (waarschijnlijkheid) X impact (ernst) = risico

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

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

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

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

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

De in de lokale DPIA geconstateerde risico's betreffen:

[RISICO] [toelichting risico]						
Risico-afweging	**kans**		**impact**		**Risico**	
Maatregel/maatregelen	[beschrijving maatregel]					
Eigenaar maatregel	[wie is verantwoordelijk voor uitvoeren maatregel: benoem de eigenaar]					
Maatregelen geïmplementeerd?	[is de maatregel al gepland, zo niet wanneer wordt deze gepland]					
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. Aanbevelingen

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

A. …

B. …

I. 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:

i