Driving innovation together

Data Protection Impact Assessment AFAS Profit (HRM en Payroll)

SURF Vendor Compliance

Auteurs: Daisy Brugman, Jan Landsaat & Sophia Gelpke
Versie: 1.0
Datum: 29 juni 2026

Revisiegeschiedenis

Versie	Datum	Wijzigingen
0.4	12-12-2025	Eerste ‘stable release’ onderdeel A.
0.41	18-12-2025	Interne feedback onderdeel A verwerkt.
0.42	19-12-2025	Document opgeschoond, onderdeel A, voor delen met AFAS ter review.
0.44	13-01-2026	Feedback onderdeel A van AFAS verwerkt.
0.70	27-03-2026	Na bezoek AFAS Eerste ‘stable relase’ onderdeel B en C.
0.71	31-03-2026	Interne feedback onderdeel A-C verwerkt.
0.75	1-04-2026	Document opgeschoond, onderdeel A-C voor delen met AFAS ter review.
0.80	23-04-2026	Eerste ‘stable release’ onderdeel D.
0.81	29-04-2026	Interne feedback onderdeel D verwerkt. Deel D opgeschoond, onderdeel D voor delen met AFAS ter review.
0.9	05-05-2026	Feedback onderdeel D van AFAS verwerkt.
0.91	21-05-2026	Feedback samenvatting en onderdeel D van AFAS verwerkt.
0.95	1-06-2026	Volledige versie van de DPIA met samenvatting, conclusie en feedback van AFAS verwerkt.
0.99	10-06-2026	Conceptversie met AFAS gedeeld voor NDA check.
1.0	29-06-206	Bijlage 3 Beveiligingsgaranties bijgewerkt n.a.v. ontvangen documenten AFAS.

Inhoudsopgave

Verklarende woordenlijst

Term	Afkorting	Definitie
AFAS Insite	-	De portal-lagen voor respectievelijk interne selfservice.
AFAS Online	-	De cloud-infrastructuur en beheerplatform.
AFAS Outsite	-	De portal-lagen voor respectievelijk externe selfservice.
AFAS Pocket	-	Pocket/Profit-webversie de client-varianten vormen die verschillende apparaten en connectiviteitspatronen bedienen.
Algemene Verordening Gegegevensbescherming	AVG	In de AVG staat hoe je omgaan met persoonsgegevens. Deze privacywetgeving gelft sinds 2018 in de hele Europese Unie.
Cloud Service	-	IT-dienst (software, opslag, rekenkracht, of infrastructuur) die via het internet op aanvraag wordt geleverd door een externe provider.
Customer Relationship Management	CRM	Softwaresysteem waarmee klantinteracties, verkoopprocessen en marketingcampagnes centraal worden beheerd en geanalyseerd.
Data Protection Impact Assessment	DPIA	Beschrijft een proces dat is ontworpen om risico's te identificeren die voortvloeien uit de verwerking van persoonsgegevens en om deze risico's zo veel mogelijk en zo vroeg mogelijk te minimaliseren.
Datacenter	-	Een datacenter is een speciaal ontworpen, fysieke locatie waar servers en andere ICT-apparatuur draaien om digitale gegevens en online diensten continu beschikbaar te houden.
Enterprise Resource Planning	ERP	Een ERP-systeem integreert alle gegevens en processen van verschillende afdelingen in één centraal systeem.

European Data Protection Board	EDPB	Het Europees Comité voor gegevensbescherming (EDPB) is een onafhankelijk Europees orgaan dat erop toeziet dat de AVG consequent wordt toegepast en dat de samenwerking tussen de gegevensbeschermingsautoriteiten van de EU bevordert. Op 25 mei 2018 verving de EDPB de Artikel 29-werkgroep.
Europees Economische Ruimte	EER	De EER (Europese Economische Ruimte) is het gebied waarin de EU-lidstaten plus IJsland, Noorwegen en Liechtenstein één gezamenlijke interne markt vormen met vrij verkeer van personen, goederen, diensten en kapitaal.
Failover	-	Automatisch mechanisme waarbij een systeem of dienst onmiddellijk overschakelt naar een backup-component of reserve-server bij uitval.
Hosting provider	-	Een hosting provider is een bedrijf dat de technische omgeving (servers, opslag en netwerk) levert en beheert zodat websites, e-mail en andere online diensten via internet bereikbaar zijn.
Infrastructure as a Service	IaaS	Cloudservice waarbij je via het internet toegang krijgt tot IT-infrastructuur die door een provider wordt beheerd, zodat je als afnemer niet zelf fysieke hardware hoeft te bezitten of onderhouden.
Multi Factor Authentication	MFA	Beveiligingsmechanisme waarbij gebruikers zich moeten identificeren met minstens twee verschillende authenticatiefactoren, zoals wachtwoord en een code op je telefoon.
Nederlandse onderzoeks- en onderwijsorganisaties	Instellingen	Deze DPIA is opgesteld voor de Nederlandse onderzoeks- en instellingen, soms afgekort tot 'de Nederlandse onderwijssector' of 'instellingen'.
Recovery Point Objective	RPO	Maximale interval tussen het moment van een storing en het laatste beschikbare backup waaruit het systeem kan worden hersteld.

Recovery Time Objective	RTO	Maximale tijd waarin een systeem of dienst na een storing moet worden hersteld voordat het weer operationeel is.
Self Service Employee Portal	SSEP	Webportaal waar werknemers zelfstandig hun personeelsgegevens kunnen beheren, aanvragen kunnen indienen en HR-informatie kunnen raadplegen.
Single Sign On	SSO	Authenticatiemechanisme waarmee gebruikers zich eenmalig aanmelden en vervolgens automatisch toegang krijgen tot meerdere gekoppelde applicaties en diensten zonder opnieuw hun inloggegevens in te hoeven voeren.

Samenvatting

Dit document is een Data Protection Impact Assessment (DPIA) over het gebruik van de SaaS-applicatie Profit door Nederlandse onderwijsinstellingen (hierna: instellingen), aangeboden door AFAS B.V. (AFAS). Deze DPIA is een referentie-DPIA uitgevoerd door sectororganisatie SURF, die instellingen een algemeen kader biedt voor het beoordelen van gegevensbeschermingsrisico's binnen Profit.

Over de software
Profit is een geïntegreerd ERP-systeem, dat bedrijfsprocessen zoals financiën, HRM, CRM, projectmanagement en voorraadbeheer in één applicatie automatiseert en verbindt.

Scope
SURF heeft zowel juridisch als technisch onderzoek verricht om algemene gegevensbeschermingsrisico's in kaart te brengen die voortvloeien uit de gegevensverwerkingsactiviteiten die instellingen in Profit uitvoeren. Deze DPIA heeft betrekking op het ERP-softwarepakket AFAS Profit, waarbij de focus specifiek ligt op de modules HRM en Payroll. Ook de native mobiele applicatie AFAS Pocket valt binnen de scope, aangezien deze als lightweight client synchroniseert met de AFAS Online backend om de HR- en payrollfunctionaliteiten op smartphones en tablets aan te bieden. Daarnaast maken de supportverzoeken en de portalen klant.afas.nl en help.afas.nl integraal deel uit van de beoordeling. Ondersteunende functionaliteiten zoals Workflow- & Documentmanagement en CRM zijn alleen in scope voor zover ze de HR- en payrollprocessen direct ondersteunen.

Buiten scope
De specifieke AFAS-modules Abonnementen, Financieel, Fiscaal, Ordermanagement en Projecten vallen volledig buiten de scope van deze DPIA, net als alle externe applicaties waarmee Profit gekoppeld kan zijn, zoals die van de arbodienst. Verder gaat deze DPIA ervan uit dat de verwerking van persoonsgegevens van minderjarigen in AFAS een uitzonderlijke situatie betreft, aangezien de meeste mensen in de beroepsbevolking volwassenen zijn. Tot slot is ook de AI-assistent 'Jonas' buiten scope gelaten

Aangezien dit een overkoepelende-DPIA betreft, bevat deze geen beoordeling van de rechtmatigheid van specifieke verwerkingsactiviteiten, noch van risico's die specifiek zijn voor individuele instellingen. In plaats daarvan wordt een meer algemene beoordeling gemaakt op basis van het beoogde gebruik van Profit door instellingen. Instellingen die Profit willen gebruiken, kunnen deze DPIA als uitgangspunt nemen, maar moeten deze aanvullen, uitbreiden en/of aanpassen op basis van de specifieke context waarin zij Profit willen gebruiken.

Methodologie
SURF heeft de volgende methoden gebruikt om de beoordeling uit te voeren:

- Juridisch onderzoek en beoordeling van de contracten, certificeringen en andere documentatie van AFAS.
- Technisch onderzoek in de in-browser applicatie, uitgevoerd in een testomgeving die AFAS voor SURF heeft gecreëerd, inclusief het gebruik van een gespecialiseerde monitoringtool (man-in-the-middle proxy).
- Verzoeken om inzage van betrokkenen, ingediend nadat het technisch onderzoek was uitgevoerd.
- Vragenlijsten aan de vertegenwoordigers van AFAS.

Resultaat: 14 hoge risico's en 2 risico's waarvan de ernst nog moet worden vastgesteld
Deze DPIA heeft veertien hoge risico's voor betrokkenen geïdentificeerd en twee risico's waarvan de ernst nog moet worden vastgesteld. Vier van de hoge risico's hebben te maken met de privacyrechtelijke rolverdeling en contractuele risico's. Drie van de hoge risico's houden verband met de rechten van betrokkenen. Zeven van de hoge risico's zijn algemene risico's, die ofwel worden veroorzaakt door de manier waarop instellingen Profit (waarschijnlijk) gebruiken, ofwel door het ontwerp van AFAS. Twee van de risico's houden verband met het gebruik van de mobiele app. Deze twee risico's bestaan voor elke app die gebruikmaakt van een app winkel en pushmeldingen van derden. Aangezien SURF een aanvullend onderzoek doet naar de impact van deze risico's, zal het risiconiveau op een later tijdstip worden vastgesteld.

Tot slot benadrukt SURF dat het merendeel van de geïdentificeerde risico's betrekking lijken te hebben op diagnostische gegevens, en niet op de gegevens die instellingen zelf in Profit invoeren.

Maatregelen
Door deze maatregelen te implementeren worden alle hoge risico's beperkt, waardoor alleen lage restrisico's overblijven.

Voor al deze risico's is er een tijdschema voor de implementatie van de maatregelen. Daarom kunnen instellingen Profit blijven gebruiken. Als de hoge risico's worden beperkt, is voorafgaand overleg met de gegevensbeschermingsautoriteit niet vereist. SURF zal in 2027 een update over deze DPIA publiceren met een conclusie over de implementatie van de resterende maatregelen.

Een overzicht van alle geïdentificeerde risico's en voorgestelde maatregelen wordt weergegeven in de onderstaande tabel. De risico's en maatregelen zijn soms van toepassing op AFAS, als leverancier van Profit, en soms op de onderwijsinstellingen als afnemers van Profit. De status van de maatregelen die AFAS moet nemen, wordt weergegeven in de rechterkolom.

#	Risico	Maatregelen instellingen	Maatregelen AFAS	Status AFAS Maatregelen
Rolverdeling en contractuele risico's				
1.1.	Verlies van controle door AFAS als verwerkingsverantwoordelijke	Herziene verwerkersovereenkomst van AFAS beoordelen en ondertekenen.	Update verwerkersovereenkomst tussen AFAS en instellingen o.a. met: alle categorieën persoonsgegevens, inclusief diagnostische gegevens indien van toepassing, die AFAS en subverwerkers namens instellingen verwerken; legitieme doeleinden waarvoor AFAS en subverwerkers persoonsgegevens mogen verwerken en onder welke voorwaarden; doeleinden waarvoor AFAS en subverwerkers geen persoonsgegevens mogen verwerken.	AFAS zal haar overeenkomsten uiterlijk op 31 december 2026 updaten.
1.2	Verlies van controle en vertrouwelijkheid door onvolledige verwerkersovereenkomsten	Herziene verwerkersovereenkomst van AFAS beoordelen en ondertekenen.	Update verwerkersovereenkomst tussen AFAS en instellingen o.a. met: alle categorieën persoonsgegevens, inclusief diagnostische gegevens indien van toepassing, die AFAS en subverwerkers namens instellingen verwerken; legitieme doeleinden waarvoor AFAS en subverwerkers persoonsgegevens mogen verwerken en onder welke voorwaarden; doeleinden waarvoor AFAS en subverwerkers	AFAS zal haar overeenkomsten uiterlijk op 31 december 2026 updaten.

#	Risico	Maatregelen instellingen	Maatregelen AFAS	Status AFAS Maatregelen
			geen persoonsgegevens mogen verwerken.	
1.3	Verlies van controle door het ontbreken van subverwerkersovereenkomsten	Beoordeel de in de DPIA geïdentificeerde subverwerkers.[1] Dien bij bezwaar een verzoek in bij de AFAS.	Ten aanzien van de supportpagina's klant.afas.nl en help.afas.nl, die in de praktijk hoofdzakelijk door functioneel beheerders worden bezocht: Verwerkersovereenkomsten met LinkedIn, Google en Vimeo afsluiten waarin de afspraken in de verwerkersovereenkomst met instellingen worden doorgezet, met een duidelijke instructie over de te verwerken persoonsgegevens en een lijst met subverwerkers.	AFAS zal de overeenkomsten uiterlijk op 31 december 2026 actualiseren.
		-	Ten aanzien van de supportpagina's klant.afas.nl en help.afas.nl, die in de praktijk hoofdzakelijk door functioneel beheerders worden bezocht: Specificatie van de verwerkingen opnemen in de subverwerkersovereenkomsten met Cookiebot, Cloudflare en Hunt & Hackett.	AFAS zal de overeenkomsten uiterlijk op 31 december 2026 actualiseren.

[1] Bij het aangaan van de overeenkomst en gedurende de overeenkomst waren deze subverwerkers onbekend bij de instellingen. Hierdoor hebben zij de partijen destijds niet kunnen beoordelen en was het onmogelijk om gebruik te maken van het contractuele bezwaarrecht.

#	Risico	Maatregelen instellingen	Maatregelen AFAS	Status AFAS Maatregelen
		-	Ten aanzien van AFAS Online: Verwerkersovereenkomsten met Leaseweb afsluiten waarin de afspraken in de verwerkersovereenkomst met instellingen worden doorgezet, met een duidelijke instructie over de te verwerken persoonsgegevens en een lijst met subverwerkers.	AFAS zal de overeenkomsten uiterlijk op 31 december 2026 actualiseren.
Rechten van betrokkenen				
1.4	Niet uit kunnen oefenen van AVG-rechten door incomplete inzageverzoeken	-	Volledige inzage in verwerkingen verschaffen bij een inzageverzoek, ofwel door beheerders de mogelijkheid te bieden zelf inzage te krijgen of door een duidelijke procedure te implementeren om inzageverzoeken te verwerken.	AFAS stelt deze maatregel reeds te hebben doorgevoerd. SURF heeft dit nog niet geverifieerd. De instelling kan alle logging direct opvragen via https://login.afasonline.com of, indien nodig, een verzoek indienen via https://klant.afas.nl.
1.5	Niet mogelijk om AVG-rechten uit te oefenen en verlies van controle door gebrek aan transparantie subverwerkers	Periodieke controle op overzicht subverwerkers.	Afhankelijk van de subverwerker: SLA (verwerkersovereenkomst), privacyverklaring en/of cookieverklaring updaten met relevante subverwerkers.	AFAS zal uiterlijk 31 december 2026 per versie van de documenten (SLA, AV en verwerkersovereenkomst) een controle uitvoeren met betrekking tot de (nieuwe) subverwerkers.
			Hoofd- en verwerkersovereenkomsten met alle	AFAS zal de overeenkomsten uiterlijk op 31

#	Risico	Maatregelen instellingen	Maatregelen AFAS	Status AFAS Maatregelen
			subverwerkers afsluiten waarin de afspraken in de verwerkersovereenkomst met instellingen worden doorgezet, met een duidelijke instructie over de te verwerken persoonsgegevens en een lijst met subverwerkers.	december 2026 actualiseren.
1.6	Niet mogelijk om AVG-rechten uit te oefenen door onduidelijke rolverdeling	Herziene verwerkersovereenkomst van AFAS beoordelen en ondertekenen.	Update verwerkersovereenkomst tussen AFAS en instellingen o.a. met: alle categorieën persoonsgegevens, inclusief diagnostische gegevens indien van toepassing, die AFAS en subverwerkers namens instellingen verwerken; legitieme doeleinden waarvoor AFAS en subverwerkers persoonsgegevens mogen verwerken en onder welke voorwaarden; doeleinden waarvoor AFAS en subverwerkers geen persoonsgegevens mogen verwerken.	AFAS zal haar overeenkomsten uiterlijk op 31 december 2026 actualiseren.
Algemene Risico's				
1.7.	Verlies van controle door zelfbouw workflows	Zorg ervoor dat HR-medewerkers goed zijn geïnstrueerd en opgeleid in de procedures van de instellingen voor het zorgvuldig registreren van persoonsgegevens.	Duidelijke strategie implementeren om klanten en gebruikers (in de context van de verwerking) te waarschuwen om de gegevensbeschermings risico's van de	AFAS stelt deze maatregel reeds te hebben doorgevoerd. SURF heeft dit nog niet geverifieerd. Er zijn legio aan (gratis)

#	Risico	Maatregelen instellingen	Maatregelen AFAS	Status AFAS Maatregelen
		Controleer periodiek door middel van steekproeven de workflows op doelmatigheid, proportionaliteit, data minimalisatie, toegang en bewaartermijnen.	workflows helder te maken.	opleidingen/cursussen voor die onderdeel zijn van de implementatie en ook los van de implementatie beschikbaar zijn voor de instellingen.
1.8.	Verlies van controle en vertrouwelijkheid door overige vrije tekstvelden	Gebruik alleen open tekstvelden met een duidelijk doel. Bij het aanmaken van vrije tekstvelden moet het functioneel beheer aanvinken of deze gevoelige of bijzondere persoonsgegevens (mogen) bevatten. Zorg ervoor dat medewerkers goed zijn geïnstrueerd en opgeleid in de procedures van de instellingen voor het zorgvuldig registreren van persoonsgegevens. Monitoring van de effectiviteit van dit beleid door middel van steekproeven.	Duidelijke strategie implementeren om klanten en gebruikers (in de context van de verwerking) te waarschuwen geen (bijzondere) persoonsgegevens in open velden op te nemen en om de gegevensbeschermingsrisico's van de vrije tekstvelden helder te maken.	AFAS stelt deze maatregel reeds te hebben doorgevoerd. SURF heeft dit nog niet geverifieerd. Er zijn legio aan (gratis) opleidingen/cursussen voor die onderdeel zijn van de implementatie en ook los van de implementatie beschikbaar zijn voor de instellingen.
1.9.	Verlies van vertrouwelijkheid en controle door handmatige invoer	Zorg ervoor dat HR-medewerkers goed worden geïnstrueerd en opgeleid in de procedures van de instellingen voor het zorgvuldig registreren van persoonsgegevens. Automatiseren invoer waar mogelijk.	-	-

#	Risico	Maatregelen instellingen	Maatregelen AFAS	Status AFAS Maatregelen
1.10.	Verlies van controle door niet automatisch te configureren bewaartermijnen	Vaststellen en beheren bewaartermijnen persoonsgegevens in AFAS.	Instellingen faciliteren bij het handhaven van hun bewaartermijnen door de mogelijkheden voor de technische configuratie en het beheer van bewaartermijnen per groep persoonsgegevens in AFAS te verbeteren.	AFAS heeft deze maatregel als wens ingestuurd op de (openbare) wensenlijst bij de afdeling Productontwikkeling. AFAS zal uiterlijk op 31 december 2026 een terugkoppeling hierover geven.
		Naleving bewaartermijnen vastleggen in processen.		
1.11.	Verlies van vertrouwelijkheid en controle door niet automatisch te configureren bewaartermijnen binnen logging	Vaststellen en beheren bewaartermijnen persoonsgegevens in AFAS.	AFAS als verwerker: Automatische bewaartermijnen op logging en monitoring mogelijk maken onder verantwoordelijkheid instellingen.	AFAS heeft deze maatregel als wens ingestuurd op de (openbare) wensenlijst bij de afdeling Productontwikkeling. AFAS zal uiterlijk op 31 december 2026 een terugkoppeling hierover geven.
		Naleving bewaartermijnen vastleggen in processen.	AFAS als verwerkingsverantwoordelijke: Vastellen, motiveren en beheren bewaartermijnen op logging en monitoring onder verantwoordelijkheid AFAS.	AFAS heeft deze maatregel als wens ingestuurd op de (openbare) wensenlijst bij de afdeling Productontwikkeling. AFAS zal uiterlijk op 31 december 2026 een terugkoppeling hierover geven.
			AFAS als verwerkingsverantwoordelijke: Automatische bewaartermijnen inregelen op logging en	AFAS heeft deze maatregel als wens ingestuurd op de (openbare) wensenlijst bij de

#	Risico	Maatregelen instellingen	Maatregelen AFAS	Status AFAS Maatregelen
			monitoring onder verantwoordelijkheid AFAS.	afdeling Productontwikkeling. AFAS zal uiterlijk op 31 december 2026 een terugkoppeling hierover geven.
1.12.	Verlies van controle door verdere verwerking van persoonsgegevens via algemene statistieken uit klantomgeving	-	Richt het proces zo in dat er geen persoonsgegevens in de algemene statistieken terechtkomen.	AFAS gaat maatregelen nemen. AFAS zal uiterlijk op 31 december 2026 een terugkoppeling hierover geven.
			Evalueer en verbeter het proces rond de uitvraag van deze rapportages door medewerkers van AFAS. Stel een procedure vast voor de omgang met persoonsgegevens en stel bewaartermijnen vast.	AFAS stelt deze maatregel reeds te hebben doorgevoerd. SURF heeft dit nog niet geverifieerd. AFAS heeft een bewaartermijn van 1 jaar vastgesteld. Deze bewaartermijn wordt ook nageleefd en geborgd in het proces.
			Houd toezicht op dit proces voor in het geval dat persoonsgegevens verwerkt worden.	AFAS stelt deze maatregel reeds te hebben doorgevoerd. SURF heeft dit nog niet geverifieerd. Elke aanvraag is onderhevig aan minimaal het vier ogen principe.

#	Risico	Maatregelen instellingen	Maatregelen AFAS	Status AFAS Maatregelen
1.13.	Verlies van controle en vertrouwelijkheid door ongeoorloofde toegang in derde landen[2]	-	Contractueel uitsluiten van doorgifte buiten de EER in de (sub)verwerkersovereenkomsten.	AFAS zal de overeenkomsten uiterlijk op 31 december 2026 actualiseren.
1.14	Verlies van controle door incorrecte cookieverklaring	-	Evalueer de procedure rondom de cookieverklaring en de optie om deze zelfstandig te beheren.	AFAS stelt deze maatregel reeds te hebben doorgevoerd. SURF heeft dit nog niet geverifieerd. AFAS gaat de cookieverklaring periodiek evalueren.
Mobiele app risico's				
1.15	Verlies van controle over persoonsgegevens door installatie van applicatie via app stores	Maak toegang via de mobiele webbrowser mogelijk.	Maak de app beschikbaar via side load.	AFAS heeft besloten dat de Pocket App niet via side load zal worden aangeboden.
		Voer proportionaliteits- en subsidiariteitsbeoordeling uit op beschikbaar stellen mobiele app via app stores of als 'side-load' en implementeer resultaten.	Maak toegang via de mobiele webbrowser mogelijk.	AFAS heeft besloten dat de Pocket App niet via mobiele webbrowser zal worden aangeboden.

2 Hoewel er juridisch gezien geen aanvullende maatregelen van de instelling nodig zijn zolang het Data Privacy Framework van kracht is, is het raadzaam om de geopolitieke situatie periodiek te evalueren – met name wat betreft de waarschijnlijkheid dat risico's zich voordoen – om te bepalen of een aanpassing van de risicobeoordeling nodig is.

#	Risico	Maatregelen instellingen	Maatregelen AFAS	Status AFAS Maatregelen
1.16	Verlies van controle door verwerken van push notificaties door Google en Apple	Neem geen persoonsgegevens op in de inhoud van de notificaties.	*Optioneel:* implementeer Unified push voor Androidgebruikers.	AFAS heeft besloten deze optionele maatregel niet uit te voeren.
		Voer proportionaliteits- en subsidiariteitsbeoordeling uit op versturen pushnotificatie via Google en Apple, of via Unified Push en implementeer resultaten.		

Inleiding

AFAS ontwikkelt en levert de software met de productnaam Profit. Deze Data Protection Impact Assessment (DPIA) uitgevoerd door SURF, onderzoekt de verwerking van persoonsgegevens die plaatsvindt wanneer Nederlandse onderwijs- en onderzoeksinstellingen Profit gebruiken. Profit is een geïntegreerd ERP-systeem van het Nederlandse bedrijf AFAS Software, dat bedrijfsprocessen zoals financiën, HRM, CRM, projectmanagement en voorraadbeheer in één applicatie automatiseert en verbindt.

Over SURF
SURF is de samenwerkingsorganisatie voor IT in het Nederlandse onderwijs en onderzoek. SURF is eigendom van haar leden, voornamelijk bestaande uit onderwijs- en onderzoeksinstellingen. Via SURF kopen de leden gezamenlijk hoogwaardige digitale diensten in, ontwikkelen en delen ze kennis en zorgen ze voor naleving van de regelgeving op het gebied van gegevensbescherming. Als onderdeel van haar dienstverlening voert SURF overkoepelende DPIA's uit voor IT-diensten die in de hele sector op grote schaal worden gebruikt.

Wat is een DPIA?
Een DPIA moet worden uitgevoerd door verwerkingsverantwoordelijken wanneer zij persoonsgegevens verwerken op een manier die "*een hoog risico voor de rechten en vrijheden van natuurlijke personen kan opleveren"*, volgens artikel 35 van de Algemene Verordening Gegevensbescherming (AVG). De beoordeling is bedoeld om onder meer inzicht te geven in de specifieke verwerkingsactiviteiten, het inherente risico voor de betrokkenen en de waarborgen die worden toegepast om deze risico's te beperken. Het doel van een DPIA is ervoor te zorgen dat alle risico's die aan het betreffende proces verbonden zijn in kaart worden gebracht en beoordeeld en dat er adequate waarborgen zijn geïmplementeerd om die risico's te beperken.

Betrokkenen hebben een fundamenteel recht op bescherming van hun persoonsgegevens en enkele andere fundamentele vrijheden die door de verwerking van persoonsgegevens kunnen worden aangetast, zoals de vrijheid van meningsuiting. Het recht op gegevensbescherming is daarom ruimer dan het recht op privacy. Overweging 4 van de AVG luidt als volgt:

> *"Deze verordening eerbiedigt alle grondrechten en neemt de vrijheden en beginselen in acht die zijn erkend in het Handvest zoals vastgelegd in de Verdragen, met name de eerbiediging van het privéleven en het gezinsleven, de woning en de communicatie, de bescherming van persoonsgegevens, de vrijheid van gedachte, geweten en godsdienst, de vrijheid van meningsuiting en informatie, de vrijheid van ondernemerschap, het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, en de culturele, religieuze en taalkundige verscheidenheid."*

Overkoepelende DPIA's versus individuele DPIA's
In termen van de AVG is SURF niet de verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens via het gebruik van de software Profit. Elke individuele onderwijs- of onderzoeksinstelling die Profit gebruikt, is verwerkingsverantwoordelijke. Als Nederlandse IT-coöperatie neemt SURF echter de verantwoordelijkheid op zich om de

gegevensbeschermingsrisico's voor de eindgebruikers te beoordelen en ervoor te zorgen dat de gegevensverwerking in overeenstemming is met de AVG. SURF voert overkoepelende DPIA's uit om haar leden te helpen bij het selecteren van een privacy conforme implementatie en om waar nodig hun eigen DPIA's uit te voeren. Alleen de organisaties zelf kunnen de specifieke risico's voor de gegevensbescherming beoordelen, die verband houden met de technische privacy-instellingen, de aard en omvang van de persoonsgegevens die zij verwerken en de kwetsbaarheid van de betrokkenen. De Autoriteit Persoonsgegevens (AP) heeft deze aanpak onderschreven om de bescherming van persoonsgegevens binnen de onderwijs- sector te verbeteren.[3] Deze overkoepelende DPIA is bedoeld om onderwijs- en onderzoeksorganisaties te helpen bij de DPIA die zij moeten uitvoeren wanneer zij de software Profit inzetten, maar kan niet in de plaats komen van de specifieke risicobeoordelingen die de organisaties zelf moeten maken.

Het uitvoeren van één overkoepelende DPIA voor een IT-dienst heeft voordelen voor zowel de leden van SURF als voor de leveranciers van de producten die SURF beoordeelt. Voor de leden bespaart het de kosten die zij zouden moeten maken als zij elk afzonderlijk een volledige DPIA zouden moeten uitvoeren. Ook kunnen zij hun gezamenlijke kennis over een product en hun ervaringen met een leverancier meenemen in de overkoepelende DPIA. Bovendien kan SURF effectiever onderhandelen over risicobeperkende maatregelen met de leveranciers, omdat het als vertegenwoordiger de gezamenlijke onderhandelingskracht van de hele sector heeft. Voor de leveranciers bespaart het tijd, moeite en geld dat ze niet elke instelling afzonderlijk hoeven te helpen met DPIA's die waarschijnlijk erg op elkaar lijken. Het is voor hen ook efficiënter om maatregelen te kunnen nemen die alle leden tegelijk ten goede komen.

DPIA-criteria
De AP heeft een lijst gepubliceerd met zeventien soorten verwerkingen waarvoor in Nederland altijd een DPIA verplicht is. Als een verwerking niet in deze lijst is opgenomen, moet een organisatie zelf beoordelen of de gegevensverwerking waarschijnlijk een hoog risico met zich meebrengt. De Europese nationale toezichthoudende autoriteiten (GBA's), verenigd in het Europees Comité voor gegevensbescherming (EDPB), hebben ook een lijst met negen criteria gepubliceerd. Als vuistregel geldt dat een DPIA vereist is als een gegevensverwerking aan twee van deze criteria voldoet.

De verwerking van persoonsgegevens binnen Profit valt onder géén van de zeventien verwerkingscategorieën uit de lijst van de AP en voldoet aan drie van de negen beoordelingscriteria van het EDPB.

Uit de lijst van het EDPB zijn de volgende criteria van toepassing:

- *Criterium 4 - Gevoelige gegevens of gegevens van zeer persoonlijke aard:* Vanwege de aard van HRM en Payroll software bevat het speciale categorieën gegevens en gevoelige gegevens.

[3] Autoriteit Persoonsgegevens, *Sectorbeeld Onderwijs 2021-2023*, 24 januari 2024, p. 5-6, geraadpleegd via: https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023.

- *Criterium 5 - Op grote schaal verwerkte gegevens*: De persoonsgegevens in de software hebben betrekking op alle werknemers en niet-gesalarieerde personeelsleden van een instelling en deze mensen kunnen daar lange tijd werken, waardoor hun gegevens ook lange tijd worden verwerkt.
- *Criterium 7 - Gegevens met betrekking tot kwetsbare betrokkenen:* Er is een machtsongelijkheid tussen werkgevers en werknemers. Werknemers zijn afhankelijk van hun werkgever en kunnen zich niet zomaar onttrekken aan de verwerking, omdat deze een voorwaarde is voor het dienstverband.

Scope van deze DPIA
Deze DPIA heeft als scope het softwarepakket Profit in de vorm van een Enterprise Resource Planning licentie.[4] Deze DPIA richt zich specifiek op de HRM- en Payroll-modules. Hierbij wordt tevens de native mobiele applicatie AFAS Pocket meegenomen. AFAS Pocket fungeert als een *lightweight client* die synchroniseert met de AFAS Online backend, waardoor de functionaliteiten van het pakket ook op mobiele formaten zoals smartphones en tablets beschikbaar zijn.

Aangezien de instelling zelf doel en middelen van de verwerking bepaalt (waaronder welke gegevenscategorieën worden opgeslagen en verwerkt in Profit), dient elke instelling zelfstandig te controleren of de in deze DPIA vermelde gegevens en verwerkingen hun specifieke situatie weerspiegelen, en deze waar nodig aan te passen. De verwerkingen waarin een hoge mate van vrijheid is voor de instelling zijn gelabeld met: *"Deze verwerking is aanpasbaar door instelling en daarmee niet representatief. Dit geldt als referentie."*

CRM als module is standaard onderdeel van Profit en biedt functionaliteit voor het registreren en beheren van organisaties, contactpersonen, activiteiten en dossiers. Binnen deze DPIA wordt de kernfunctionaliteit van CRM echter buiten scope gelaten. Voor zover CRM-objecten technisch aanwezig zijn (zoals de werkgeversrelatie of systeemmatig aangemaakte relaties), worden deze uitsluitend getoetst als onderliggende stamgegevens ten behoeve van HRM- en payrollprocessen, en niet als zelfstandig CRM-domein voor klant- of leadopvolging.

Net als CRM is Workflow- & Documentmanagement een standaard onderdeel van Profit, dit om het documentmanagement te ondersteunen. Alleen de functionaliteiten van workflow- & documentmanagement rond HR & Payroll processen vallen binnen de scope.

Tot slot vallen de supportverzoeken en de supportpagina's klant.afas.nl en help.afas.nl binnen de scope. De support is namelijk een integraal onderdeel van de dienstverlening en gebruikers worden bij vragen over de applicatie naar deze websites verwezen.

Buiten scope
Er zijn ook modules die buiten de scope van deze DPIA vallen en niet meegenomen worden in de beoordeling. Het gaat om de volgende modules:

- Abonnementen

[4] Uit een steekproef blijkt dat de meeste instellingen gebruikmaken van de ERP-licentie en de bijbehorende diverse modules.

- Financieel
- Fiscaal
- Ordermanagement
- Projecten

Buiten de scope van deze DPIA vallen ook de externe applicaties waarmee Profit koppelingen kan leggen binnen het applicatielandschap van de instelling (zoals die van de arbodienst).

Verder gaat deze DPIA ervan uit dat de verwerking van persoonsgegevens van minderjarigen in AFAS een uitzonderlijke situatie betreft, aangezien de meeste mensen in de beroepsbevolking volwassenen zijn. Een voorbeeld waarbij gegevens van minderjarigen verwerkt kunnen worden, is de registratie van de namen van kinderen van werknemers.

Tot slot is de AI-assistent 'Jonas' van AFAS niet opgenomen in de scope van deze DPIA. Dit besluit is genomen vanwege het beperkte gebruik dat uit de recente enquête naar voren is gekomen, alsook om onnodige vertraging in het proces te voorkomen. Een beoordeling hiervan kan, indien gewenst door de instellingen, op een later tijdstip worden uitgevoerd.

Methodologie
Deze DPIA is tot stand gekomen door een combinatie van documentatieonderzoek, technisch onderzoek en uitleg van AFAS in antwoord op vragen.

De documentatiebeoordeling bestaat uit het opvragen en analyseren van overeenkomsten, beleidsdocumenten, procedures en informatiebeveiligingscertificeringen. AFAS kreeg ook de gelegenheid om te reageren op bevindingen, aangezien er specifieke vervolgvragen werden gesteld. Dit deel van het onderzoek richtte zich voornamelijk op de juridische overeenkomsten die zijn gesloten met betrekking tot de verwerking van gegevens in AFAS.

Het technische onderzoek binnen de DPIA analyseert de technische aspecten van AFAS aan de hand van gebruiksscenario's (zie Bijlage 1 Technisch onderzoek). Deze scenario’s zijn opgesteld voor een gelijktijdig lopend assessment op een ander HR-systeem, in het kader van gelijke behandeling is besloten dezelfde scenario’s te gebruiken. De scenario’s zijn ingekort doordat de flexibiliteit in workflows een groot deel van de scenario’s (onderzoek) irrelevant maakt. De huidige scenario’s zien toe op de verschillende technische onderdelen/acties van de dienstverlening. Denk aan downloaden, delen, aanmaken, verwijderen en exporteren. Dit onderzoek sluit aan bij de juridische bevindingen en onderzoekt hoe gegevens worden verzameld, verwerkt, opgeslagen, gedeeld en beveiligd. Technische analyse van gegevensstromen, opslagmethoden, logboekregistratie, beveiligingsmaatregelen en privacy-instellingen is gebruikt om te beoordelen of de technische implementatie voldoet aan de AVG-vereisten:

1. Het onderscheppen van netwerkverkeer tijdens het uitvoeren van testscenario's in de applicatie;
2. Het analyseren van technische documentatie; en
3. Het analyseren van de gegevens die voortkomen uit verzoeken om inzage van betrokkenen.

Ook de technische documentatie wordt onderzocht en hierover zijn vragen gesteld aan AFAS.

Tot slot heeft SVC de DPIA van SIVON in ogenschouw genomen.[5]

DPIA-model
Deze DPIA is gebaseerd op het Nederlandse model DPIA voor overheidsinstanties.[6] Dit model is zeer geschikt voor de activiteiten van onderwijs- en onderzoeksinstellingen, aangezien deze ook taken van algemeen belang uitvoeren. Aangezien het hier om een overkoepelende DPIA gaat, zijn waar nodig wijzigingen aangebracht in de structuur van het oorspronkelijke model.

Het model bestaat uit vier delen.

- Deel A beschrijft de feiten van de gegevensverwerkingen;
- Deel B beoordeelt de rechtmatigheid van de in deel A verwerkte feiten;
- Deel C gaat over de risico's voor de rechten en vrijheden van betrokkenen; en
- Deel D gaat over de maatregelen die worden overwogen om die risico's aan te pakken.

[5] SIVON heeft in samenwerking met een aantal externe partijen een DPIA op AFAS. In deze DPIA is ingezoomd op de modules CRM, HRM en Payroll. Geraadpleegd op 1 december 2025: https://sivon.nl/dpia-afas-2023/.

[6] Model DPIA Rijksdienst, geraadpleegd op 6 mei 2025 via https://www.kcbr.nl/sites/default/files/2023-09/Model%20DPIA%20Rijksdienst%20v3.0.pdf.

Part A Beschrijving van de gegevensverwerking

Deel A van deze DPIA geeft een overzicht van de relevante feiten van de gegevensverwerkingsactiviteiten. Het beschrijft de gegevensverwerkingsactiviteiten, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingsactiviteiten. Daarnaast geeft deel A een overzicht van de verwerkte persoonsgegevens, de betrokken partijen en de technieken en methoden van gegevensverwerking. Ook komen het wettelijke kader, het beleidskader en de bewaartermijnen aan bod.

A.1 Beschrijving van de diensten

A.1.1 Applicatielandschap

Deze DPIA kijkt naar Profit (ERP licentie) met een focus op de modules HRM en Payroll. Vanuit de instelling kunnen er koppelingen gemaakt worden met AFAS om zo gegevens uit te wisselen met andere systemen, deze gekoppelde systemen vallen buiten scope.

A.1.1.1 AFAS als service

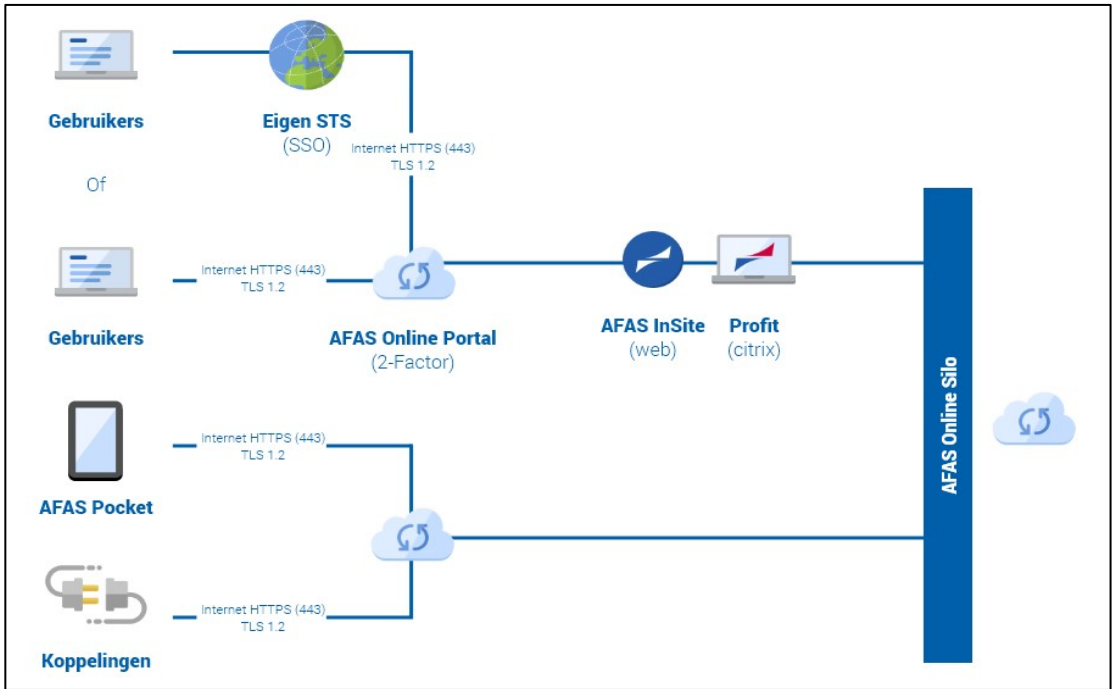
AFAS levert een multi-tenant cloudplatform waarmee de software AFAS(ERP) aan haar klanten wordt aangeboden. Zoals vermeld in A.3 Doeleinden van de gegevensverwerking ondersteunt AFAS hiermee, via de HRM en Payroll modules, instellingen bij meerdere essentiële HR-gerelateerde processen.

A.1.1.2 Cloudplatform

AFAS Online, als cloudplatform, is niet gehost op servers van AFAS of van de instellingen maar volledig op externe infrastructuur. Het is geïnstalleerd op servers in de datacenters van Leaseweb[7] via Infrastructure as a Service (IaaS). IaaS is een cloudservice waarbij je via het internet toegang krijgt tot IT-infrastructuur (servers, opslag, netwerk) die, in dit geval, door AFAS wordt beheerd, zodat je deze op aanvraag kunt gebruiken zonder zelf fysieke hardware te hoeven bezitten of onderhouden. Voor meer details [zie Hoofdstuk #]. Deze servers worden periodiek gecertificeerd, voor meer details zie [Hoofdstuk # Beveiligingscertificeringen].

AFAS biedt een multi-tier applicatiearchitectuur waarbij Profit de centrale backoffice-laag vormt, AFAS Online de cloud-infrastructuur en beheerplatform, InSite/OutSite de portal-lagen voor respectievelijk interne en externe selfservice, en Pocket/Profit-webversie de client-varianten vormen die verschillende apparaten en connectiviteitspatronen bedienen.

[7] AFAS Help Center Nederland, *AFAS Online Continuïteit*, geraadpleegd op 4 december 2025 via https://klant.afas.nl/afas-online/continuiteit.



Figuur A-1 Algemeen stroomschema applicatie landschap AFAS.[8]

A.1.1.3 Gebruikersendpoints

Klanten maken gebruik van Profit als backoffice, AFAS InSite als medewerkersportaal en AFAS Pocket als mobiele applicatie variant van InSite en/of twee factor authenticatie via push-berichten. Toegang wordt geregeld via een login-portaal met verplichte 2-factor authenticatie (SMS, push of SSO via federatie met Secure Token Service). Administraties, werkgevers en modules worden beheerd in afgeschermde SQL-databases per klant.

A.1.1.4 Profit (Backoffice)[9]

Profit is de reguliere Windowsapplicatie waarmee je als beheerder, salarisadministrateur en/of HR-manager toegang krijgt tot de AFAS-omgeving. Profit gebruikt Citrix Workspace als de traditionele lokale applicatie benadering. Hiermee is er directe toegang tot de applicatie. Dit is een virtualised application delivery-model waarbij gebruikers via Citrix Workspace verbinding maken met de AFAS Online-infrastructuur.

Citrix Workspace functioneert als een remote application server die de volledige Profit-omgeving naar de clientmachine streamt. Dit model biedt compatibiliteit met oudere systemen en volledige functionaliteit inclusief printmogelijkheden en caching. De applicatie draait virtueel op de Citrix-servers bij Leaseweb en wordt via het netwerk naar het lokale workstation getransporteerd.

[8] AFAS Help Center Nederland, *AFAS Online Architectuur*, geraadpleegd op 4 december 2025 via https://klant.afas.nl/afas-online/architectuur.

[9] AFAS Help Center Nederland, *AFAS Online Architectuur*, geraadpleegd op 4 december 2025 via https://klant.afas.nl/afas-online/architectuur.

De applicatie kan ook via de browser[10] benaderd worden. De webversie van Profit is een browser-gebaseerde client-variant waarvoor geen software-installatie nodig is. Dit is een HTML5/JavaScript-implementatie die rechtstreeks in ondersteunde browsers (Chrome, Firefox, Safari, Edge) wordt uitgevoerd zonder tussenkomst van Citrix. Deze benadering biedt meer flexibiliteit en lagere systeemvereisten dan Citrix Workspace. Echter, de webversie kent enkele beperkingen: printen is niet ondersteund, en clipboard-operaties werken anders dan in de Citrix-variant.

A.1.1.5 AFAS InSite

AFAS InSite[11] is een intranet-platform dat als Self Service Employee Portal (SSEP) en communicatiekanaal voor medewerkers functioneert. AFAS InSite biedt een web-interface waarin medewerkers HR-zaken zelf kunnen regelen; verlof aanvragen, loonstroken inzien, persoonlijke gegevens bijwerken, en eventueel bedrijfsnieuws tot zich nemen. Leidinggevenden en HR-managers kunnen ook hun HR-werkzaamheden via AFAS InSite regelen. AFAS InSite werkt direct op basis van gegevens uit de AFAS-backoffice.

A.1.1.6 AFAS Pocket App

AFAS Pocket is een native mobiele applicatie (iOS en Android) die het softwarepakket in het kleinere mobiele formaat van smartphones en tablets biedt. AFAS Pocket fungeert als een lightweight client die met AFAS Online backend synchroniseert. De app ondersteunt twee primaire processen:

- Twee-factorauthenticatie voor veilig inloggen op Profit en InSite via push-authenticatie.
- Mobile workflow execution waarmee gebruikers onderweg selfservice-taken kunnen uitvoeren—verlofaanvragen insturen, uren boeken, dossieritems indienen, projecttaken beheren, signalen ontvangen, zakelijke berichten verzenden, en teamschema's controleren.

A.1.1.7 AI-Assistent Jonas[12]

Jonas is de verzamelnaam voor de AI-functionaliteit binnen Profit en kan in verschillende workflows en processen worden ingevoegd. In de kern voert Jonas vooraf gedefinieerde AI-opdrachten uit op gegevens die in een workflow beschikbaar zijn, zoals inhoud van dossiers, voorstel voor reacties (bv. Bij goed- of afkeuren van een declaratie) of audio-opnamen. De resultaten worden teruggegeven in velden of reacties binnen dezelfde workflowstap, zonder dat eindgebruikers zelf prompts hoeven op te stellen. Via "Jonas-opdrachten" kan een beheerder bepalen op welk moment in de workflow deze wordt gebruikt en welke input (bijvoorbeeld tekst of transcriptie van audio) wordt verwerkt.

De functionaliteiten van Jonas zijn:

[10] AFAS Help Center Nederland, *Webversie in laats van Citrix Workspace*, geraadpleegd op 4 december 2025 via https://help.afas.nl/help/NL/SE/plv2_User_2FA_web.htm.

[11] AFAS Help Center Nederland, *Mogelijkheden van InSite*, geraadpleegd op 4 december 2025 via https://help.afas.nl/help/NL/SE/plv2_User_2FA_web.htm.

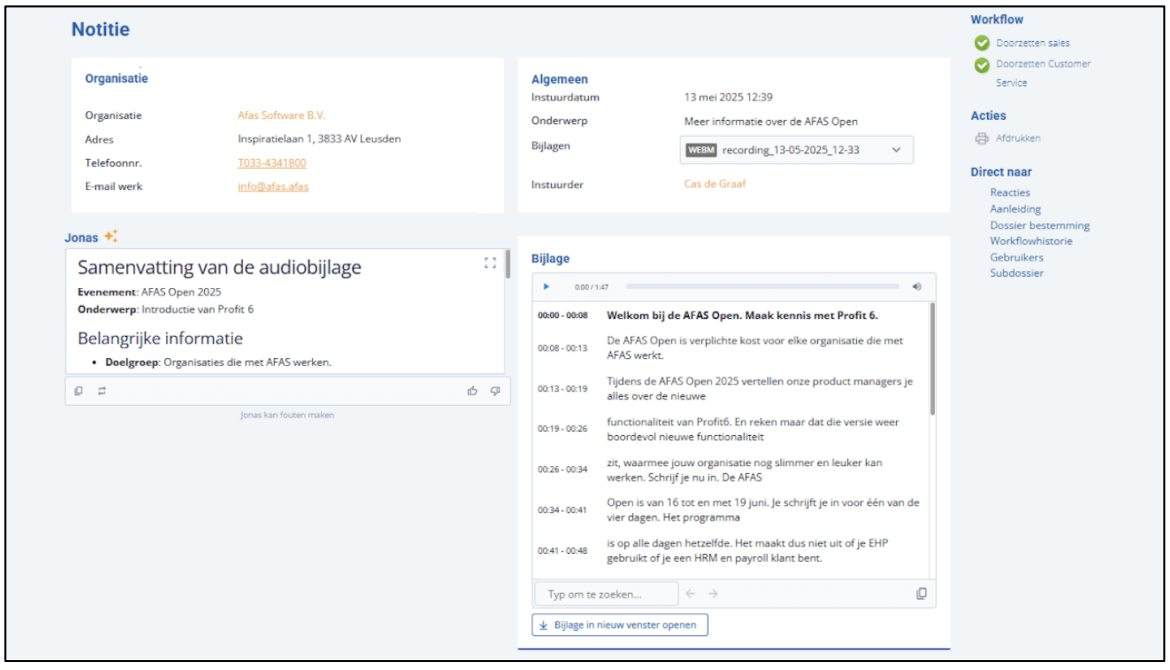
[12] AFAS Help Center Nederland, *AI in AFAS (Jonas)*, geraadpleegd op 18 december 2025 via https://help.afas.nl/help/NL/SE/jonas.htm.

Transcriptie
Het omzetten van een audio opname naar tekst.

Samenvatten
Samenvatten van tekst en het genereren van tekstvoorstellen bijvoorbeeld in workflow reacties.

Geavanceerde analysetaken
Zoals het laten uitvoeren van een “slimme analyse”. AFAS positioneert dit als een generiek mechanisme waarbij de AI-opdracht op de achtergrond de inhoud beoordeelt en een tekstuele uitkomst teruggeeft, die de medewerker kan gebruiken bij besluitvorming in het proces. Hier wordt gebruik gemaakt van: information extraction, semantic role labeling en deviation detection.

De instelling bepaalt waar in een workflow welke functionaliteit wordt ingevoegd. Enkele voorbeelden die door AFAS en partners worden gegeven zijn: spraaktaak (gespreksverslagen), automatische verwerking van declaraties, controle loonstroken/contracten, beantwoorden HR-vragen en reactie voorstellen binnen workflows.



Figuur A-2 Overzicht workflows.

A.1.1.8 Connector

AFAS ondersteunt via *Connector* een standaard set aan koppelingen met applicaties/diensten van derde partijen of het maken van een eigen koppeling. Deze standaard koppelingen worden onderhouden en gecertificeerd.[13]

AFAS heeft geen invloed op welke koppelingen de klant aanmaakt of in gebruik neemt. Alle koppelingen werken wel volgens dezelfde standaard functionaliteit.

Voor meer over koppelingen zie *A.6.8 Koppelingen*.

[13] AFAS Partnerportal, *Koppel je favoriete software aan AFAS*, geraadpleegd op 5 december 2025 via https://partner.afas.nl/koppelingen.

A.2 Wettelijk kader en beleidskader

A.2.1 Algemeen contractueel kader[14]

Klanten maken gebruik van een standaard SaaS-oplossing bij AFAS. Voor iedere klantrelatie worden drie documenten[15] gehanteerd:

- een offerte;
- de Algemene Voorwaarden (AV); en
- een Service Level Agreement (SLA).

Wanneer een klant de offerte (vaak digitaal via het klantportaal) ondertekent, stemt deze tegelijkertijd in met de toepasselijkheid van de AV en de SLA. Dat betekent dat klanten geen individuele contractuele voorwaarden kunnen afdwingen.

AFAS biedt geen afzonderlijke verwerkersovereenkomsten aan klanten aan. De bepalingen over gegevensverwerking maken integraal deel uit van de SLA.[16] Daarmee wordt niet gebruikgemaakt van sectorstandaarden.[17]

In de SLA worden geen specifieke categorieën van persoonsgegevens, verwerkingsdoeleinden en bewaartermijnen opgenomen. AFAS geeft aan dat de klant zelf bepaalt welke gegevens in de software worden ingevoerd, en dat de aard van die gegevens kan variëren. Indien gewenst kunnen de categorieën persoonsgegevens op verzoek van de klant worden opgeslagen bij de overeenkomst. Wijzigingen daarin dienen door de klant aan AFAS te worden doorgegeven. Dit geldt echter niet voor onderwerpen zoals de verwerkingsdoeleinden en bewaartermijnen; deze kunnen niet opgeslagen worden bij de overeenkomst.[18]

AFAS heeft in de AV en de SLA aangegeven dat ze continu bezig zijn met het verbeteren en het veranderen van de dienstverlening. Klanten die het niet eens zijn met een wijziging, kunnen een ‘verbetersuggestie’ insturen. AFAS zal vervolgens onderzoeken of een wijziging noodzakelijk is. De overeenkomst kan in het uiterste geval na wijziging beëindigd worden. De oude voorwaarden gelden dan nog twee maanden.

A.2.2 Corporate AFAS beleid

Om de vertrouwelijkheid van klantgegevens te waarborgen, hanteert AFAS een intern privacybeleid. Alle medewerkers volgen verplichte trainingen op het gebied van

[14] AFAS Klantportaal, *Service Level Agreement en Algemene Voorwaarden*, geraadpleegd op 7 november 2025 via https://klant.afas.nl/sla-av.

[15] AFAS actualiseert deze documenten periodiek, doorgaans per kwartaal.

[16] Artikel 28, lid 3 van de AVG bepaalt dat afspraken tussen de verwerkingsverantwoordelijke en de verwerker mogen worden vastgelegd via een overeenkomst óf via een ‘andere rechtshandeling’. Dat laatste is hier van toepassing.

[17] Zoals het SURF Model Verwerkersovereenkomst – SURF Juridisch Normenkader (Cloud)services 3.0, of het SURF Model Verwerkersovereenkomst 4.0.

[18] AFAS Klantportaal, *Service Level Agreement en Algemene Voorwaarden*, geraadpleegd op 16 april 2026 via https://klant.afas.nl/sla-av#sla.

informatiebeveiliging en handelen volgens diverse vastgelegde richtlijnen en risicomanagementbeleid.

A.3 Doeleinden van de gegevensverwerking

Dit hoofdstuk gaat over de doeleinden waarvoor AFAS de persoonsgegevens van gebruikers verwerkt. Deze doeleinden omvatten voornamelijk personeels- en salarisadministratie. Door de doeleinden van instellingen te beschrijven, krijg je een algemeen beeld van waarvoor Profit (HRM en Payroll) wordt gebruikt. De hieronder beschreven doeleinden zijn gebaseerd op beschrijvingen van de twee AFAS-modules en het onderzoek naar de feitelijke verwerkingsactiviteiten.

De doeleinden zijn onderverdeeld in doeleinden op basis van de functies die worden beschreven in het model 'Hoger Onderwijs Referentie Architectuur' (HORA) en andere doeleinden. De HORA is een bedrijfsfunctiemodel voor instellingen. Het beschrijft de functies van een organisatie, onafhankelijk van hoe deze functies in een specifieke organisatie worden geïmplementeerd. Aangezien de HORA de essentiële functies van instellingen op hoog niveau beschrijft, is het een goed model om de belangrijkste doeleinden voor gegevensverwerking in applicaties zoals Profit uit af te leiden. Door de HORA als referentie te gebruiken, wordt ook gewaarborgd dat instellingen gemakkelijk de juiste plaats in hun organisatiestructuur kunnen vinden om eventuele maatregelen of wijzigingen uit deze DPIA te implementeren. De tweede categorie bestaat uit 'ondersteunende' doeleinden, die de hoofdprocessen ondersteunen. De derde categorie bestaat uit ‘eigen’ bepaalde doeleinden van AFAS.

A.3.1 Door de instellingen vastgestelde doeleinden van HORA

A.3.1.1 Bedrijfsvoering - HRM

Het ervoor zorgdragen dat er competente medewerkers beschikbaar zijn voor de uitvoering van bedrijfsprocessen.

1. **Formatieplanning**
   Het vaststellen welke budgetten en formatieplaatsen beschikbaar zijn voor afdelingen.
2. **Werving en selectie**
   Het werven en selecteren van nieuwe medewerkers.
3. **Medewerkersontwikkeling**
   Het expliciet ontwikkelen van de kennis en vaardigheden van medewerkers, inclusief de daarbij behorende begeleiding.
4. **Medewerkersbeoordeling**
   Het beoordelen van de prestaties van de medewerker en het besluiten over beloning en promotie alsook over ontslag en demotie.
5. **Medewerkersadministratie**
   Het administreren van alle gegevens van medewerkers.
6. **Tijdregistratie**
   Het registreren waaraan de tijd van medewerkers is besteed.
7. **Salaris- en declaratieverwerking**
   Het berekenen en uitkeren van het salaris en declaraties van medewerkers.
9. **Ziekte- en verlofadministratie**
   Het administreren van ziekte en verlof van medewerkers.

A.3.1.2 Sturing - verantwoording

De informatie uit AFAS wordt ook gebruikt om inzicht te krijgen in het functioneren van de organisatie.

10. Interne rapportages

Het beschikbaar stellen van informatie over het functioneren van de organisatie aan interne partijen.

A.3.2 Door de instellingen vastgestelde ondersteunende doeleinden

Instellingen gebruiken AFAS voor de in paragraaf 2.1 beschreven doeleinden. Om ervoor te zorgen dat AFAS effectief, efficiënt en veilig functioneert, verwerkt AFAS persoonsgegevens voor de volgende doeleinden. Verwerkingsactiviteiten voor deze doeleinden zijn verspreid vastgelegd in de SLA. Zie ook hoofdstuk A.2

Wettelijk kader en beleidskader. De SLA geeft echter onvoldoende duidelijkheid over welke specifieke gegevens, zoals het IP-adres, voor deze verwerkingen worden gebruikt.

11. De dienst leveren en up-to-date houden
De nodige handelingen uitvoeren om ervoor te zorgen dat de dienst continu en naar behoren functioneert, zoals opslag, hosting, het verhelpen van bugs, enz.

12. De dienst beveiligen
Zorgen voor de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens in de dienst en zorgen voor de veerkracht van de dienst, onder meer door identificatie en authenticatie te vergemakkelijken en back-ups te maken.

13. De dienst personaliseren
Ondersteuning bieden voor individuele gebruikersvoorkeuren en efficiënte informatievoorziening.

14. Klantenservice bieden
Opties aanbieden waarmee klanten en gebruikersondersteuning kunnen aanvragen en ontvangen wanneer ze problemen ondervinden.

15. De dienst verbeteren
Wijzigingen aanbrengen in de dienst in overeenstemming met de wensen van klanten.

A.3.3 Door AFAS vastgestelde doeleinden

AFAS stelt geen verwerkingsverantwoordelijke te zijn. In lijn daarmee ontbreekt documentatie waarin expliciet is vastgelegd dat AFAS zelfstandig de doeleinden van de gegevensverwerking bepaalt. Tijdens het technisch onderzoek is echter gebleken dat AFAS feitelijk een (verdere) verwerkingen uitvoert die niet expliciet zijn omschreven of begrensd in de SLA voor het volgende doel[19]:

[19] AFAS Service License Agreement januari 2026, *paragraaf 2.3.6*, geraadpleegd op 27 maart 2026 via https://klant.afas.nl/sla-av.. Zie voor de specifieke verwerkingsactiviteiten de volgende paragrafen in de DPIA: A.5.6.1, A.5.6.2, A.5.6.3 en A.5.6.4 en de A.5.6.5.

Monitoring

- Storingen voorkomen of in een vroeg stadium oplossen
- Algemene gebruikersstatistieken verzamelen
- Anonieme statistieken uit de klantomgeving te verzamelen
- Het meten en analyseren van systemeenreactietijden
- Het verzamelen, monitoren en analyseren van loggegevens om misbruik te voorkomen

SURF stelt zich op het standpunt dat AFAS, althans voor deze specifieke verwerkingsactiviteiten, kwalificeert als zelfstandig verwerkingsverantwoordelijke, nu zij feitelijk invloed uitoefent op het doel en de middelen van deze (verdere) verwerkingen. Zie A.7 voor een uitgebreidere analyse van de rolverdeling.

A.4 Verwerkte persoonsgegevens

Volgens artikel 4 (1)(a) van de AVG zijn persoonsgegevens:

> *”alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.’’*

A.4.1 Categorieën betrokkenen

AFAS verwerkt in Profit de volgende categorieën betrokkenen:

- Werknemers[20]
- Personeel niet in loondienst
- Oud-werknemers en (oud)personeel niet in loondienst
- Beheerders
- Docenten
- Sollicitanten
- Noodcontactpersoon/partners/kinderen van (oud-)werknemers[21]

A.4.2 Categorieën persoonsgegevens

A.4.2.1 Verzoek om toegang tot persoonsgegevens

Als onderdeel van het technische onderzoek zijn inzageverzoeken[22] ingediend bij de leverancier.

We hebben geen reactie op de inzageverzoeken ontvangen. SURF heeft de mogelijkheid om de data die beschikbaar is voor de verwerkingsverantwoordelijke handmatig te exporteren, maar op het gebied van persoonsgegevens verwerkt in verwerkingen onzichtbaar voor verwerkingsverantwoordelijke zijn de inzageverzoeken tot op heden onvolledig.

A.4.2.2 Categorieën

Voor deze DPIA zijn de persoonsgegevens in Profit onderverdeeld in categorieën. Elke categorie bevat persoonsgegevens die qua aard vergelijkbaar zijn. Zie bijlage 2 voor een beschrijving van de categorieën. Sommige persoonsgegevens kunnen in meerdere categorieën thuishoren. In dat geval worden ze ingedeeld in de categorie met de hoogste gevoeligheid.

[20] Binnen het kader van deze DPIA vallen stagiairs onder de categorie 'werknemers'.

[21] De verwerking van persoonsgegevens van minderjarigen die gebruikers zijn in AFAS valt buiten het toepassingsgebied van deze DPIA. Zie paragraaf 'Scope' in de inleiding.

[22] Binnen het technisch onderzoek en communicatie rond dit assessment gebruiken we ook de Engelse vertaling van inzageverzoek; Data Subject Access Request (DSAR).

In de onderstaande tabellen zijn sommige gegevens van een vergelijkbaar type voor de duidelijkheid gegroepeerd in subgroepen. De subgroep 'Naam' bevat bijvoorbeeld de naam die wordt gebruikt om iemand aan te spreken, de voornaam, achternaam, initialen, bijnaam en voorvoegsels. Voor een volledig overzicht van de persoonsgegevens kunt u contact opnemen met SURF Vendor Compliance.

Opgemerkt moet worden dat de persoonsgegevens in deze tabel niet één-op-één overeenkomen met de datavelden in AFAS. Een deel van de gegevens betreft afgeleiden (bijvoorbeeld leeftijd als afgeleide van de geboortedatum) of komt voor in veelvoorkomende geüploade documenten, zoals een handtekening in een arbeidscontract.

Direct identificeerbare persoonsgegevens

Persoonsgegevens	Betrokkene	Type persoonsgevens	Herkomst
Naam	Werknemers, docenten, sollicitanten, noodcontactpersoon/ partners/kinderen van (oud-)werknemers, personeel niet in loondienst, voormalige werknemers	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
Geboortedatum	Werknemers, docenten, partners/kinderen van oud-werknemers, personeel niet in loondienst, voormalige werknemers	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
ID-gegevens	Werknemers, ex-werknemers, docenten, personeel niet in loondienst	Bijzonder (in combinatie met nationaliteit)	Betrokkene of andere gebruikers van Profit / ATS-systeem
Bankgegevens	Werknemers, ex-werknemers, docenten, personeel niet in loondienst	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
Gebruiker	Werknemers, ex-werknemers, docenten, personeel niet in loondienst	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
Handtekening	Werknemers, ex-werknemers, docenten, personeel niet in loondienst	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
ID-nummer	Werknemers, ex-werknemers, docenten, personeel niet in loondienst	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
Werknemersnummer	Werknemers, ex-werknemers, docenten, personeel niet in loondienst	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
IBAN	Werknemers, ex-werknemers, docenten, personeel niet in loondienst	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
Foto	Werknemers, ex-werknemers, docenten, personeel niet in loondienst	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem

Nationaal identificatienummer	Werknemers, ex-werknemers, docenten, personeel niet in loondienst	Gevoelig	Betrokkene of andere gebruikers van Profit / ATS-systeem

Contactgegevens

Persoonsgegevens	Betrokkene	Type persoonsgegevens	Herkomst
Adres	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
E-mailadres	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
Telefoonnummer	Werknemers, docenten, noodcontactpersoon/partners/kinderen van (oud-)werknemers, niet-betaalde medewerkers	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
Postcode	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem

Demografische gegevens

Persoonsgegevens	Betrokkene	Type persoonsgegevens	Herkomst
Titel	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
Geslacht	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
Leeftijd	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
Datum van ingaan van pensioen	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Nationaliteit	Werknemers, docenten, niet-gesalarieerd personeel	Bijzonder (in combinatie met land/geboorteplaats)	Betrokkene of andere gebruikers van Profit / ATS-systeem
Land van geboorte	Werknemers, docenten, niet-gesalarieerd personeel	Bijzonder (in combinatie met nationaliteit)	Betrokkene of andere gebruikers van Profit / ATS-systeem
Burgerlijke staat	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
Opleiding	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
Werkervaring	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem

Type relatie	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit / ATS-systeem
Locatie	Werknemers, docenten, niet-gesalarieerd personeel	Gevoelig	Betrokkene of andere gebruikers van Profit / ATS-systeem

Organisatorische gegevens

Persoonsgegevens	Betrokkene	Type persoonsgegevens	Herkomst
Contractuele gegevens	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Afdeling	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Werkplek	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Functie	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Deeltijdfactor	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Nevenactiviteiten	Werknemers, docenten, niet-gesalarieerd personeel	Normaal, mogelijk gevoelig of speciaal	Betrokkene of andere gebruikers van Profit
Eigenaarsaccount	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Beoordelingen	Werknemers, docenten, niet-gesalarieerd personeel	Normaal, mogelijk gevoelig of speciaal	Betrokkene of andere gebruikers van Profit
Overeenkomsten opleiding	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Competenties	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Afwezigheidsgegevens	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Verlofgegevens	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Betalingen	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Contractuele gegevens	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Documenten	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Notities	Werknemers, docenten, niet-gesalarieerd personeel	Normaal, mogelijk gevoelig of speciaal	Betrokkene of andere gebruikers van Profit
Arbeidsrelatie	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Activiteiten	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Gebeurtenissen	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit

Gesprekverslagen	Werknemers, docenten, niet-gesalarieerd personeel	Normaal, mogelijk gevoelig of bijzonder	Betrokkene of andere gebruikers van Profit
E-mails	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Salarisgegevens	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Verzekeringsgegevens	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit
Loonbeslag	Werknemers, docenten, niet-gesalarieerd personeel	Normaal	Betrokkene of andere gebruikers van Profit

Gezondheidsgegevens[23]

Persoonsgegevens	Betrokkene	Type persoonsgegevens	Herkomst
Afwezigheidsgegevens	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Bijzonder	Betrokkene of andere gebruikers van Profit
Belastinggegevens	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Bijzonder	Betrokkene of andere gebruikers van Profit
Salarisgegevens	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Bijzonder	Betrokkene of andere gebruikers van Profit
Pensioengegevens	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Bijzonder	Betrokkene of andere gebruikers van Profit
Uitkeringen	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Bijzonder	Betrokkene of andere gebruikers van Profit
Arbeidsrelatie	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Bijzonder	Betrokkene of andere gebruikers van Profit

Financiële gegevens

Persoonsgegevens	Betrokkene	Type persoonsgegevens	Bron
Salarisgegevens	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Gevoelig	Betrokkene of andere gebruikers van Profit
Onkostendeclaraties	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Gevoelig	Betrokkene of andere gebruikers van Profit

[23] Hoewel deze persoonsgegevens op het eerste gezicht geen gezondheidsgegevens lijken, geven ze indirect wel informatie over iemands gezondheidstoestand. Denk hierbij aan registraties van afwezigheid wegens zwangerschap of zorgverlof.

Documenten	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Gevoelig	Betrokkene of andere gebruikers van Profit
Contractgegevens	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Gevoelig	Betrokkene of andere gebruikers van Profit
Reisgegevens	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Gevoelig	Betrokkene of andere gebruikers van Profit
Loonbeslag	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Gevoelig	Betrokkene of andere gebruikers van Profit
Arbeidsrelatie	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Gevoelig	Betrokkene of andere gebruikers van Profit
Secundaire arbeidsvoorwaarden	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Gevoelig	Betrokkene of andere gebruikers van Profit
Pensioengegevens	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Gevoelig	Betrokkene of andere gebruikers van Profit
Salarisgegevens	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Gevoelig	Betrokkene of andere gebruikers van Profit
Onkostendeclaraties	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Gevoelig	Betrokkene of andere gebruikers van Profit
Documenten	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Gevoelig	Betrokkene of andere gebruikers van Profit
Contractgegevens	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Gevoelig	Betrokkene of andere gebruikers van Profit
Levenslange lijfrente	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Gevoelig	Betrokkene of andere gebruikers van Profit

Vakbond gegevens

Persoonsgegevens	Betrokkene	Type persoonsgegevens	Bron
Salarisgegevens (compensatie voor vakbondscontributie)	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Bijzonder	Betrokkene of andere gebruikers van Profit

Politieke gegevens

Persoonsgegevens	Betrokkene	Type persoonsgegevens	Bron
Salarisgegevens (politiek verlof)	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel	Bijzonder	Betrokkene of andere gebruikers van Profit

Overige gegevens

In Profit is het mogelijk om vrije velden aan te maken. Conform handleiding van AFAS is het bij het aanmaken van vrije velden cruciaal om te specificeren of deze gevoelige of bijzondere persoonsgegevens (mogen) bevatten.[24] Persoonsgegevens labelen is een standaard functionaliteit in Profit.

Persoonsgegevens	Betrokkene	Type persoonsgevens	Bron
Vrije velden	Werknemers, docenten, noodcontactpersoon/ partners/kinderen van (oud-)werknemers, personeel niet in loondienst, voormalige werknemers	Bijzonder	Betrokkene of andere gebruikers van Profit / ATS-systeem

Diagnostische/loggegevens

Aangezien dit een overkoepelende DPIA is, die zich voornamelijk richt op risico's die inherent zijn aan het gebruik van de dienst die de leverancier aanbiedt, zijn de diagnostische gegevens die leveranciers gewoonlijk verzamelen cruciaal. De verwerking van deze gegevens kan op de achtergrond plaatsvinden zonder dat gebruikers en beheerders hiervan op de hoogte zijn, wat kan leiden tot een gebrek aan transparantie. De onderstaande tabel toont de diagnostische gegevens die uit het onderzoek voor deze DPIA naar voren zijn gekomen. De volledigheid van deze dataset is niet geverifieerd, omdat SURF geen reactie op de inzageverzoeken heeft ontvangen.

Persoonsgegevens	Type persoonsgevens	Bron
Logging	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel, bestuurders	Profit
Door cookies verzamelde gegevens	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel, bestuurders	Betrokkene, Profit
Apparaat gegevens	Werknemers, ex-werknemers, docenten, niet-gesalarieerd personeel, bestuurders	Profit

A.4.2.3 Bijzondere categorieën van persoonsgegevens

Artikel 9 van de AVG verbiedt de verwerking van bijzondere categorieën van persoonsgegevens, waaronder persoonsgegevens waaruit het ras of de etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen of het lidmaatschap van een vakvereniging blijken, en de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, gegevens betreffende de gezondheid of gegevens betreffende het seksleven of de seksuele geaardheid van een natuurlijke persoon. Dit soort persoonsgegevens mag alleen worden verwerkt wanneer een uitzondering uit artikel 9, lid 2, van toepassing is.

[24] AFAS Help Center Nederland, *Vrije velden kenmerken als Privacygegevens*, geraadpleegd op 11 december 2025 via https://help.afas.nl/help/NL/SE/Crm_Config_PerOrg_Relat_AVG.htm#o93144.

De meeste bijzondere persoonsgegevens in Profit zijn gezondheidsgegevens. Instellingen kunnen in Profit registreren wanneer werknemers afwezig zijn, bijvoorbeeld vanwege ziekte of zwangerschap, en de gegevens over de ziekte classificeren. Zij kunnen hiervoor hun eigen categorieën bepalen. De ziekte van werknemers heeft ook invloed op hun ziekte-uitkering en dus op hun salaris. Verder bevat Profit gezondheidsgegevens over gebruikers die vanwege ziekte of een handicap in aanmerking komen voor bepaalde uitkeringen of belastingvoordelen.

Profit kan ook politieke en vakbondsgegevens bevatten. Werkgevers kunnen werknemers politiek verlof toekennen en vakbondscontributie compenseren, wat van invloed is op hun salaris.

Bovendien geeft de nationaliteit in combinatie met de geboorteplaats, het geboorteland en de foto het ras of de etnische afkomst van een betrokkene weer en is daarom een bijzondere categorie persoonsgegevens.

Ten slotte kunnen vrije velden, beoordelingen, notities, gespreksverslagen en nevenactiviteiten mogelijk bijzondere categorieën persoonsgegevens bevatten, afhankelijk van wat er is geregistreerd.

A.4.3 Gevoelige persoonsgegevens

Sommige persoonsgegevens zijn volgens artikel 9 niet bijzonder, maar kunnen gevoelig zijn vanwege hun relatief grote impact op iemands privacy. Persoonsgegevens die informatie onthullen over iemands financiële situatie worden als gevoelig beschouwd.

Er zijn veel financiële gegevens in Profit, voornamelijk over het salaris van werknemers. Profit kan ook worden gebruikt om te registreren hoe de arbeidsrelatie tussen werknemers en hun werkgevers van invloed is op hun salaris, hoe het pensioen van werknemers wordt beïnvloed door bepaalde omstandigheden, of er loonbeslag op iemands salaris ligt en of iemand uitkeringen ontvangt.

Bepaalde workflows, zoals beoordelingen, gespreksverslagen, notities en nevenactiviteiten, kunnen gevoelige gegevens bevatten.

A.4.3.1 Nationaal identificatienummer

Werkgevers kunnen nationale identificatienummers (BSN's) registreren in Profit. Zij zijn verplicht deze te registreren voor belastingdoeleinden en mogen deze alleen verwerken in overeenstemming met de Wet op de loonbelasting.

A.4.4 Herkomst van persoonsgegevens

Volgens artikel 13 en 14 van de AVG moeten betrokkenen worden geïnformeerd over de verwerking van hun persoonsgegevens, ongeacht of deze rechtstreeks bij hen zijn verzameld of via een andere bron. In dit geval kunnen persoonsgegevens op twee manieren in AFAS terechtkomen:

1 Handmatige invoer: Gegevens kunnen handmatig worden ingevoerd. Persoonsgegevens worden dan rechtstreeks bij de gebruikers verzameld, door andere gebruikers ingevoerd of automatisch gegenereerd op basis van al aanwezige gegevens of gebruikersgedrag.

2 Koppeling met een Applicant Tracking Systeem (ATS) van een derde partij of de recruitmentsoftware van AFAS (vergelijkbaar met een ATS)[25]: Profit kan worden gekoppeld aan een ATS-systeem, waardoor gegevens van nieuwe medewerkers automatisch in AFAS worden overgenomen. [26]

[25] Met de recruitmentsoftware van AFAS wordt bedoeld de' Sollicitant Self Service'.

[26] Deze gekoppelde (externe) applicaties vallen buiten de scope van deze DPIA. Zie paragraaf 'Scope' in de inleiding.

A.5 Gegevensverwerkingsactiviteiten

In dit hoofdstuk worden alle concrete gegevensverwerkingsactiviteiten via dienstverlening van AFAS systematisch in kaart gebracht, zodat helder wordt welke categorieën van persoonsgegevens met welk doel worden verwerkt.

Verwerking volgens artikel 4, lid 2:

> *"een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, samenvoegen, afschermen, wissen of vernietigen van gegevens."*

Onderstaande beschrijvingen gaan dieper in op de details en zijn gebaseerd op de daadwerkelijke verwerkingsactiviteiten zoals vastgesteld in het onderzoek voor deze DPIA.

De functionaliteit van Profit, binnen de vastgelegde scope, bestaat voor een groot deel uit processen. Deze processen worden bepaald door de soorten activiteiten en handelingen die instellingen op gegevens kunnen uitvoeren, zoals indienen en goedkeuren/afwijzen. Dit deel van de verwerkingsactiviteit kan worden omschreven als het 'hoe'.

Instellingen hebben echter veel vrijheid en eigen verantwoordelijkheid in de soorten gegevens en mate van toegang die zij in deze processen willen gebruiken. Dit deel van de verwerkingsactiviteit kan worden omschreven als het 'wat'. Hierdoor kunnen de verwerkingsactiviteiten voor verschillende instellingen er verschillend uitzien, afhankelijk van de manier waarop zij de door AFAS aangeboden processen hebben geïmplementeerd, hoewel sommige processen minder flexibel zijn dan andere.

In dit hoofdstuk worden labels gebruikt om de verbanden tussen de processen en andere onderdelen van deze DPIA aan te geven, zoals de soorten persoonsgegevens en de doeleinden van verwerking. Het is echter belangrijk te beseffen dat de doeleinden en de verwerking van persoonsgegevens zoals beschreven in A.3 Doeleinden van de gegevensverwerking en A.4

Verwerkte persoonsgegevens, kunnen afwijken van de standaardinstellingen.

A.5.1 Verzamelen van gegevens

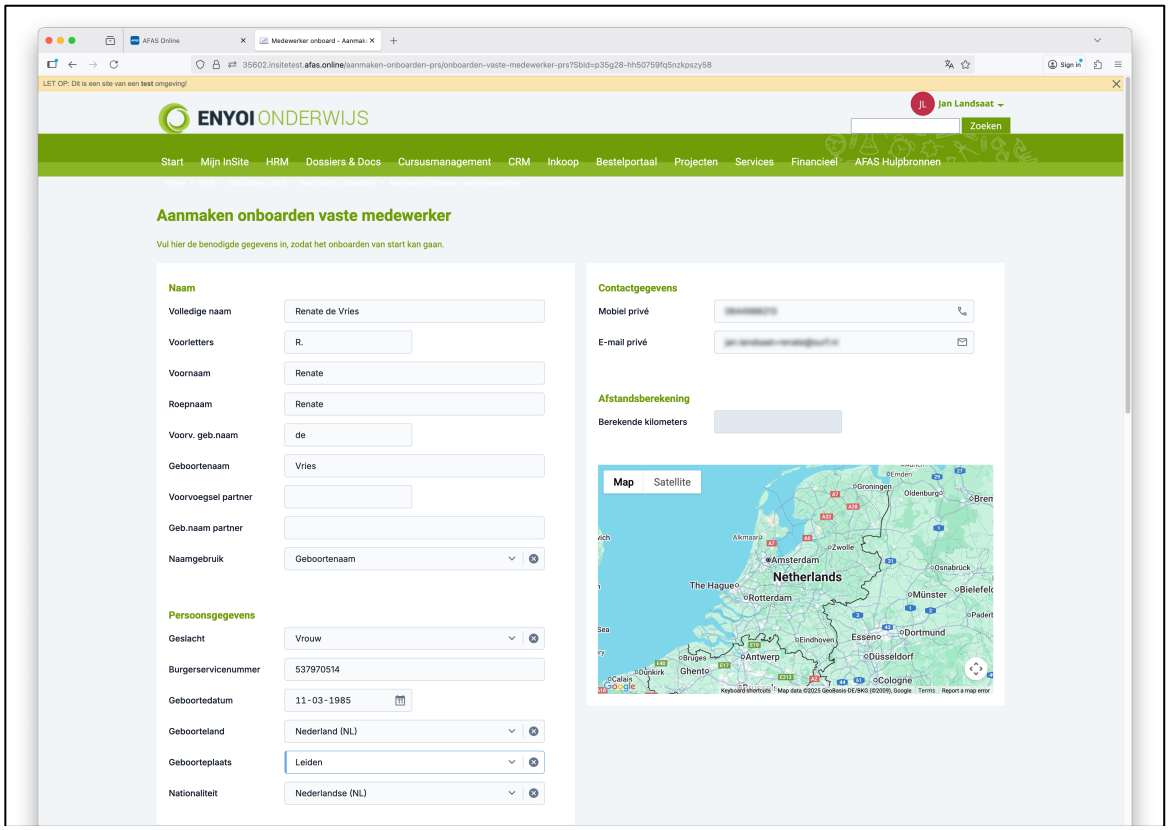
A.5.1.1 Workflow: instroomproces

Doel	Medewerkersadministratie	Salaris-en declaratieverwerking	Dienst beveiligen	
Gegevens	Direct identificeerbare gegevens	Contactgegevens	Organisatiegegevens	Demografische gegevens
	Organisatorische gegevens	Gezondheidgegevens	Financiële gegevens	
	Vakbond gegevens	Politieke gegevens	Overige gegevens	
Gevoeligheid	Normaal	Gevoelig		
Betrokkenen	Medewerkers	Personeel niet in loondienst	Sollicitanten	

Instellingen kunnen in AFAS hun eigen workflows ontwerpen. Deze verwerking kent een hoge mate van inrichtingsflexibiliteit voor instellingen, waardoor de inrichting sterk kan verschillen per instelling.

Het instroomproces (onboarding) vindt plaats op vier verschillende manieren:
- Via een workflow (A.5.3.2 Workflows: algemeen)
- De recruitmentsoftware (Sollicitant Self Service) van AFAS
- Een gekoppelde recruitmentapplicatie (ATS) van een derde partij (A.6.8 Koppelingen)
- Handmatig

In de testomgeving voor deze DPIA is er gebruik gemaakt van een workflow waarbij een gebruiker met de gebruikersrechten van een HR-manager de gegevens van een nieuwe medewerker heeft ingevoerd in AFAS InSite.



Figuur A-3 Start van workflow ‘Aanmaken onboarden vaste medewerker’.

Tijdens of na dit proces maakt de HR-manager (of ander geautoriseerde gebruiker) een gebruikersaccount aan voor de medewerker om Profit te kunnen gebruiken en wijst de HR-manager een profiel aan de gebruiker toeg. Daarna moet de gebruiker dit account activeren en een MFA koppelen. *Let op! Dit is hoe de testomgeving is ingericht, bij instellingen verschilt dit aangezien daar een SSO gekoppeld is en de workflow anders ingericht kan zijn.*

Figuur A-4 Tijdens het instroomproces kiest de HR-manager met welk emailadres de medewerker toegang krijgt tot AFAS.

A.5.2 Vrije velden

Doel	Formatieplanning	Werving en selectie	Medewerkersontwikkeling	
	Medewerkersbeoordeling	Medewerkersadministratie	Tijdregistratie	
	Salaris-en declaratieverwerking		Ziekte- en verlofadministratie	
Gegevens	Direct identificeerbare gegevens	Contactgegevens	Organisatiegegevens	Organisatiegegevens
	Organisatorische gegevens	Financiële gegevens	Gezondheidgegevens	Vakbond gegevens
	Politieke gegevens		Overige gegevens	
Gevoeligheid	Normaal	Gevoelig	Bijzonder	
Betrokkenen	Medewerkers	Personeel niet in loondienst	Beheerder	
	Docenten	Sollicitanten	Oud-werknemers en (oud)personeel niet in loondienst	
	Noodcontactpersoon/partners/kinderen van (oud-)werknemers			

Instellingen kunnen in AFAS hun eigen workflows ontwerpen. Deze verwerking kent een hoge mate van inrichtingsflexibiliteit voor instellingen, waardoor de inrichting sterk kan verschillen per instelling. Zie voor een toelichting A.5.3.

AFAS past op veel open velden datavalidatie toe. Bij de invoer van bijvoorbeeld e-mailadressen, telefoonnummers, kvk-nummers en persoonlijk identificeerbare nummers (bv. BSN) controleert het systeem automatisch of de invoer bestaat uit legitieme waarden die aan de criteria voldoen. Waar validatie mogelijk is wordt dat toegepast. Daarnaast zijn alle vrije velden in de standaard inrichting duidelijk gelabeld.

AFAS biedt instellingen de mogelijkheid vrije velden in te stellen binnen workflows. Dit geeft klanten volledige autonomie over welke gegevens zij verwerken en in welke workflows deze beschikbaar zijn en door wie deze kunnen worden geraadpleegd. Ook de labeling is dan in beheer van de instelling.

Deze velden kunnen in formulieren, rapportages, autorisatieworkflows en data-uitwisseling via koppelingen worden opgenomen.

A.5.3 Gebruik

A.5.3.1 In- en uitloggen

Doel	De dienst beveiligen	De dienst personaliseren		
Gegevens	Direct identificeerbare persoonsgegevens	Contactgegevens		Organisatorische gegevens
Gevoeligheid	Normaal			
Betrokkenen	Medewerkers	Docenten	Personeel niet in loondienst	Oud-medewerkers

Gebruikers kunnen inloggen met hun gebruikersaccount of via SSO. De service implementeert SSO-functionaliteit om het inloggen te vereenvoudigen en te beveiligen.

Gebruikers kunnen toegang krijgen via de eigen AFAS-aanmeldpagina, die Multi-Factor Authenticatie (MFA) bevat, of door gebruik te maken van de SSO-oplossing van hun eigen organisatie. Als gebruikers toegang inregelen via de native AFAS-aanmeldpagina kan hierbij gekozen worden om de AFAS Pocket App te gebruiken of een andere zelfgekozen authenticator-app om de authenticatietoken te verkrijgen.

A.5.3.2 Workflows: algemeen

Doel	Medewerkersadministratie	Salaris-en declaratieverwerking	Medewerkersbeoordeling
	Tijdregistratie	Ziekte- en verlofadministratie	Medewerkersontwikkeling
	Werving en selectie		
Gegevens	Contactgegevens	Demografische gegevens	Organisatiegegevens
	Direct identificeerbare gegevens	Financiële gegevens	Gezondheidsgegevens
	Vakbond gegevens	Politieke gegevens	Overige gegevens
Gevoeligheid	Normaal	Gevoelig	Bijzonder
Betrokkenen	Medewerkers	Personeel niet in loondienst	Docenten	Oud-medewerkers

Instellingen kunnen in AFAS hun eigen workflows ontwerpen. Deze verwerking kent een hoge mate van inrichtingsflexibiliteit voor instellingen, waardoor de inrichting sterk kan verschillen per instelling.

Workflows zijn processen die bestaan uit een reeks stappen die elkaar automatisch opvolgen. Ze dienen om standaardtaken die telkens dezelfde stappen volgen, te vereenvoudigen. Voorbeelden zijn het indienen van verlofaanvragen, het melden van ziekteverzuim, declaraties indienen en wijzigingen aanbrengen in belangrijke (HR-)gegevens, zoals adres, bankrekeningnummer, burgerlijke staat en competenties.

Deze stappen bestaan uit het indienen van wijzigingen door medewerkers/managers en kunnen ook een goedkeuring of afwijzing door een andere persoon omvatten. Elke afwijzing gaat gepaard met een toelichting in een open tekstveld. Het invoeren van informatie in workflows is mogelijk via dropdownmenu's, meerkeuze-vinkjes, vrije tekstvelden (kort of

lang) en het toevoegen van documenten. Verschillende rollen kunnen toegang hebben tot verschillende workflows, of tot verschillende stappen binnen workflows. Medewerkers en managers krijgen toegang tot verschillende workflows. Bijvoorbeeld: medewerkers kunnen verlofaanvragen indienen, zich ziekmelden en wijzigingen in hun contactgegevens aanbrengen, terwijl managers wijzigingen kunnen aanbrengen in contracten en salarissen van hun medewerkers.

Medewerkers krijgen een overzicht van de lopende processen die zij zelf hebben gestart. Daarnaast ontvangen zij notificaties voor acties die zij moeten uitvoeren. Deze signalen kunnen leiden tot het starten van een nieuwe workflow door medewerkers. Medewerkers kunnen een overzicht van alle workflows krijgen die hen betreffen en/of die door hun managers zijn gestart wanneer de instelling dat heeft ingericht.

Instellingen zijn vrij om hun eigen workflows te ontwerpen, maar in de standaardconfiguratie van AFAS zijn al enkele workflows aanwezig. Het is mogelijk om deze standaardworkflows te negeren en/of te verwijderen.

A.5.3.3 Workflow: mobiliteit

Doel	Medewerkersadministratie	Salaris-en declaratieverwerking	
Gegevens	Direct identificeerbare gegevens	Contactgegevens	Demografische gegevens
	Organisatiegegevens	Financiële gegevens	Overige gegevens
Gevoeligheid	Normaal		
Betrokkenen	Medewerkers	Personeel niet in loondienst	Docenten

Instellingen kunnen in AFAS hun eigen workflows ontwerpen. Deze verwerking kent een hoge mate van inrichtingsflexibiliteit voor instellingen, waardoor de inrichting sterk kan verschillen per instelling.

In workflows voor mobiliteitsvergoedingen berekent AFAS automatisch de reisafstand tussen twee locaties. Deze berekening wordt uitgevoerd wanneer een gebruiker adresgegevens registreert in de context van woon-werkverkeer, werklocaties, adreswijzigingen of kilometerdeclaraties. Het systeem stuurt de start- en eindadressen (Van en Naar) naar een externe routeplanningsservice, die de afstand retourneert. AFAS ondersteunt hiervoor zowel Google Maps als TomTom als serviceprovider.

Bij het berekenen van de reisafstand wisselt het systeem de volgende gegevens met de gekozen routeprovider (Google Maps of TomTom) uit: de API-key, de ingevulde vertrek- en bestemmingsadressen (Van en Naar) en technische instellingen die de wijze van routeberekening bepalen, zoals de keuze voor kortste of snelste route. Bij Google Maps specificeert AFAS dat enkel de API-key, adressen en technische instellingen worden uitgewisseld, zonder aanvullende persoonsgegevens. Voor TomTom geldt een vergelijkbare uitwisseling (API-key, adressen, routevoorkeur), maar zonder expliciete bevestiging van AFAS over uitsluiting van aanvullende persoonsgegevens.

De routeberekening verloopt server-side (Profit → Google API), waarbij Google/TomTom het AFAS-server-IP loggen. De optionele routekaart-weergave op InSite gebruikt browser-side

Javascript, waardoor Google/TomTom toegang hebben tot het IP-adres van de eindgebruiker.

A.5.3.4 Toegang tot je eigen data

Doel	Medewerkersadministratie			
Gegevens	Contactgegevens	Demografische gegevens	Organisatiegegevens	
	Direct identificeerbare gegevens	Financiële gegevens	Gezondheidsgegevens	
	Vakbond gegevens	Politieke gegevens	Overige gegevens	
Gevoeligheid	Normaal	Gevoelig	Bijzonder	
Betrokkenen	Medewerkers	Personeel niet in loondienst	Oud-werknemers	Docenten

Instellingen kunnen in AFAS hun eigen workflows ontwerpen. Deze verwerking kent een hoge mate van inrichtingsflexibiliteit voor instellingen, waardoor de inrichting sterk kan verschillen per instelling.

Medewerkers kunnen toegang tot hun gegevens krijgen via Profit, AFAS InSite of de AFAS Pocket App.

Dit bevat:

- Een overzicht van acties die de medewerker kan uitvoeren, waarmee workflows worden gestart.
- De salarisspecificaties.
- Een overzicht van meldingen, die de medewerker kan uitschakelen.
- Een overzicht van het verlof.
- Een overzicht van afwezigheden anders dan verlof.
- Een overzicht van openstaande acties, lopende processen en afgeronde processen.
- Het aantal openstaande en in behandeling zijnde onkostendeclaraties, met de mogelijkheid om de declaraties zelf te bekijken.
- Een overzicht van persoonlijke relaties.
- Toegang tot persoonlijke documenten, die onder meer kunnen bestaan uit:
  - Een kopie van identiteitsbewijzen
  - Salarisspecificaties
  - Curriculum vitae
  - Contracten
  - En andere documenten die in het personeelsdossier zijn opgenomen

Leidinggevenden hebben toegang tot alle bovenstaande informatie van hun medewerkers, met het verschil t.o.v. wat medewerkers zien van zichzelf, dat leidinggevenden toegang hebben tot een overzicht van o.a. verjaardagen, rapportages en (type) afwezigheid van teamleden.

A.5.3.5 Toegang tot en het bewerken van medewerkersdossier

Doel	Medewerkersadministratie			
Gegevens	Contactgegevens	Demografische gegevens	Organisatiegegevens	
	Direct identificeerbare gegevens	Financiële gegevens	Gezondheidsgegevens	
	Vakbond gegevens	Politieke gegevens	Overige gegevens	
Gevoeligheid	Normaal	Gevoelig	Bijzonder	
Betrokkenen	Medewerkers	Personeel niet in loondienst	Oud-werknemers	Docenten

Instellingen kunnen in AFAS hun eigen workflows ontwerpen. Deze verwerking kent een hoge mate van inrichtingsflexibiliteit voor instellingen, waardoor de inrichting sterk kan verschillen per instelling.

De leidinggevendenpagina geeft leidinggevenden/managers toegang tot volledige personeelsdossiers. Naast het gebruik van workflows is het, afhankelijk van de autorisaties van de gebruiker, ook mogelijk om direct wijzigingen in dit dossier aan te brengen. Het dossier bevat:

- basale persoonlijke gegevens van de medewerker;
- documenten;
- afwezigheid;
- verlof;
- (betaalde) salarissen;
- persoonlijke relaties;
- beoordelingen;
- competenties en opleidingen;
- dienstverbanden;
- onkostendeclaraties;
- activiteiten en taken;
- digitale dossier;
- foto's en handtekeningen;
- geregistreerde gesprekken.

A.5.3.6 Supportverzoeken

Supportverzoeken[27] (incidenten) worden door geautoriseerde contactpersonen van de instelling via de AFAS Klantportal[28] ingediend. Daarnaast kunnen ze via het Help Center naar een oplossing zoeken en eventueel een incidentformulier openen bij AFAS Support.

In dit formulier vult de medewerker gestructureerde gegevens in zoals type vraag en product. Daarnaast worden foutmeldingen en relevante informatie in vrije velden beschreven. Daarnaast bestanden worden gekoppeld (bijvoorbeeld screenshots).

[27] AFAS Help Center Nederland, *Incident bij AFAS Support insturen en raadplegen*, geraadpleegd op 18 december 2025 via https://help.afas.nl/help/NL/SE/Str_Portal_Sup.htm.

[28] AFAS Klantportaal via http://klant.afas.nl.

Na verzending wordt het supportverzoek als incident in de AFAS-supportomgeving opgeslagen, is de voortgang door de melder en bevoegde rollen via de Klantportal te volgen en registreert AFAS Support de behandeling en afhandeling totdat het incident wordt gesloten.

De bewaartermijnen van supportmeldingen zijn niet vermeld in de door AFAS aangeleverde documentatie.

A.5.3.7 Relatie Beheer Systeem (AFAS CRM)

Doel	Medewerkersadministratie		
Gegevens	Direct identificeerbare gegevens	Contactgegevens	Demografische gegevens
	Organisatiegegevens	Overige gegevens	
Gevoeligheid	Gevoelig	Normaal	Bijzonder
Betrokkenen	Docenten	Medewerkers	Sollicitanten
	Personeel niet in loondienst	Oud-werknemers	

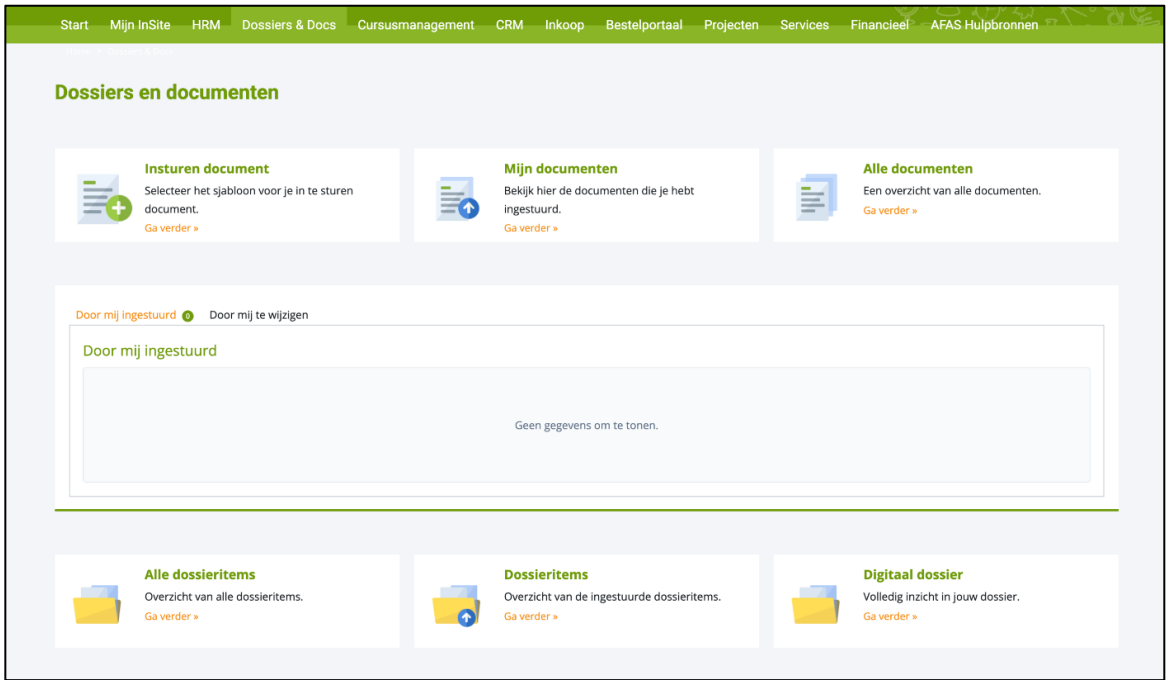
Voor zover CRM-objecten technisch aanwezig zijn (zoals de werkgeversrelatie of systeemmatig aangemaakte relaties), worden deze uitsluitend gebruikt als onderliggende stamgegevens ten behoeve van HRM- en payrollprocessen, en niet als zelfstandig CRM-domein voor klant- of leadopvolging.

A.5.3.8 Documentbeheer

Doel	Medewerkersadministratie		
Gegevens	Direct identificeerbare gegevens	Contactgegevens	Demografische gegevens
	Gezondheidsgegevens	Financiële gegevens	Overige gegevens
Gevoeligheid	Normaal	Gevoelig	Bijzonder
Betrokkenen	Docenten	Medewerkers	Personeel niet in loondienst

Instellingen kunnen in AFAS hun eigen workflows ontwerpen. Deze verwerking kent een hoge mate van inrichtingsflexibiliteit voor instellingen, waardoor de inrichting sterk kan verschillen per instelling.

Alle in Profit aangemaakte en toegevoegde documenten worden toegevoegd aan het digitale dossier. Dit omvat bestanden die tijdens workflows worden opgeslagen, wijzigingen in het personeelsdossier, salarisspecificaties die aan medewerkers worden verzonden en documenten die handmatig aan het dossier zijn toegevoegd.



Figuur A-5 Dossiers & Docs pagina in AFAS InSite.

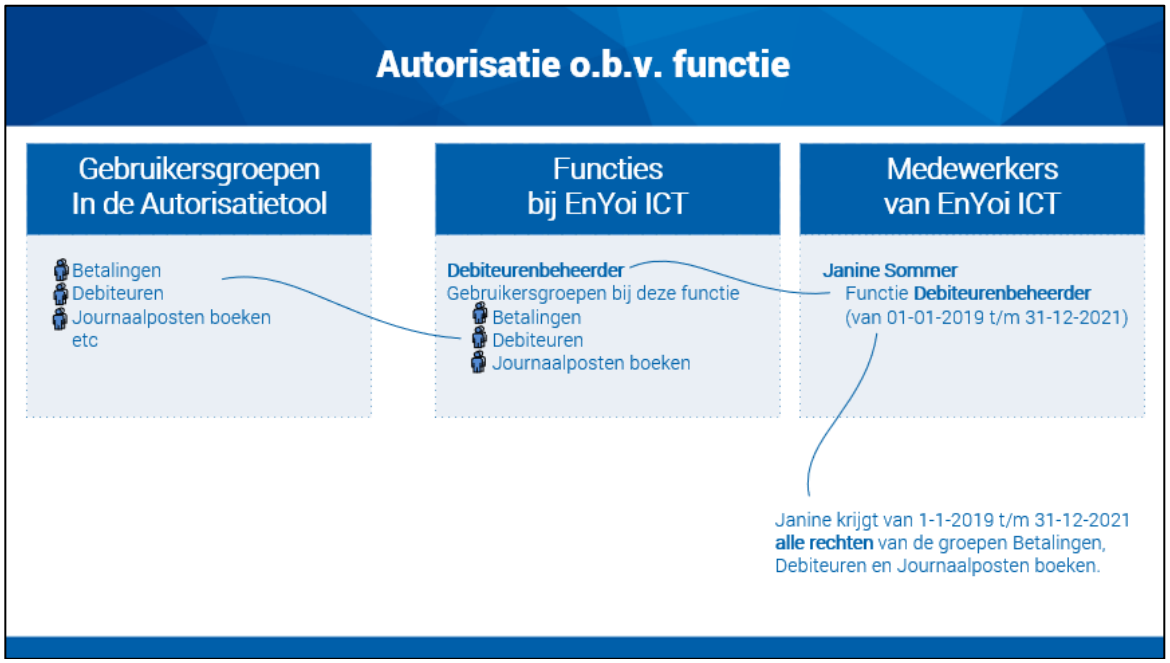
A.5.3.9 Beheer gebruikersrechten

Doel	De dienst personaliseren	De dienst beveiligen	Medewerkersadministratie
Gegevens	Direct identificeerbare persoonsgegevens	Contactgegevens	Organisatorische gegevens
Gevoeligheid	Normaal		
Betrokkenen	Docenten	Medewerkers	Personeel niet in loondienst

Gebruikersrechten in AFAS zijn toegangsregels die bepalen welke functionaliteiten en gegevens een gebruiker kan bekijken, bewerken of beheren binnen het systeem. Deze rechten zorgen ervoor dat bedrijfsgegevens alleen toegankelijk zijn voor geautoriseerd personeel.

Een gebruiker/medewerker kan automatisch worden geautoriseerd op basis van de functie van deze medewerker. Buiten de autorisatie op basis van functie kun je een medewerker ook een tijdelijke of persoonlijke rol geven. Denk hierbij aan vertrouwenspersoon en BHV'ers. Hiervoor worden per doel gebruikersgroepen aangemaakt. Je bepaalt bij persoonlijke rollen per medewerker (dus niet per functie) tot welke persoonlijke gebruikersgroepen deze behoort en kan hierbij een begin- en einddatum opgeven.

Idealiter worden rechten toegekend op basis van functie in combinatie met standaard gebruikersgroepen of je eigen gebruikersgroepen.



Figuur A-6 Stroomschema autorisatie op basis van functie.[29]

Deze inrichting wordt gedaan door een geautoriseerde medewerker via de autorisatietool in Profit (applicatie). Automatische wijzigingen, bijvoorbeeld op basis van functiewijziging worden verwerkt door een ingeplande taak (A.6.5 Inplannen van taken).

A.5.3.9.1 Autorisatie Auditor

AFAS heeft een functionaliteit genaamd 'autorisatie auditor' waarmee extra regels kunnen worden opgesteld om 'te brede' autorisaties te inventariseren. Je kan als instelling het bij een inventarisatie laten of voorkomen dat medewerkers lid zijn van conflicterende gebruikersgroepen. In dit laatste geval kan deze gebruiker geen lid worden van de tweede gebruikersgroepen wat tot dit conflict leidt.

In de AFAS Helpcenter Nederland[30] staat het volgende erover: '*Met de Autorisatie auditor voorkom je dat gebruikers lid zijn van een bepaalde combinatie van gebruikersgroepen. Het gaat telkens om een combinatie van twee gebruikersgroepen, bijvoorbeeld HRM applicatiebeheer en Payroll applicatiebeheer. Door deze combinatie uit te sluiten, voorkom je dat medewerkers lid zijn van beide groepen en te veel 'macht' krijgen in Profit. Door deze oplossing kun je de functiescheiding in de organisatie beter bewaken.*'

[29] AFAS Help Center Nederland, *Gebruikersgroep o.b.v. functie of persoonlijke rol inrichten*, geraadpleegd op 5 december 2025 via https://help.afas.nl/help/nl/se/App_Auth_Group_HRM.htm.

[30] AFAS Help Center Nederland, *Gebruikersgroepen beheren met de Autorisatie Auditor*, geraadpleegd op 5 december 2025 via https://help.afas.nl/help/NL/SE/133133.htm.

A.6 Verwerkingstechnieken en -methoden

A.6.1 Hosting

Leaseweb is de hostingprovider en levert zodoende ook de hostingdiensten. De Leaseweb servers waar AFAS gebruik van maakt voor hosting staan binnen de EER, specifiek in Nederland in Schiphol Rijk en Haarlem.

Deze locaties zijn gekozen op ruime afstand van elkaar om risico's door omgevingsfactoren te beperken en continuïteit te waarborgen, met failover-mogelijkheden tussen deze twee datacenters. AFAS stelt expliciet[31] dat AFAS Online volledig binnen Nederland wordt gehost, bij Leaseweb-datacenters, onder Nederlandse en Europese wetgeving.

A.6.2 Back-up

In de SLA is vastgelegd dat AFAS gebruikmaakt van een datacenter van Leaseweb Deutschland GmbH in Frankfurt voor disaster recovery-doeleinden.[32] In dit Duitse datacenter worden uitsluitend back-ups van data opgeslagen. Dit datacenter is bedoeld als uitwijklocatie om regionale disasters op te kunnen vangen.

De SLA[33] van AFAS beschrijft dat er dagelijks een volledige back-up wordt gemaakt van alle klantdata, die 31 dagen worden bewaard. Daarnaast worden er maandelijkse back-ups bewaard van de eerste dag van de maand gedurende 12 maanden, en jaarlijkse back-ups van de eerste dag van ieder jaar gedurende 7 jaar.

De data wordt opgeslagen op twee speciale locaties binnen Leaseweb met een gescheiden netwerk om het risico op verlies, niet beschikbaar zijn of corruptie van data tot een minimum te beperken. Deze twee servers draaien mirrored aan elkaar, en dienen daarmee als elkaars directe back-up. Naast deze opslag is er nog een derde locatie binnen Leaseweb Haarlem, in een andere fysieke hal waar deze derde back-up wordt opgeslagen.

Het terugzetten van een back-up (restoren) is geautomatiseerd en voor elke klant binnen de Profit-applicatie beschikbaar om zelfstandig uit te voeren op een zelfgekozen moment en van een zelfgekozen back-up.

AFAS hanteert een Recovery Point Objective (RPO) van maximaal 2 uur en een handmatige failover tussen datacenters bij calamiteiten, met een maximaal dataverlies tot 6 uur. Voor kleine omgevingen kan het dataverlies oplopen tot maximaal 24 uur.

A.6.3 Cookies

AFAS InSite zet uitsluitend functionele cookies (zie bijlage) in voor sessiebeheer en inlogverificatie zonder noodzaak voor toestemming. Dit betekent dat voor het overgrote deel van de medewerkers enkel deze niet-invasieve cookies van kracht zijn. Slechts een

[31] AFAS Help Center Nederland, *Data-soevereiniteit met AFAS Online*, geraadpleegd op 4 december 2025 via .

[32] AFAS Service License Agreement april 2026, paragraaf 5.7, geraadpleegd op 8 juni 2026 via https://klant.afas.nl/sla-av.

[33] AFAS Service License Agreement april 2026, geraadpleegd op 8 juni 2026 via https://klant.afas.nl/sla-av.

beperkte groep gebruikers heeft toegang tot specifieke pagina's waar ook niet-functionele cookies worden geplaatst

Klant.AFAS.nl en help.afas.nl laden aanvullende essentiële cookies voor voorkeuren en beperkt analytische doeleinden. Veel van deze cookies worden pas bij specifieke pagina-aanvragen geladen. Voor deze websites is er wel de mogelijkheid om toestemming te geven voor meer cookies via cookie consent.

De privacy statement[34] bevat een uitgebreide cookieverklaring die bijna alle cookies beschrijft. Enkele cookies staan qua omschrijving op 'in afwachting'. Deze cookieverklaring wordt bijgehouden door Cookiebot.

Zie bijlage voor een overzicht van alle cookies.

A.6.4 Encryptie

AFAS gebruikt cryptografische maatregelen (versleuteling) om de vertrouwelijkheid van de informatie te beschermen.

A.6.4.1 Data at rest

AFAS Online beschermt klantgegevens in de database via SQL Server Transparent Data Encryption (TDE). De techniek werkt op databaseniveau. Dat wil zeggen dat alle opgeslagen records in de SQL-database zijn versleuteld met het AES256-algoritme (Advanced Encryption Standard met 256-bits sleutellengte). Het wachtwoord wordt gedeeld tussen alle databaseservers van AFAS Online.

Naast databaserecords versleutelt AFAS ook dossieritem bijlagen (documenten, bijlagen, afbeeldingen). Deze worden periodiek in gecomprimeerde bestanden opgeslagen en versleuteld met wz-aes encryptie met 256-bits sleutellengte.

A.6.4.2 Data in transit

Alle communicatie tussen eindgebruikers, applicaties en de AFAS Online Infrastructuur loopt over versleutelde verbindingen. AFAS specificeert dat alle data die van en naar de klantdata gaat via encryptie wordt beveiligd met TLS 1.2. Zie ook *Figuur A-1 Algemeen stroomschema applicatie landschap AFAS*.

A.6.4.3 Backup

Doordat de productiedata (A.6.4.1) op databaseniveau (TDE AES256) en fileniveau (wz-aes 256-bit) versleuteld is, wordt deze encryptie automatisch meegenomen naar alle back-ups.

A.6.4.4 Sleutelbeheer

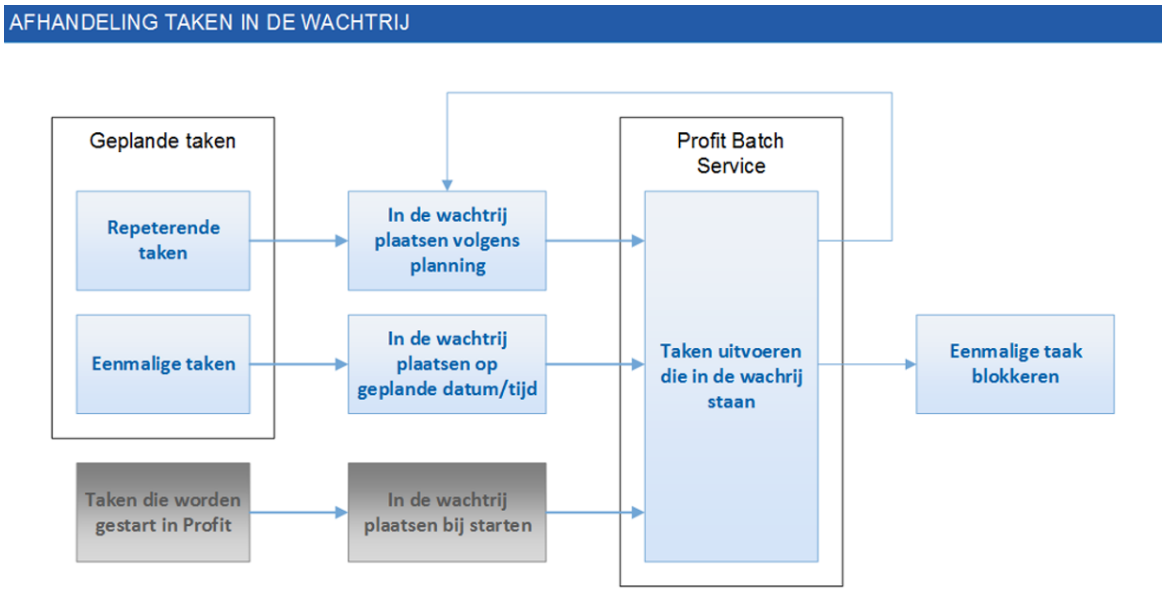
AFAS beheert de versleutelingssleutels via een gecentraliseerd sleutelbeheerproces, waarbij privésleutels automatisch worden gegenereerd, opgeslagen en geroteerd. De SQL-hoofdsleutel valt echter niet onder de standaardrotatiecyclus vanwege de complexiteit van

[34] AFAS Privacy Statement, geraadpleegd op 9 december 2025 via https://www.afas.nl/privacy-statement.

het systeem en de aanzienlijke inspanning die nodig is voor het opnieuw versleutelen, aldus AFAS. In plaats daarvan past AFAS compenserende maatregelen toe rond deze sleutel, waaronder opslag in een wachtwoordkluis, strikte beperkingen op de toegangscontrole en periodieke externe beoordeling van het toegangsbeheer. Bevoegde medewerkers, zoals systeemingenieurs en productbeheerders, hebben toegang tot de versleutelingssleutels, maar deze toegang is beperkt tot geautoriseerd personeel van de leverancier en wordt verleend op basis van just-in-time-toegang met volledige logboekregistratie en monitoring. Eventuele resterende insiderrisico's worden beperkt door strikte toegangscontrolemechanismen, beveiliging van de kluis en continue auditlogboekregistratie, wat resulteert in een laag risicoprofiel.[35]

A.6.5 Inplannen van taken

Binnen AFAS is het mogelijk voor de instelling om bepaalde taken automatisch uit te laten voeren. Deze ingeplande taken hebben onder andere invloed op wijzigingen in autorisaties en verwerken van salaris.



Figuur A-2 Stroomschema van afhandelen van taken.[36]

A.6.6 Monitoren door AFAS[37]

AFAS monitort de performance en beschikbaarheid van AFAS Online en achterliggende onderdelen continu.

A.6.6.1 Storingen

Storingen te voorkomen of in een vroeg stadium op te lossen: monitoring is gericht op het tijdig ontdekken van storingen en ongewenst gedrag.

[35] Zie voor meer toelichting Bijlage 3 Beveiligingsgaranties.

[36] AFAS Help Center Nederland, *Geplande taken*. Geraadpleegd op 4 december 2025 via https://help.afas.nl/help/nl/se/App_Cmd_Tasks.htm.

[37] AFAS Service Licence Agreement oktober 2025, paragraaf 2.3.6, geraadpleegd op 4 december 2025 via https://klant.afas.nl/sla-av.

AFAS gebruikt SPLUNK en PRTG om rate limiting, anomaly detection en logging uit te voeren. AFAS heeft geen datasets aangeleverd om een proportionaliteit analyse uit te kunnen voeren.

A.6.6.2 Misbruik

Serveruitval en inlogpogingen worden continu gemonitord, waarbij gebruik wordt gemaakt van netwerkmonitoring op basis van Managed Detection and Response van Hunt & Hackett, in combinatie met SPLUNK en PRTG voor het verzamelen, monitoren en analyseren van loggegevens.

Naast logging binnen de programmatuur vindt aanvullende logging plaats van bezoeken aan pagina's en onderdelen van de applicatie, waarbij deze logging bij beveiligingsissues kan worden geraadpleegd via de AFAS Online loginportal.

Voor deze beveiligingslogging worden gebruikerscode en het IP-adres van de gebruiker verwerkt. Hierdoor kunnen verdachte activiteiten herleid worden. De toegang tot deze logs en monitoringdata is beperkt tot AFAS Online-beheerders, waarbij deze toegang zelf eveneens gemonitord kan worden om misbruik te voorkomen. Voor security logging geldt een bewaartermijn van minimaal één jaar.

A.6.6.3 Systeemreactietijden

AFAS monitort de performance van haar systemen door het meten en analyseren van systeemreactietijden. De gemeten gegevens worden geaggregeerd op zowel klant- of instellingsniveau als op gebruikersniveau.

Voor de analyse worden gegevens verwerkt zoals de bron (source), het doelpad of de geraadpleegde URL (target path en URL), waarmee AFAS trage of foutgevoelige onderdelen in de systemen kan identificeren. Daarnaast wordt het IP-adres gebruikt om de herkomst op geografisch niveau (bijvoorbeeld land of regio) te kunnen bepalen.

Voor overzicht van deze dataset zie Tabel D-5, overzicht systeemreactietijden logging AFAS InSite.

A.6.6.4 Anonieme statistieken uit klantomgeving

AFAS verzamelt, conform de afspraken in de SLA[38], geanonimiseerde gebruiksstatistieken uit de klantomgeving. Deze statistieken worden gebruikt om de werking van de producten en diensten van AFAS te analyseren en te verbeteren. De verzamelde gegevens hebben betrekking op gebeurtenissen die plaatsvinden binnen de omgeving van de instelling, zoals handelingen die individuele gebruikers uitvoeren.

Iedere gebruiker krijgt een unieke gebruikers-ID en apparaat-ID toegewezen. De enige informatie die herleidbaar blijft, is het member-ID (de identificatie van de instelling). Dit

[38] AFAS Service License Agreement oktober 2025, *paragraaf 2.3.6*, geraadpleegd op 4 december 2025 via https://klant.afas.nl/sla-av.

maakt het voor AFAS mogelijk om contact op te nemen met de betreffende instelling bij technische inrichtingsfouten of andere aandachtspunten die uit de statistieken blijken.

A.6.6.5 Algemene gebruikersstatistieken uit klantomgeving

AFAS gebruikt algemene statistieken uit klantomgevingen ter verbetering van haar producten en diensten. De SLA beschrijft dat het om algemene gebruikersstatistieken gaat (zoals systeemreactietijden). Uit het onderzoek blijkt echter dat niet volledig kan worden uitgesloten dat in sommige gevallen persoonsgegevens worden verwerkt.

Medewerkers van AFAS kunnen een verzoek indienen om specifieke statistieken te verkrijgen voor een bepaald doel. Deze verzoeken volgen geen standaardformat, waardoor het kan voorkomen dat in afzonderlijke aanvragen persoonsgegevens voorkomen.

Elk verzoek wordt beoordeeld door een Software Engineer en is toegankelijk voor zowel de Privacy Officer als de Functionaris Gegevensbescherming. Wanneer een verzoek wordt goedgekeurd, worden de betreffende statistieken gedeeld met de aanvragende medewerker.

Op de gegenereerde rapportages zijn geen automatische bewaartermijnen van toepassing. De verantwoordelijkheid voor verwijdering of archivering ligt bij de medewerker of het team dat de gegevens heeft opgevraagd.

A.6.7 Applicatielogging

Binnen de applicatie zijn er verschillende typen logging van toepassing, deze worden beheerd door de instelling zelf.

A.6.7.1 Mutatielogboek[39]

Het mutatielogboek in Profit registreert op veldniveau welke gebruiker gegevens heeft toegevoegd, gewijzigd of verwijderd in geselecteerde tabellen, inclusief oude en nieuwe waarde, datum/tijd, type mutatie (insert, update, delete) en de betrokken gebruiker. De instelling bepaalt zelf per veld welke mutaties worden gelogd.

Mutatielogboeken kunnen worden opgeschoond op basis van een “ouder dan”-datum, waarbij alle logregels vóór die datum uit de algemene logtabellen worden verwijderd.

Voor meer zie A.10 Bewaartermijnen.

Mutaties in de logginginrichting zelf (bijvoorbeeld het aan- of uitzetten van logging) worden altijd gelogd en deze logregels kunnen niet worden verwijderd, zodat wijzigingen in de loggingconfiguratie achteraf controleerbaar zijn.

[39] AFAS Help Center Nederland, *Logboek (logging van gewijzigde gegevens)*, geraadpleegd op 5 december 2025 via https://help.afas.nl/help/NL/SE/App_Log_Book.htm.

A.6.7.2 Loginanalyse[40]

Loginanalyse van alle gebruikers levert een overzicht van gebruikers en hun inloginformatie over alle omgevingen (productie, test en acceptatie) heen. In dit overzicht worden per gebruiker en per omgeving vastgelegd: of de gebruiker kan inloggen in Profit, AFAS InSite en AFAS OutSite, en het tijdstip van de laatste login.

De loginanalyse wordt niet continu als automatisch logbestand aangeboden, maar op aanvraag gegenereerd via de AFAS Online- portal; die aanvragen zelf worden ook gelogd.

Alle aanvragen van alle beheerders in het toegangslogboek blijven op de portal staan, kunnen niet worden verwijderd en zijn voor alle beheerders zichtbaar.

A.6.7.3 Logging op dossier en reacties[41]

Met logging op dossieritems en reacties op dossieritems wordt vastgelegd welke gebruiker welke actie heeft uitgevoerd op deze gegevens. Nadat deze logging is ingeschakeld voor de tabellen Dossieritem en Reactie, registreert het systeem per gebruiker het aanmaken, wijzigen en verwijderen van dossieritems en reacties. Per veld wordt het oude en nieuwe gegeven gelogd, met uitzondering van memo-velden waarbij alleen de eerste 255 tekens worden opgeslagen.

Alleen daartoe bevoegde medewerkers kunnen de dossierlogging bekijken.

Om bewaartermijnen na te kunnen leven moeten deze logs handmatig door instelling worden opgeschoond.

A.6.7.4 Logging op autorisatiemutaties[42]

Wijzigingen in gebruikersautorisaties en machtigingen kunnen worden gelogd. Daarmee wordt vastgelegd welke beheerder welke wijzigingen in gebruikers- en groepsmachtigingen heeft aangebracht. Nadat logging is ingeschakeld registreert het systeem per wijziging de betrokken gebruiker, de gebruiker die de wijziging heeft uitgevoerd (Log gebruiker), en de specifieke wijzigingen zelf (bijvoorbeeld wijzigingen op het tabblad Autorisatie per gebruiker of Menu per gebruiker).

De organisatie bepaalt zelf welke autorisatie-rubriek en welke velden daarvan gelogd moeten worden, en kan ook instellen of alleen toevoegingen, wijzigingen, verwijderingen of een combinatie daarvan worden geregistreerd.

Alleen daartoe bevoegde medewerkers kunnen de deze logs inzien.

---

[40] AFAS Help Center Nederland, *Loginanalyse van alle gebruikers*, geraadpleegd op 5 december 2025 via https://help.afas.nl/help/NL/SE/123780.htm.

[41] AFAS Help Center Nederland, *Logging op dossier en reacties*, geraadpleegd op 5 december 2025 via https://help.afas.nl/help/NL/SE/Crm_Config_Doss_Log.htm.

[42] AFAS Help Center Nederland, *Logging op mutaties autorisatie*, geraadpleegd op 5 december 2025 via https://help.afas.nl/help/NL/SE/App_Auth_Manage_Log.htm.

Er is geen standaard bewaartermijn; organisaties kunnen oude logregels handmatig exporteren en verwijderen als deze niet meer nodig zijn.

A.6.7.5 Logging op wijzigingen workflow[43]

De logging bij het wijzigen van een workflow registreert configuratiewijzigingen die in de workflow-editor zijn doorgevoerd, waaronder het aanmaken, aanpassen en verwijderen van complete workflows. De logregistratie vindt plaats op het moment dat een workflow wordt gepubliceerd; per publicatie wordt vastgelegd welke taken en acties in de workflow zijn toegevoegd, gewijzigd of verwijderd, maar de inhoud van de mutatie (zoals de oude en nieuwe bestemming van een taak) wordt niet getoond.

Om bewaartermijnen na te kunnen leven moeten deze logs handmatig door instelling worden opgeschoond.

A.6.7.6 E-mail logboek[44]

Met 'Verzonden e-mail' worden alle e-mailberichten geregistreerd die via de ingebouwde mailserver zijn verzonden, inclusief de verzendstatus. Deze logging is bedoeld voor beheer en ondersteuning, bijvoorbeeld wanneer een relatie meldt dat een bericht niet is aangekomen. Een beheerder kan dan een overzicht raadplegen van alle verzonden e-mail. Vanuit deze weergave kan worden doorgeklikt naar de betreffende organisatie of persoon om bijvoorbeeld het e-mailadres te controleren of aan te passen. De weergegeven informatie omvat welke berichten zijn verzonden, de bijbehorende status (geslaagd/fout), en de koppeling met de relatie (organisatie/persoon). De inhoud van de e-mail kan niet worden ingezien[45].

Beheerders kunnen gelogde verzonden e-mail opschonen via de actie 'collectief verwijderen'. Om bewaartermijnen na te kunnen leven moeten deze logs handmatig door instelling worden opgeschoond.

A.6.7.7 Mutatielogging InSite[46]

Mutatielogging voor AFAS InSite registreert wijzigingen die via de AFAS InSite- en OutSite-portalen in Profit worden doorgevoerd, bijvoorbeeld het indienen of wijzigen van declaraties. Hierin kunnen meerdere velden worden opgenomen zoals het betrokken object (bijvoorbeeld declaratie), type mutatie, datum/tijd en de gebruiker via wiens AFAS InSite-sessie de mutatie is gedaan.

---

[43] AFAS Help Center Nederland, *Logging bij het wijzigen van een workflow*, geraadpleegd op 5 december 2025 via https://help.afas.nl/help/NL/SE/119575.htm.

[44] AFAS Help Center Nederland, *Status van verzonden e-mail raadplegen*, geraadpleegd op 5 december 2025 via https://help.afas.nl/help/NL/SE/App_Output_Sent_Mail_View.htm.

[45] AFAS Help Center Nederland, *Verzonden e-mailberichten raadplegen*, geraadpleegd op 11 december via https://help.afas.nl/help/NL/SE/135654.htm.

[46] AFAS Help Center Nederland, *Mutatielogging InSite*, geraadppleegd op 5 december via https://help.afas.nl/help/NL/SE/Ins_Config_Profil_Log.htm.

Om bewaartermijnen na te kunnen leven moeten deze logs handmatig door instelling worden opgeschoond.

A.6.7.8 Logging / historie voorcalculatie[47]

Mutatielogging Payroll registreert wijzigingen in de salarisverwerking, zoals wijzigingen in looncomponentparameters, cao instellingen, werkgeversinstellingen en medewerker parameters.

Deze logging bestaat uit drie delen:

- Het algemene logboek waarbij de instelling zelf per veld bepaald of mutaties worden gelogd.
- Het parameterlogboek waarin wijzigingen in parameterwaarden van looncomponenten worden bijgehouden.
- Logging binnen weergaven waar per record zichtbaar is wie gegevens heeft toegevoegd of als laatste gewijzigd.

In het parameterlogboek worden per wijziging onder meer vastgelegd: de betrokken parameter (nummer), het niveau (cao, werkgever, medewerker), datum van de mutatie, de gebruiker die de wijziging heeft doorgevoerd, oude en nieuwe begin- en einddatum, omschrijvingen, en eventueel de opgegeven reden voor de wijziging.

Om bewaartermijnen na te kunnen leven moeten deze logs handmatig door instelling worden opgeschoond.

A.6.7.9 Read Access logging

Read access logging is een mechanisme dat het lezen (consultatie) van persoonsgegevens registreert, inclusief wie, wanneer en welke data is opgevraagd dit om toegang tot gegevens te registreren. AFAS ondersteunt read access logging. De instelling kan deze logs via het Login Portal bij AFAS opvragen. AFAS levert de opgevraagde gegevens automatisch aan binnen een niet gespecificeerde termijn. Deze termijn is niet vooraf vastgelegd, omdat de tijd voor het genereren van het rapport afhankelijk is van de omvang van de aanvraag. AFAS heeft aangegeven dat de levering doorgaans binnen korte tijd plaatsvindt, ruim binnen een mogelijke meldplichttermijn van 72 uur bij een potentieel datalek (Autoriteit Persoonsgegevens).

Deze logging is er voor zowel Profit, InSite als de PocketApp. Zie Bijlage 0 Logging & Monitoring voor een overzicht van deze logs. Deze logs worden opgevraagd voor een gebruiker binnen een bepaalde periode.

Dit logboek gaat terug tot circa november 2024, dit type logging is in november 2024 gefaseerd geactiveerd.

[47] AFAS Help Center Nederland, *Logging / historie van voorcalculatie raadplegen*, geraadppleegd op 5 december via https://help.afas.nl/help/NL/SE/Pro_PrEst_Log_View.htm.

A.6.8 Koppelingen

AFAS biedt drie gestandaardiseerde koppelingen voor data-uitwisseling met externe systemen.

A.6.8.1 AFAS Connect[48]

AFAS Connect is het online platform voor het testen van connectoren. Het ondersteunt REST/JSON en SOAP/XML-standaarden, met vaste IP-adressen voor firewallconfiguratie en IP-restricties. Dit platform is beschikbaar voor klanten (instellingen), partners en AFAS-consultants.

A.6.8.2 Directe API-integraties[49]

Wanneer een instelling zelf een koppeling met een derde systeem wil maken kan het gebruik maken van Directe API-integraties. API-integraties gebruiken REST/JSON of SOAP/XML voor aangepaste koppelingen buiten gestandaardiseerde connectors (AFAS Connect of standaard gecertificeerde koppelingen) om. Dit gaat om dezelfde technieken die gebruikt worden als bij AFAS connect, maar dan zonder tussenkomst van het online platform. Beschikbaar voor klanten met behoefte aan een hogere controlegraad of met specifieke integratiebehoeften.

A.6.8.3 Standaard gecertificeerde koppelingen[50]

Standaard gecertificeerde koppelingen zijn door partners van AFAS ontwikkeld en gecertificeerd op werking, veiligheid. Het onderhoud van de code die gebruikt wordt bij deze standaard koppeling is ook in beheer bij de respectievelijke partner. Deze koppelingen maken gebruik van dezelfde directe API-integraties de koppelingen zijn altijd in beheer van de instelling, de partner heeft alleen invloed op de code niet op de koppeling zelf of de data die daar verwerkt wordt.

A.6.8.4 Authenticatie[51]

Authenticatie bij AFAS Connect en directe API-integraties verloopt via classic token of OAuth. Dit model zorgt voor (gebruikers)gespecificeerde toegang, maar geeft aan dat geauthentiseerde connectoren vervolgens toegang tot hun geregistreerde omgeving met dezelfde rechten die horen bij de gebruiker/gebruikersgroep.

---

[48] AFAS Help Center Nederland, *AFAS Connect*, geraadpleegd op 5 december via https://help.afas.nl/help/NL/SE/cnr_cnct.htm.

[49] AFAS Help Center Nederland, *Rest API voor ontwikkelaars,* geraadpleegd op 5 december via https://help.afas.nl/help/NL/SE/App_Cnr_Rest_Api.htm.

[50] AFAS Partnerportal, *Koppel je favoriete software aan AFAS*, geraadpleegd op 5 december via https://partner.afas.nl/koppelingen.

[51] AFAS Help Center Nederland, *Authenticatie*, geraadpleegd op 5 december via https://docs.afas.help/profit/nl/authentication.

A.7 Betrokken partijen

In dit hoofdstuk worden de partijen beschreven die betrokken zijn bij de verwerking van persoonsgegevens binnen het AFAS-software en de wijze waarop hun rollen zijn vormgegeven op basis van de bepalingen uit de AVG.

A.7.1 Juridisch kader voor rolverdeling

De AVG onderscheidt verschillende rollen voor partijen die betrokken zijn bij de verwerking van persoonsgegevens, waaronder de verwerkingsverantwoordelijke, de gezamenlijke verwerkingsverantwoordelijke, de verwerker en de subverwerker. Bij de beoordeling van de rol van partijen onder de AVG is de feitelijke situatie doorslaggevend.

Artikel 4, lid 7, AVG definieert de (gezamenlijke) verwerkingsverantwoordelijke als: "*een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lid statelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.''*

Artikel 26 AVG bepaalt dat wanneer twee of meer partijen gezamenlijk de doeleinden en middelen van de verwerking vaststellen, zij worden aangemerkt als gezamenlijke verwerkingsverantwoordelijken. Deze partijen dienen in een onderlinge regeling vast te leggen hoe zij de verplichtingen uit hoofde van de AVG verdelen, met name voor de uitoefening van rechten van betrokkenen en informatieverplichtingen.

Artikel 4, lid 8, AVG definieert de verwerker als: "*en natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.*"

Een subverwerker is een derde partij die door de verwerker wordt ingeschakeld om specifieke verwerkingsactiviteiten uit te voeren namens de verwerkingsverantwoordelijke.

Artikel 28 AVG bevat verschillende verplichtingen van verwerkers ten opzichte van de verwerkingsverantwoordelijken voor wie zij gegevens verwerken. Artikel 28, lid 3, AVG bevat specifieke verplichtingen voor de verwerker. Deze verplichtingen omvatten onder meer het uitsluitend verwerken van persoonsgegevens in overeenstemming met de gedocumenteerde instructies van de verwerkingsverantwoordelijke en het meewerken aan audits door een verwerkingsverantwoordelijke. Artikel 28, lid 4, AVG bepaalt dat de verwerker subverwerkers mag inschakelen voor specifieke taken, mits de verwerkingsverantwoordelijke daarvoor vooraf toestemming heeft gegeven.

A.7.2 Feitelijke situatie

AFAS sluit met haar klanten instellingen een Service Level Agreement (SLA), waarin tevens een geïntegreerde verwerkersovereenkomst is opgenomen. In deze SLA is expliciet vastgelegd dat de klant kwalificeert als verwerkingsverantwoordelijke en AFAS als verwerker in de zin van artikel 4, onder 7 en 8, AVG. AFAS stelt zich contractueel in geen enkele situatie

op als verwerkingsverantwoordelijke voor de persoonsgegevens die binnen de AFAS-software worden verwerkt (zie A.4

Verwerkte persoonsgegevens). De contractuele rolverdeling sluit niet aan bij de feitelijke situatie.

AFAS als verwerkingsverantwoordelijke
Tijdens het technisch onderzoek is gebleken dat AFAS feitelijk (verdere) verwerkingen uitvoert die niet expliciet zijn omschreven of begrensd in de SLA, namelijk:

- Monitoring om storingen voorkomen of in een vroeg stadium op lossen
- Algemene gebruikersstatistieken verzamelen
- Anonieme statistieken uit de klantomgeving te verzamelen
- Het meten en analyseren van systeemreactietijden
- Het verzamelen, monitoren en analyseren van loggegevens om misbruik te voorkomen

SURF stelt zich op het standpunt dat AFAS, althans voor deze specifieke verwerkingsactiviteiten, kwalificeert als zelfstandig verwerkingsverantwoordelijke, nu zij feitelijk invloed uitoefent op het doel en de middelen van deze (verdere) verwerkingen. Instellingen kunnen immers geen invloed uitoefenen op het doel en de middelen van deze verwerkingen, omdat deze verwerkingen niet (voldoende) transparant zijn voor instellingen. Daardoor ontbreekt voor instellingen de feitelijke en contractuele mogelijkheid om deze verwerkingen aan te sturen, te beperken of uit te schakelen.

AFAS als verwerker
Voor zover het de in A.3.1 en A.3.2 beschreven verwerkingsdoelen betreft, kwalificeert AFAS als verwerker. AFAS verwerkt persoonsgegevens uitsluitend voor en in opdracht van de instelling en uitsluitend ter uitvoering van de tussen partijen gesloten overeenkomst. AFAS heeft geen zeggenschap over de doeleinden van de verwerking, de grondslag of de inhoudelijke keuzes met betrekking tot persoonsgegevens. AFAS handelt uitsluitend op basis van instructies van de instelling, welke instructies door de instelling worden gegeven via de software zelf of via de klantportal.

De instellingen bepalen zelfstandig het doel en de middelen van de verwerking van persoonsgegevens die zij binnen Profit invoeren, vastleggen en beheren. Dit betreft onder meer:

- welke (categorieën) persoonsgegevens worden vastgelegd;
- welke categorieën betrokkenen worden verwerkt;
- voor welke doeleinden de software wordt ingezet;
- welke functionaliteiten (waaronder eventuele aanvullende of optionele functionaliteiten) worden geactiveerd.

Dit betekent dat de inhoudelijke verwerkingen van persoonsgegevens volledig afhankelijk zijn van de wijze waarop de instelling Profit inricht en gebruikt.

Vanwege deze rolverdeling en het karakter van Profit als generieke standaardsoftware, kiest AFAS er bewust voor om in de SLA geen omschrijving op te nemen van:

- categorieën betrokkenen
- categorieën persoonsgegevens
- verwerkingsdoeleinden
- bewaartermijnen

In plaats daarvan verwijst AFAS naar een dynamisch overzicht binnen de software zelf, waarin inzichtelijk is welke persoonsgegevens worden verwerkt in datavelden, inclusief door instellingen zelf aangemaakte datavelden.[52] Andere persoonsgegevens die worden verwerkt, maar niet aan een specifiek dataveld zijn gekoppeld, worden niet getoond.

Indien een instelling dat wenst, kunnen de categorieën persoonsgegevens op verzoek worden opgeslagen bij de overeenkomst. Dit geldt echter niet voor de verwerkingsdoeleinden, betrokkenen en bewaartermijnen; deze kunnen niet opgeslagen worden bij de overeenkomst.[53] (zie hoofdstuk A.2

[52] AFAS Service Licence Agreement oktober 2025, paragraaf 5.1, geraadpleegd op 18 december 2025 via https://klant.afas.nl/sla-av.

[53] AFAS Klantportaal, *Service Level Agreement en Algemene Voorwaarden*, geraadpleegd op 16 april 2026 via https://klant.afas.nl/sla-av#sla

Wettelijk kader en beleidskader).

Naast de verwerking van persoonsgegevens in opdracht van de instelling verricht AFAS verwerkingen die ondersteunend en technisch van aard zijn. Deze verwerkingen zijn noodzakelijk voor de uitvoering van de overeenkomst en omvatten:

- hosting van de SaaS-omgeving (A.6.1);
- technisch beheer, onderhoud, patches en upgrades (0);
- het maken en beheren van back-ups en herstelprocedures (A.6.2);
- het treffen en handhaven van passende technische en organisatorische beveiligingsmaatregelen (waaronder ISO 27001 en NEN 7510) (0);
- het detecteren, afhandelen en rapporteren van beveiligingsincidenten en (mogelijke) datalekken (0).

Deze ondersteunende verwerkingen worden uitgevoerd binnen het kader van artikel 28, lid 3, AVG en vinden uitsluitend plaats ten behoeve van de dienstverlening aan de instelling. Deze verwerkingen zijn expliciet vastgelegd in de SLA. Zie hoofdstuk A.3.2 Door de instellingen vastgestelde ondersteunende doeleinden.

A.7.3 Door AFAS genoemde subverwerkers in de SLA

De subverwerkers die in hoofdstuk 5 ‘Verwerkersovereenkomst’ van de SLA van AFAS worden genoemd, zijn:

Naam	Verwerkingsactiviteiten	Categorieën persoonsgegevens	OVK
Leaseweb Netherlands B.V.	AFAS host de SaaS-dienst AFAS Online op de datacenters van Leaseweb.	Alle persoonsgegevens die een instelling invoert in de software van AFAS.	Het huidige contract is verlopen. Momenteel is AFAS in onderhandeling over nieuwe contractuele voorwaarden.
Leaseweb Deutschland GmbH	AFAS slaat back-ups van data uitsluitende op voor disaster recovery-doeleinden.	Alle persoonsgegevens die een instelling invoert in de software van AFAS.	Momenteel is AFAS in onderhandeling over contractuele voorwaarden.
Microsoft B.V.	Niet van toepassing	Niet van toepassing.	Niet van toepassing

A.7.3.1 Leaseweb Netherlands B.V.

Het huidige contract met Leaseweb Netherlands B.V. is verlopen. Momenteel is AFAS in onderhandeling over nieuwe contractuele voorwaarden. AFAS heeft echter geen indicatie

gegeven van het moment waarop deze nieuwe overeenkomsten naar verwachting zullen worden gesloten. SURF heeft van AFAS het voorgaande contract met Leaseweb Netherlands B.V. ontvangen en dit als uitgangspunt genomen voor de onderhavige DPIA.

A.7.3.2 Microsoft B.V.

Ten aanzien van de subverwerker Microsoft stelt AFAS dat Microsoft voor de verwerkingen die in deze DPIA worden beschreven, niet als subverwerker kwalificeert. Alleen bij specifieke inzet van AI-Assistent 'Jonas' (die buiten de scope van deze DPIA valt) wordt Microsoft als subverwerker ingezet. Uit de SLA blijkt deze informatie echter niet.

A.7.4 Door SURF geïdentificeerde subverwerkers

Tijdens het technisch onderzoek zijn in de onderschepte data en de geraadpleegde documentatie meerdere subverwerkers geïdentificeerd die niet in de SLA zijn opgenomen. Cookiebot en Google zijn naar voren gekomen uit het cookieonderzoek en de controle van het privacystatement van klant.afas.nl. Cloudflare is zichtbaar geworden als end-point in de onderschepte netwerkverkeerdata. Hunt&Hackett is tenslotte naar voren gekomen uit de documentatie en gesprekken met AFAS.

Naam	Verwerkingsactiviteiten	Categorieën persoonsgegevens
Cookiebot	Onbekend	IP-adres, verder onbekend
Cloudflare	Onbekend	IP-adres, verder onbekend
Hunt & Hackett	Monitoren van de omgeving	Useragents, IP-adressen, verder onbekend
Google	Onbekend	Onbekend

Cookiebot, Cloudflare en Hunt & Hackett

SURF heeft van AFAS de verwerkersovereenkomsten ontvangen met betrekking tot Cookiebot en Cloudflare. De verwerkersovereenkomsten voor Cookiebot en Cloudflare zijn gesloten via Gladior (als een tussenpartij). De betreffende verwerkersovereenkomst is publiek beschikbaar[54], maar bevat geen specificatie van de verwerkingen.

Daarnaast heeft SURF van AFAS de verwerkersovereenkomst ontvangen die is gesloten met Hunt & Hackett. In deze verwerkersovereenkomst is ook geen specificatie van de verwerking(en) opgenomen. In plaats daarvan wordt in de bijlage verwezen naar andere documentatie, zoals opgenomen in de volgende bepaling:

[54] Gladior Verwerkersovereenkomst, geraadpleegd op 16maart 2026 via https://www.gladior.com/resources/2024/09/Verwerkersovereenkomst-Gladior-1.pdf.

> "*This Appendix is intentionally left blank and refers to the technical (implementation) documentation that details the (personal) data (sources) that will be processed as part of the services. Parties may update this Appendix or the documentation it refers to during the term of the agreement.*"

De technische documentatie waarnaar in de appendix wordt verwezen, is niet door AFAS met SURF gedeeld.

SURF heeft AFAS verzocht om nadere informatie te delen over Cookiebot, Cloudflare en Hunt & Hackett in het bijzonder om te specificeren welke verwerkingsactiviteiten, categorieën persoonsgegevens en bewaartermijnen van toepassing zijn voor Cookiebot, Cloudflare en Hunt & Hackett. Deze informatie is niet gedeeld.

Google
AFAS heeft geen subverwerkersovereenkomst met Google verstrekt.

A.7.5 Ontvangers

Het begrip ontvanger is zeer ruim gedefinieerd als "*een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt*". Naar de letter van de definitie zijn daar zelfs alle in paragraaf 7.3. beschreven verwerkers onder te verstaan. [55]

In het kader van deze DPIA worden de volgende andere ontvangers onderscheiden:

A.7.5.1 Overheidsinstanties

Onder ontvangers zijn geen overheidsinstanties te verstaan die gegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het nationale of Europese recht.[56] Andere overheidsinstanties vallen hier echter wel onder. Zodra instellingen of AFAS wettelijk verplicht zijn om persoonsgegevens te delen met de overheid, gelden deze instanties dus wel als ontvangers.

A.7.5.2 Mapsintegratie

Andere te verwachten ontvangers van persoonsgegevens zijn kaartdiensten van Google Maps of TomTom.

Wanneer binnen een mobiliteitsworkflow een integratie met een kaartenprovider gewenst is dan ligt verantwoordelijkheid hiervoor bij de instelling. De instelling kiest en implementeert zelf een kaartenservice (Google Maps of TomTom), beschikt over een eigen account bij dienst, beheert de API-sleutel en is verantwoordelijk voor de contractuele afspraken.

[55] Art. 4, onder 9, AVG.

[56] Art. 4, onder 9, AVG.

AFAS fungeert in dit proces als technisch integrator en biedt de routeberekeningsfunctionaliteit, op basis van deze derde partij, binnen haar eigen applicatie aan. De verwerking van persoonsgegevens inclusief (adres)gegevens door de gekozen kaartenprovider valt daarmee buiten de verwerkingsovereenkomst met AFAS.

A.7.5.3 Appstores

De AFAS Pocket app kan worden geïnstalleerd via de Apple App Store en de Google Play Store. Daardoor hebben Apple en Google een koppeling tussen het gebruik van de AFAS Pocket app en het Apple- en Google-account van de gebruiker. Dit is niet specifiek voor de AFAS Pocket app, maar geldt voor alle apps die via de Apple App Store worden aangeboden. AFAS heeft geen verwerkersovereenkomsten met Apple en Google getoond.

A.8 Belangen bij gegevensverwerking

A.8.1.1 Instelling (verwerkingsverantwoordelijke)

Als instelling, en daarmee verwerkingsverantwoordelijke, heeft de instelling diverse belangen die samenhangen met een zorgvuldige en rechtmatige verwerking van persoonsgegevens binnen Profit.

- Zorgvuldige omgang met persoonsgegevens: De instelling verwerkt via Profit omvangrijke en deels gevoelige gegevens van haar medewerkers. Instellingen hebben daarom een groot belang bij een goed verloop van dit proces. Dit belang vloeit mede voort uit de wettelijke plicht om te voldoen aan de AVG, waarbij de focus ligt op het bieden en onderhouden van een veilige werkomgeving waarin de zorgvuldige omgang van medewerkersgegevens geborgd blijft.
- Efficiënte en betrouwbare HRM- en payrollprocessen: Het gebruik van Profit stelt de instelling in staat haar wettelijke taken als werkgever efficiënt uit te voeren. Dit omvat onder meer het zorgen voor correcte salarisbetalingen en loonheffingen, de uitvoering van arbeidsovereenkomsten en de gehele personeelsadministratie, evenals het naleven van arbeidsrechtelijke en fiscale verplichtingen. Een efficiënt werkend HRM- en payrollsysteem vermindert administratieve lasten, voorkomt fouten en draagt bij aan een betrouwbare bedrijfsvoering.
- Kwaliteit van bedrijfsvoering en organisatie: AFAS biedt mogelijkheden voor workflow-management, dossiervorming, verlofbeheer, ziekteverzuimregistratie en contractbeheer. Deze functionaliteiten helpen de instelling bij tijdige en correcte administratieve afhandeling, planning van inzet van medewerkers en het vergroten van wendbaarheid bij veranderingen in personeelsbehoefte. Dit bevordert een goed functionerende onderwijsorganisatie en draagt indirect bij aan de kwaliteit van het onderwijs.

A.8.1.2 AFAS (als verwerker en verwerkingsverantwoordelijke)

AFAS heeft in haar hoedanigheid als verwerker en verwerkingsverantwoordelijke diverse belangen die samenhangen met een zorgvuldige en rechtmatige verwerking van persoonsgegevens binnen Profit.

- Leveren en onderhouden van betrouwbare, veilige en compliant software: AFAS heeft een belang bij het goed laten functioneren van haar software, inclusief beveiligingsmonitoring, onderhoud en technische ondersteuning. Dit belang moet altijd verenigbaar zijn met de instructies van de verwerkingsverantwoordelijke en ook voldoen aan regelgeving.
- Behoud en versterking van de marktpositie: AFAS heeft een commercieel belang bij het leveren van kwalitatieve software die voldoet aan de AVG en sectorverwachtingen, waardoor klanten worden behouden en nieuwe instellingen worden aangetrokken.

A.8.1.3 Subverwerkers

Subverwerkers hebben een commercieel belang bij het behoud van AFAS, door kwalitatief hoogwaardige diensten te leveren en het bedrijf in staat te stellen te voldoen aan wet- en regelgeving. Daarnaast hebben zij er belang bij om te voldoen aan wet- en regelgeving en hun reputatie te beschermen, zeker gezien de toenemende publieke en toezichthoudende aandacht voor gegevensverwerkingen door grote technologiebedrijven en doorgiften naar derden landen. Hoewel de subverwerkers weliswaar een commercieel belang hebben bij

het behouden van AFAS als klant, zijn deze subverwerkers minder afhankelijk van AFAS als klant dan andersom door hun enorme omvang en wereldwijde bereik.

A.9 Verwerkingslocaties

De AVG bevat specifieke regels voor de doorgifte van persoonsgegevens naar landen buiten de EER. Niet alleen de opslag van persoonsgegevens is relevant om te beoordelen, maar ook bijvoorbeeld de locaties waar gegevens worden geraadpleegd, gestreamd of tijdelijk opgeslagen. In principe mogen persoonsgegevens alleen worden doorgegeven aan landen buiten de EER als daar een passend beschermingsniveau voor de persoonsgegevens is gewaarborgd. Een passend beschermingsniveau kan op verschillende manieren worden bereikt. Indien het land waarnaar gegevens worden doorgegeven een adequaatheidsbesluit van de Europese Commissie heeft ontvangen, kan de bescherming worden beschouwd als gelijkwaardig aan de bescherming binnen de EER. Als een dergelijk adequaatheidsbesluit ontbreekt, kunnen andere mechanismen worden gebruikt om bescherming te waarborgen, zoals het toepassen van de EU-standaardcontractbepalingen.

A.9.1 Feitelijke verwerkingslocaties van AFAS

AFAS heeft haar hoofdkantoor in Nederland. De SLA van AFAS bevat informatie over de verwerkingslocatie van drie subverwerkers. De volgende tabel geeft een overzicht van de informatie in de SLA:

Naam	Onderwerp	Locatie	Land van vestiging	Buiten de EU/EER	Waarborgen internationale doorgifte
Leaseweb Netherlands B.V.	Hosting	Schiphol-Rijk en Haarlem[57]	Nederland	Nee	Niet van toepassing
Leaseweb Deutschland GmbH	Disaster recovery (back-up van data)	Frankfurt	Duitsland	Nee	Niet van toepassing
Microsoft	Niet van toepassing				

Tabel A-1, Verwerkingslocaties subverwerkers

[57] AFAS maakt daarbij gebruik van specifieke datacenters van Leaseweb Netherlands B.V. die zijn gevestigd in Schiphol-Rijk en Haarlem. Deze datacenters vallen onder Nederlandse en Europese wet- en regelgeving. Statement op de website van Leaseweb: **'***Datasoevereiniteit Leaseweb Nederland: We hebben als bedrijf ons hoofdkwartier in Nederland, en onze Nederlandse datacenters vallen uitsluitend onder de Europese wet, inclusief de AVG. Dat betekent dat ze niet onderhevig zijn aan buitenlandse wetgeving – inclusief die van de Verenigde Staten. Daarom kunnen we Europese datasoevereiniteit claimen en het hoogst mogelijke niveau van gegevensbeveiliging conform AVG bieden.'* Geraadpleegd op 18 december 2025 via https://www.leaseweb.com/nl/products-services/dedicated-servers/netherlands?srsltid=AfmBOoqivYL2oAdxdus2ARn6ipXDX6QdTY0U8_IRss4G1NpesxZ84n4x.

Ten aanzien van de subverwerker Microsoft stelt AFAS dat Microsoft voor de verwerkingen die in deze DPIA worden beschreven, niet als subverwerker kwalificeert. Alleen bij specifieke inzet van AI-Assistent 'Jonas' (die buiten de scope van deze DPIA valt) wordt Microsoft als subverwerker ingezet. Uit de SLA blijkt deze informatie echter niet.

De overige subverwerkers die zijn geïdentificeerd tijdens het technisch onderzoek, staan hieronder vermeld:

Naam	Onderwerp	Locatie	Land van vestiging	Buiten de EU/EER	Waarborgen internationale doorgifte
Cloudflare	DDos-beveiliging Versleuteld verkeer	Wereldwijd (het dichtstbijzijnde datacenter bij de gebruiker)	Verenigde Staten	Onbekend	Onbekend
Cookiebot	Cookie banner	Onbekend	Denemarken	Nee	Niet van toepassing
Google	Videospeler	Onbekend	Verenigde Staten	Onbekend	Onbekend

Tabel A-2, Verwerkingslocaties van andere door SURF geïdentificeerde subverwerkers

In de SLA is vastgelegd dat de verwerking van persoonsgegevens door AFAS en de door haar ingeschakelde subverwerkers uitsluitend plaatsvindt binnen de EER.[58] Het technische onderzoek en de cookieverklaring identificeren echter subverwerkers met 'moeders' in de Verenigde Staten. Dit roept de vraag op of er sprake is van doorgifte buiten de EER.

Hoewel de SLA contractueel bepaalt dat data binnen de EER blijft, kan SURF deze garantie bij het ontbreken van (volledige) subverwerkersovereenkomsten met alle betrokken partijen niet onafhankelijk verifiëren. Dit betekent dat er mogelijk sprake is van doorgifte van persoonsgegevens naar een derde land in de zin van hoofdstuk V AVG, waarvoor passende waarborgen vereist zijn.

Daarnaast zijn bepaalde partijen (zoals Vimeo en LinkedIn) wel vermeld in de cookieverklaring, maar ontbreken zij in de SLA én zijn deze partijen niet naar voren gekomen uit het technisch onderzoek. Ten aanzien van deze partijen geldt eveneens dat deze ondernemingen (althans hun moedermaatschappijen) in de Verenigde Staten zijn gevestigd. Dit betekent dat ook hier mogelijk sprake is van doorgifte van persoonsgegevens naar een derde land in de zin van hoofdstuk V AVG, waarvoor passende waarborgen vereist zijn.

[58] AFAS Service License Agreement April 2026, paragraaf 5.7, geraadpleegd op 9 juni 2026 via https://klant.afas.nl/sla-av.

A.9.2 Doorgiftemechanismen

A.9.2.1 Adequaatheidsbesluit

Een adequaatheidsbesluit houdt in dat een derde land (of een bepaalde sector binnen een land) een passend niveau van gegevensbescherming in de nationale wetgeving biedt. De Europese Commissie (EC) stelt dan vast dat deze bescherming in dat land van een vergelijkbaar niveau is als de AVG. Dat betekent dat er geen aanvullende waarborgen getroffen hoeven worden.

Momenteel zijn er adequaatheidsbesluiten met betrekking tot Andorra, Argentinië, Canada (alleen commerciële organisaties), de Faeröer Eilanden, Guernsey, Israël, Isle of Man, Japan, Jersey, Nieuw-Zeeland, Uruguay, Verenigd Koninkrijk, Verenigde Staten (organisaties die gecertificeerd zijn onder het Data Privacy Framework (DPF)), Zwitserland en Zuid-Korea.[59]

Met uitzondering van het Verenigd Koninkrijk hebben deze adequaatheidsbesluiten geen betrekking op gegevensuitwisselingen in de rechtshandhavingssector, die vallen onder de richtlijn inzake rechtshandhaving (artikel 36 van Richtlijn (EU) 2016/680).

Op 10 juli 2023 zijn nieuwe afspraken in werking getreden tussen de EC en de VS over de doorgifte van persoonsgegevens vanuit de EER naar de VS. Die afspraken staan bekend onder de naam Data Privacy Framework.[60] Dat houdt in dat de EC heeft beoordeeld dat het niveau van bescherming van persoonsgegevens in de VS vergelijkbaar is met dat in de EER. Dit adequaatheidsbesluit is onderdeel van het Data Privacy Framework.

Organisaties in de VS kunnen meedoen aan het Data Privacy Framework. Doorgifte van persoonsgegevens vanuit de EER naar deze organisaties is dan toegestaan zonder dat de Europese partij extra juridische en technische maatregelen hoeft te nemen.

Google LLC, Cloudflare, inc, Vimeo.com, Inc, en LinkedIn Corporation doen mee aan het Data Privacy Framework.[61]

---

[59] Europese Commissie, *Adequacy decisions*, geraadpleegd op 30 maar 2026 via https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[60] Europese Commissie, *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows*, geraadpleegd op 30 maart 2026 via,https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

[61] Data Privacy Framework Program, '*Data Privacy Framework List*', geraadpleegd op 30 maart 2026 via https://www.dataprivacyframework.gov/list.

A.10 Bewaartermijnen

A.10.1 Bewaartermijn als verwerkingsverantwoordelijke

Verwerkingsverantwoordelijken hebben de wettelijke verplichting om persoonsgegevens niet langer te bewaren dan noodzakelijk om de verwerkingsdoeleinden te verwezenlijken.[62] Dat betekent dat zowel instellingen én AFAS verantwoordelijk zijn voor het beschrijven van de (wettelijke) bewaartermijn en het hebben van een proces omtrent vernietiging/verwijdering voor eigen doeleinden, zie A.3 Doeleinden van de gegevensverwerking.

A.10.1.1 Instellingen

Het beschrijven en hebben van een proces ligt in het verantwoordelijkheidsgebied van de instelling en valt daarmee buiten de scope van deze DPIA. Voor bewaartermijnen verwijst SURF de instellingen naar de specifiek voor het onderwijs opgestelde selectielijsten.

A.10.1.2 AFAS

Uit het technisch onderzoek is gebleken dat op de gegenereerde rapportages (zie bijlage) geen automatische bewaartermijnen van toepassing zijn. De verantwoordelijkheid voor verwijdering of archivering ligt bij de medewerker of het team dat de gegevens heeft opgevraagd. Voor SURF is onduidelijk of AFAS een bewaartermijn heeft beschreven en beschikt over een proces omtrent de vernietiging of verwijdering van deze rapportages.

A.10.2 AFAS: Bewaartermijn als verwerker

AFAS geeft in haar Help Center aan dat de instellingen, in hun rol als verwerkingsverantwoordelijke, de bewaartermijnen vastleggen en hun persoonsgegevens op eigen initiatief dienen te verwijderen uit Profit.[63]

A.10.2.1 Bewaartermijnen vastleggen in Profit

In Profit is het mogelijk voor de instellingen om zelf bewaartermijnen in jaren vast te leggen voor een type dossieritem en/of voor een kenmerkcombinatie van een type dossieritem.[64] De instelling bepaalt eveneens het startmoment van de bewaartermijn, bijvoorbeeld:

- de aanmaakdatum van het dossieritem
- de begin- en of einddatum
- de uitdienstdatum van de werknemer

A.10.2.2 Verwijderen uit Profit

AFAS verwijdert als verwerker nooit op eigen initiatief persoonsgegevens noch automatisch noch handmatig. Verwijdering door AFAS vindt uitsluitend plaats op basis van een

[62] Art. 5, lid 1, sub e AVG.

[63] AFAS Help Center Nederland, *Verwijderen personen, medewerkers en relaties met mutaties*, geraadpleegd op 4 december 2025 via https://help.afas.nl/help/NL/SE/Crm_PerOrg_Relat_Delete_AVG.htm.

[64] AFAS Help Center Nederland, *Dossieritem verwijderen o.b.v. wettelijke* bewaartermijn, geraadpleegd op 4 december 2025 via https://help.afas.nl/help/NL/SE/CRM_Doss_Legal_Del.htm#o118431.

schriftelijke instructie van de instelling. De instelling kan deze instructie geven via een verzoek via de Klantportal of via de software.[65] De monitorings- en loggingsgegevens (zie bijlage) die klanten zelf niet kunnen beheren worden wél binnen een termijn van 1 jaar verwijdert.

Na het einde van de overeenkomst verwijdert AFAS *alle* persoonsgegevens waarvoor geen wettelijke bewaarplicht voor AFAS zelf geldt, binnen een termijn van 1 jaar.[66] Indien de instelling wenst dat gegevens eerder worden verwijderd, kan zij hiervoor een separaat verzoek indienen.[67]

Er zijn drie verwijdermogelijkheden voor instellingen:

A.10.2.2.1 Dossieritems verwijderen

AFAS verwijdert dossieritems niet automatisch zodra de bewaartermijn is verstreken. De instelling moet hiervoor een verwijderset aanmaken, gebaseerd op een bepaalde peildatum. Vervolgens bepaalt de instelling zelf welke typen dossieritem ze wil meenemen en de verwijderset toont alle relevante dossieritems. De instelling kan eventueel nog dossieritems uitsluiten die ze niet wil verwijderen, bijvoorbeeld na een controle door een medewerker. Daarna start de instelling het verwijderen van de dossieritems die ze wel wil verwijderen.[68] AFAS waarschuwt in haar Help Center dat medewerkers met toegang tot “Te verwijderen dossieritems” alle typen dossieritems kunnen zien.

A.10.2.2.2 Verwijderen van dataset van personen[69]

Het verwijderen van personen in Profit vereist een zorgvuldige, stapsgewijze aanpak omdat een persoon in Profit vaak meerdere rollen vervult, zoals medewerker, gebruiker, cliënt of inkoop- of verkooprelatie. AFAS verwijdert bij het wissen van één rol uitsluitend de daarbij behorende specifieke gegevens; de persoon blijft bestaan zolang er andere gekoppelde rollen of dossieritems aanwezig zijn. De verwerkingsverantwoordelijke moet daarom eerst alle rolgebonden gegevens verwijderen voordat de persoon als entiteit kan worden gewist. Indien bepaalde gegevens niet kunnen worden verwijderd, worden deze binnen Profit verplaatst naar een speciaal aangemaakte anonieme entiteit (“Anoniem persoon” of “Anoniem medewerker”), waarna aanvullende opschoning nodig kan zijn om te waarborgen dat daar niet te veel informatie aanwezig is.

A.10.2.2.3 Opschonen logging

In hoofdstuk A.6.7 Applicatielogging wordt nader ingegaan op de logging en de diverse methoden voor het verwijderen van gegevens.

---

[65] AFAS Service Licence Agreement oktober 2025, paragraaf 5.1, geraadpleegd op 4 december 2025 via https://klant.afas.nl/sla-av.

[66] AFAS Service Licence Agreement oktober 2025, paragraaf 4, geraadpleegd op 4 december 2025 via https://klant.afas.nl/sla-av.

[67] AFAS Service Licence Agreement oktober 2025, paragraaf 5.9, geraadpleegd op 4 december 2025 via https://klant.afas.nl/sla-av.

[68] AFAS Help Center Nederland, *Dossieritem verwijderen o.b.v. wettelijke* bewaartermijn, geraadpleegd op 4 december 2025 via https://help.afas.nl/help/NL/SE/CRM_Doss_Legal_Del.htm#o118431.

[69] AFAS Help Center Nederland, *Persoonsgegevens stapsgewijs verwijderen*, geraadpleegd op 5 december 2025 via https://help.afas.nl/help/NL/SE/Crm_PerOrg_Relat_Delete_AVG.htm.

Part B Beoordeling van de rechtmatigheid van de gegevensverwerking

In het tweede deel van de DPIA wordt de rechtmatigheid van de gegevensverwerking beoordeeld. Dit deel bevat een bespreking van de grondslag, een beoordeling van de noodzaak en evenredigheid van de verwerking, en van de verenigbaarheid van de verwerking met de doeleinden.

B.1 Rechtsgrondslag

De AVG geeft als beginsel dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.[70] Als uitwerking van dit beginsel is geregeld dat een gegevensverwerking alleen rechtmatig is indien deze gebaseerd kan worden op ten minste één van de volgende zes rechtsgronden[71]:

a) de betrokkene heeft **toestemming** gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
b) de verwerking is noodzakelijk voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c) de verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting** die op de verwerkingsverantwoordelijke rust;
d) de verwerking is noodzakelijk om de **vitale belangen** van de betrokkene of van een andere natuurlijke persoon te beschermen;
e) de verwerking is noodzakelijk voor de vervulling van een **taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag** dat aan de verwerkingsverantwoordelijke is opgedragen;
f) de verwerking is noodzakelijk voor de behartiging van de **gerechtvaardigde belangen** van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Daarbij geldt dat per afzonderlijk doel slechts één rechtsgrondslag leidend behoort te zijn, waarbij cumulatie of “shoppen” tussen grondslagen moet worden vermeden. De keuze voor een grondslag dient voorafgaand aan de verwerking te worden gemaakt en te worden onderbouwd, mede in het licht van de beginselen van doelbinding en behoorlijkheid. Het EDPB benadrukt dat:

> *‘’Wanneer verwerkingsverantwoordelijken de passende rechtsgrondslag identificeren in overeenstemming met het behoorlijkheidsbeginsel, zal dit moeilijk zijn als ze niet eerst duidelijk de doeleinden van de verwerking hebben bepaald of*

[70] Artikel 5, lid 1, onder a AVG.

[71] Artikel 6, lid 1 AVG.

wanneer de verwerking van de persoonsgegevens verder gaat dan noodzakelijk is voor de opgegeven doeleinden.''[72]

B.1.1 Grondslagen instellingen (verwerkingsverantwoordelijken)

Deze DPIA richt zich op de verwerkingen die technisch mogelijk zijn of voortkomen uit de inrichting van Profit. Instellingen dienen voor de verwerkingen die zij uitvoeren met behulp van de functionaliteiten van Profit zelf te beoordelen of er per doel een toereikende grondslag aanwezig is.

Artikel 6, lid 1 onder e van de AVG (Taak van algemeen belang)

Instellingen hebben een wettelijke verplichting om een publieke taak uit te voeren, namelijk het organiseren van onderwijs. Om een beroep te doen op deze grondslag, moeten instellingen een noodzakelijkheidstoets uitvoeren om aan te tonen dat de verwerking noodzakelijk is voor de goede uitvoering van hun publieke taak. Het is onwaarschijnlijk dat de verwerking van HR- en payrollgegevens deze toets zal doorstaan. Voor de verwerking van gegevens die niet noodzakelijk zijn voor hun publieke taak, kunnen instellingen mogelijk een van de volgende gronden toepassen.

Artikel 6, lid 1 onder c van de AVG (Wettelijke verplichting)

Voor een groot deel van de HR- en payrollverwerkingen ligt het voor de hand dat deze gebaseerd worden op een wettelijke verplichting. Hierbij kan worden gedacht aan verplichtingen uit fiscale wetgeving, socialezekerheidswetgeving en arbeidsrechtelijke wetgeving. Het hoeft echter niet expliciet in de wet te staan dat persoonsgegevens verwerkt moeten worden om een specifieke taak uit te voeren. Soms is de verplichting in de wet namelijk ruimer geformuleerd. Het is dan aan de instelling om te bepalen of het verwerken van persoonsgegevens noodzakelijk is om aan de verplichting te voldoen.[73]

Artikel 6, lid 1 onder b van de AVG (Uitvoering van een overeenkomst)

De noodzaak voor een verwerking kan ook voortvloeien uit een contractuele verbintenis, zoals de arbeidsovereenkomst met de betrokkene. Ook hier moeten instellingen een noodzakelijkheidstoets uitvoeren om aan te tonen dat het doel van de overeenkomst niet kan worden bereikt zonder de relevante verwerking van persoonsgegevens.[74]

Artikel 6, lid 1 onder f van de AVG (Gerechtvaardigd belang)

In bepaalde gevallen kan een beroep worden gedaan op het gerechtvaardigd belang. Om deze grond te kunnen gebruiken, moeten instellingen beoordelen of zij (1) een

[72] EDPB, Richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens op grond van artikel 6, lid 1, onder b), van de AVG in het kader van de verlening van onlinediensten aan betrokkenen, versie 2.0 (8 oktober 2019), Geraadpleegd op 14 januari 2026 via: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_nl.pdf

[73] Autoriteit Persoonsgegevens, *Grondslagen AVG uitgelegd*, geraadpleegd op 16 maart 2026 via https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/grondslagen-avg-uitgelegd#grondslag-wettelijke-verplichting.

[74] Richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens op grond van artikel 6, lid 1, onder b), van de AVG in het kader van de verlening van onlinediensten aan betrokkenen, EDPB. versie 2.0 (8 oktober 2019), Geraadpleegd op 14 januari 2026 via: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_nl.pdf

gerechtvaardigd belang hebben, (2) de verwerking noodzakelijk is om dit belang te behartigen en (3) of het belang van de instelling zwaarder weegt dan dat van de betrokkenen.[75]

Artikel 6, lid 1 onder a van de AVG (Toestemming)

Toestemming is in de basis geen geschikte grondslag voor HR- en payrollverwerkingen. Door de gezagsverhouding tussen werkgever en werknemer is er sprake van een machtsongelijkheid, waardoor toestemming zelden 'vrijelijk' kan worden gegeven.[76] Dit is alleen een geldige grondslag in uitzonderlijke situaties waarin de werknemer een reële keuze heeft en weigering of intrekking geen nadelige gevolgen heeft.

B.1.2 Grondslagen AFAS (verwerker)

Voor zover het de in A.3.1 en A.3.2 beschreven verwerkingsdoelen betreft, kwalificeert AFAS als verwerker. Omdat AFAS de verwerking namens de instelling uitvoert, geldt de grondslag voor de verwerking die door de instelling wordt gebruikt ook voor AFAS als verwerker.

B.1.3 Grondslagen AFAS (verwerkingsverantwoordelijke)

SURF stelt zich op het standpunt dat AFAS, althans voor het specifieke verwerkingsdoel genoemd in A.3.3 kwalificeert als zelfstandig verwerkingsverantwoordelijke, nu zij feitelijk invloed uitoefent op het doel en de middelen van de verwerkingen. Zie A.7 voor een uitgebreidere analyse van de rolverdeling.

Er is momenteel onvoldoende inzicht in de vraag of er sprake is van verdere verwerkingen door AFAS. Dergelijke verdere verwerkingen zijn slechts rechtmatig indien zij, overeenkomstig artikel 6, lid 4 AVG, verenigbaar zijn met de oorspronkelijke doeleinden waarvoor de persoonsgegevens door de instellingen zijn verzameld. Deze toets wordt uitgevoerd, aan de hand van de volgende factoren:

a) Ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld, en de doeleinden van de voorgenomen verdere verwerking;
b) Het kader waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke betreft;
c) De aard van de persoonsgegevens, met name of bijzondere categorieën van persoonsgegevens worden verwerkt;
d) De mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen;
e) Het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.

[75] Autoriteit Persoonsgegevens, *Grondslagen AVG uitgelegd: Gerechtvaardigd belang*, geraadpleegd op 16 maart 2026 via https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/grondslagen-avg-uitgelegd#grondslag-gerechtvaardigd-Belang.

[76] Art. 7 AVG.

SURF heeft AFAS verzocht om nadere informatie te delen over deze verwerkingen om ook te kunnen vaststellen of er sprake is van verenigbare verder verwerkingen. Deze informatie is niet gedeeld. Als gevolg daarvan kan niet beoordeeld worden of bij een verdere verwerking aan de voorwaarden voor verenigbare verdere verwerking is voldaan.

Gelet hierop moet SURF concluderen dat er een rechtsgeldige grondslag ontbreekt voor deze verwerkingen.

B.2 Bijzondere en gevoelige persoonsgegevens

Verwerkingsverantwoordelijken moeten een geldige uitzonderingsgrond uit artikel 9 AVG hebben voor de verwerking van bijzondere persoonsgegevens. Aangezien er in Profit bijzondere categorieën gegevens worden verwerkt, moeten de instellingen een beroep kunnen doen op een uitzondering op het verbod van artikel 9 om deze gegevens te kunnen verwerken. Of de instellingen zich op een uitzonderingsgrond kunnen beroepen, valt buiten de scope van deze DPIA.

AFAS

AFAS fungeert als verwerker voor de doeleinden in A.3.1 en A.3.1. Omdat zij dit in opdracht van de instelling doet, is de voor de instelling geldende uitzonderingsgrond ook op AFAS van toepassing.

Voor het doeleinde in A.3.3 is AFAS echter zelf verwerkingsverantwoordelijke. Dit betekent dat AFAS zelf moet vaststellen of ze zich kunnen beroepen op een uitzonderingsgrond. Daarbij dient te worden opgemerkt dat momenteel niet is vastgesteld door SURF of AFAS bijzondere persoonsgegevens verwerkt voor eigen doeleinde.

B.2.1 Bijzondere categorieën van persoonsgegevens

Aangezien er in AFAS bijzondere categorieën van gegevens worden verwerkt, moeten de instellingen een beroep kunnen doen op een uitzondering op het verbod van artikel 9 om deze persoonsgegevens te kunnen verwerken. Het is aan instellingen zelf om te beoordelen of ze voldoen aan de AVG-voorwaarden om een geslaagd beroep te kunnen doen op deze uitzonderingsgronden voor het verwerken van de bijzondere persoonsgegevens in AFAS.

B.2.1.1 Gezondheidsgegevens

De grootste categorie betreft gezondheidsgegevens. AFAS kan worden gebruikt voor de registratie van ziekteverzuim en afwezigheid. Instellingen kunnen eigen classificaties voor afwezigheid definiëren en koppelen aan werknemersdossiers. Deze classificaties dienen zodanig te zijn ingericht dat zij niet meer informatie over de gezondheidstoestand van de werknemer bevatten dan strikt noodzakelijk voor de administratieve verplichtingen van de werkgever. Werkgevers kunnen hiervoor de bestaande richtlijnen gebruiken. [77]

Daarnaast biedt AFAS de mogelijkheid om opmerkingen toe te voegen in vrije tekstvelden bij het personeelsdossier, waaronder toelichtingen bij afwezigheid. Ook bevat AFAS vooraf gedefinieerde classificaties op basis van wettelijke verplichtingen, fiscale regelgeving en collectieve arbeidsovereenkomsten. Deze classificaties kunnen indirect gezondheidsgegevens bevatten, bijvoorbeeld wanneer wordt vastgelegd dat een werknemer recht heeft op (fiscale) voordelen in verband met een handicap of dat sprake is van loondoorbetaling bij ziekte.

[77] Autoriteit Persoonsgegevens, *Beleidsregels verwerking persoonsgegevens gezondheid zieke werknemers*, geraadpleegd op 27 maart 2026 via https://wetten.overheid.nl/BWBR0037896/2016-04-29.

Een voor de hand liggende uitzondering voor ten minste een deel van de gezondheidsgegevens is artikel 9, lid 2, onder b), van de AVG, wanneer "*de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht*". Hieraan is gevolg gegeven in artikel 30, lid 1, onder b, van de Nederlandse uitvoeringswet AVG, die werkgevers toestaat gezondheidsgegevens te verwerken indien de verwerking noodzakelijk is voor:

a. een correcte uitvoering van wettelijke bepalingen, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene; of
b. de re-integratie of begeleiding van werknemers of uitkeringsgerechtigden in verband met ziekte of arbeidsongeschiktheid.

De AP heeft richtlijnen gepubliceerd over wat wel en niet noodzakelijk is in 'De zieke werknemer'[78], waarvan de geldigheid is bevestigd in de boete die zij aan CP&A heeft opgelegd.[79]

B.2.1.2 Politieke en vakbondsgegevens

Salarisgegevens over een werknemer kunnen ook politieke gegevens zijn, wanneer daaruit blijkt dat de werknemer politiek verlof heeft gekregen, en gegevens over vakbondslidmaatschap, wanneer daaruit blijkt dat de werkgever bijdraagt aan de betaling van de vakbondsbijdrage.

B.2.1.3 Raciaal of etnisch afgeleide gegevens

De nationaliteit, in combinatie met de geboorteplaats en het geboorteland kan informatie opleveren over het ras of de etnische afkomst van een betrokkene. Verwerking van deze gegevens is uitsluitend toegestaan als dit noodzakelijk is voor de identificatie van de werknemer of het toepassen van positieve discriminatie.[80]

B.2.1.4 Vrije tekstvelden

Het is mogelijk om door middel van vrij in te vullen velden opmerkingen toe te voegen aan dossiers van betrokkenen. Deze vrije velden dienen geen bepaald doel en instellingen zijn dus vrij hier zelf invulling aan te geven. Bij het aanmaken van vrije velden kan het functioneel beheer aanvinken of deze gevoelige of bijzondere persoonsgegevens (mogen) bevatten.[81]

---

[78] Autoriteit Persoonsgegevens, *Beleidsregels verwerking persoonsgegevens gezondheid zieke werknemers*, geraadpleegd op 27 maart 2026 via https://wetten.overheid.nl/BWBR0037896/2016-04-29.

[79] Autoriteit Persoonsgegevens, *Boete CP&A verzuimregistratie*, geraadpleegd op 27 maart 2026 via https://autoriteitpersoonsgegevens.nl/uploads/imported/boete_cpa_verzuimregistratie.pdf.

[80] Autoriteit Persoonsgegevens, *Personeelsdossier,* geraadpleegd op 14 januari via https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/personeelsgegevens/personeelsdossier.

[81] AFAS Help Center Nederland, *Vrije velden kenmerken als Privacygegevens*, geraadpleegd op 11 december 2025 via https://help.afas.nl/help/NL/SE/Crm_Config_PerOrg_Relat_AVG.htm#o93144.

B.2.2 Gevoelige gegevens

Financiële gegevens vormen de belangrijkste groep gevoelige informatie in de salarisadministratie. Deze persoonsgegevens geven informatie over de financiële situatie van betrokkenen. AFAS bevat persoonsgegevens over (wijzigingen in) het salaris van betrokkenen, aanvullende (reiskosten)vergoedingen, pensioen, of er beslag wordt gelegd op hun loon en alle componenten – wettelijk en in hun contract – waaruit hun loon per periode bestaat. Er zijn ook veel vrije tekstvelden die onbedoeld met gevoelige gegevens kunnen worden gevuld.

Hoewel de AVG geen aanvullende bepalingen voor dit soort gegevens kent, brengt de verwerking van dergelijke gevoelige persoonsgegevens een verhoogd risico met zich mee. De verwerkingsverantwoordelijke dient daarom passende technische en organisatorische maatregelen te nemen die nodig zijn om aan de AVG te voldoen.[82]

B.2.3 Nationale identificatienummers

Werkgevers kunnen nationale identificatienummers van werknemers en niet-gesalarieerd personeel verwerken in AFAS.

Nummers die worden gebruikt om een persoon te identificeren en die bij wet zijn voorgeschreven, mogen alleen worden verwerkt voor doeleinden die bij wet zijn gespecificeerd. Het gebruik van deze identificatienummers moet met de grootst mogelijke zorgvuldigheid gebeuren en de noodzaak om deze identificatienummers te gebruiken moet goed worden onderbouwd.[83] Bovendien schrijft de Nederlandse wet voor dat het bsn alleen mag worden gebruikt door overheidsinstanties of door andere organisaties voor zover dit bij wet is voorgeschreven.[84] Werkgevers en opdrachtgevers mogen het bsn alleen onder strikte voorwaarden verwerken voor belastingdoeleinden.[85]

[82] Artikel 24 AVG.

[83] Artikel 87 AVG en artikel 46, lid 1, van de Nederlandse uitvoeringswet AVG.

[84] Artikel 1, onder d, Wet algemene bepalingen burgerservicenummer.

[85] Autoriteit Persoonsgegevens, *BSN op werk*, geraadpleegd op 24 maart 2026

via https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/burgerservicenummer-bsn/bsn-op-het-werk.

B.3 Doelbinding

Het doelbindingsbeginsel schrijft volgens artikel 5 lid 1 sub b AVG het volgende voor:

> *"Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd'*.

In de kern betekent dit dat de verwerkingsverantwoordelijke een specifiek doel moet hebben waarvoor zij persoonsgegevens verzamelt, en deze gegevens alleen mag verwerken voor doeleinden die verenigbaar zijn met dat oorspronkelijke doel. Verwerkingsverantwoordelijken moeten op basis van artikel 5, lid 2, van de AVG kunnen aantonen dat zij dit beginsel naleven (verantwoordingsplicht).

Het is aan de instellingen als verwerkingsverantwoordelijken om te bepalen voor welke doeleinden zij de gegevens in Profit verwerken. Hoofdstuk 2 geeft een overzicht van mogelijke doeleinden voor de verwerking in Profit. In dit hoofdstuk wordt uitsluitend beoordeeld of instellingen zeggenschap hebben over de doeleinden waarvoor AFAS hun persoonsgegevens verwerkt.

Als verwerker mag AFAS persoonsgegevens uitsluitend verwerken in opdracht van de instellingen en in overeenstemming met de in de SLA vastgelegde doeleinden. Indien AFAS persoonsgegevens verwerkt voor eigen doeleinden als zelfstandig verwerkingsverantwoordelijke, dient AFAS transparant te zijn over welke persoonsgegevens worden verwerkt en voor welke specifieke doeleinden. Voor zover sprake is van verdere verwerking door AFAS, geldt dat deze slechts rechtmatig is indien deze verenigbaar is met de oorspronkelijke doeleinden waarvoor de persoonsgegevens door de instellingen zijn verzameld.[86] AFAS dient deze verenigbaarheid aantoonbaar te maken.

Geconcludeerd kan worden dat instellingen geen controle hebben over de verwerking voor de in A.3.3 beschreven doeleinden en niet in staat zijn deze verwerking te stoppen indien deze plaatsvindt. De oorzaken hiervan zijn:

- AFAS heeft ervoor gekozen om in de SLA geen concrete omschrijving op te nemen van de verwerkingsdoeleinden van de instellingen. Bij gebrek aan een duidelijke en gedocumenteerde afbakening van doeleinden kan niet worden vastgesteld of wordt voldaan aan het beginsel van doelbinding.

[86] Artikel 5 lid 1 onder b en artikel 6 lid 4 AVG.

- Er ontbreekt transparantie van AFAS ten aanzien van eigen verwerkingsdoeleinden voor persoonsgegevens die via de instellingen zijn verkregen. Hierdoor zijn instellingen niet in staat om te voldoen aan hun verantwoordingsplicht.

Indien er sprake is van een verdere verwerking: SURF kan niet met zekerheid vast stellen of sprake is van (on)verenigbare verdere verwerking door het ontbreken van een duidelijke afbakening van doeleinden en van transparantie over (verdere) verwerkingen. Dit leidt tot een verhoogd risico voor de rechten en vrijheden van betrokkenen.

B.4 Noodzaak en evenredigheid

Alle verwerkingen moeten voldoen aan de beginselen van noodzaak en evenredigheid. Het begrip noodzaak bestaat uit twee samenhangende begrippen, namelijk proportionaliteit en subsidiariteit. De persoonsgegevens die worden verwerkt, moeten noodzakelijk zijn voor het doel van de verwerking. Proportionaliteit betekent dat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding staat tot de doeleinden. Subsidiariteit betekent dat de doeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, kunnen worden verwezenlijkt.

Evenredigheid betekent dat er een evenwicht is tussen de belangen van de betrokkene en de belangen van de verwerkingsverantwoordelijke. Een evenredige gegevensverwerking houdt in dat de hoeveelheid verwerkte gegevens niet buitensporig is in verhouding tot het doel van de verwerking. Als een verantwoordelijke zijn doel kan bereiken door minder persoonsgegevens te verwerken, moet hij de hoeveelheid verwerkte persoonsgegevens beperken tot wat noodzakelijk is. Daarom mag een verantwoordelijke alleen die persoonsgegevens verwerken die noodzakelijk zijn om het legitieme doel te bereiken. De toepassing van het beginsel van proportionaliteit is dus nauw verwant aan de beginselen van gegevensbescherming uit artikel 5 van de AVG.

In dit hoofdstuk wordt onderzocht of AFAS instellingen in staat stelt te voldoen aan de vereisten van noodzakelijkheid en evenredigheid. Instellingen kunnen dit gebruiken om een volledige beoordeling uit te voeren op basis van de details van hun HRM- en payroll processen.

B.4.1 Doeltreffendheid en subsidiariteit

Om de noodzaak van de verwerkingsactiviteiten in AFAS te beoordelen, zal de DPIA onderzoeken of AFAS een doeltreffend instrument is om de in hoofdstuk 2 beschreven doeleinden te bereiken. Er zal ook worden beoordeeld of er minder ingrijpende alternatieven (zoals andere tools) beschikbaar zijn voor AFAS om dezelfde doeleinden te bereiken.

B.4.1.1 Doeltreffendheid

Het hoofddoel van de instellingen is om HRM- en payroll processen snel en efficiënt uit te voeren in het belang van een verantwoord personeelsbeleid voor zowel het individu als de organisatie als geheel. Een tool die personeels- en payrolladministratie combineert en helpt bij het automatiseren en stroomlijnen van processen, is een effectieve manier om dit te bereiken.

B.4.1.2 Subsidiariteit

Om de bedrijfsactiviteiten op het gebied van HRM te kunnen uitvoeren, zullen de meeste instellingen tot de conclusie komen dat een HRM-applicatie zoals AFAS noodzakelijk is. De keuze voor een bepaalde applicatie heeft grote gevolgen voor de impact op de privacy bij de verwerking van persoonsgegevens, aangezien deze bepaalt met welke leverancier instellingen hun gegevens delen. Deze DPIA heeft geen marktonderzoek gedaan naar alternatieve applicaties die mogelijk een minder ingrijpende verwerking van persoonsgegevens met zich brengen. Deze vergelijking moeten instellingen zelf maken.

Het feit dat AFAS de architectuur van de eigen applicatie verzorgt, betekent dat alle persoonsgegevens (zoals klantgegevens, gebruiksgegevens, loggegevens) niet worden gedeeld met andere leveranciers (met mogelijk veel subverwerkers en locaties buiten de EER). AFAS maakt daarbij gebruik van Leaseweb als hostingprovider, waarbij de servers zich binnen de EER bevinden (Nederland).

Daarnaast maakt AFAS gebruik van andere subverwerkers, zoals nader gespecificeerd in A.7. De SLA benoemt echter niet alle verwerkingen en subverwerkers.[87] Daarnaast zijn een aantal van deze subverwerkers, althans hun moedermaatschappijen, gevestigd in de Verenigde Staten. In de SLA is vastgelegd dat de verwerking van persoonsgegevens door AFAS en de door haar ingeschakelde subverwerkers uitsluitend plaatsvindt binnen de EER.[88] SURF kan deze garantie echter niet verifiëren door het ontbreken van (volledige) subverwerkersovereenkomsten. Doordat onvoldoende inzicht is in deze verwerkingen en subverwerkers, kan niet worden vastgesteld of de verwerkingen strikt noodzakelijk zijn voor het aanbieden van Profit.

Een ander punt is dat de AFAS Pocket mobiele app beschikbaar is via de Apple App Store en de Google Play Store. Wanneer een betrokkene de app downloadt, wordt er automatisch een koppeling gemaakt tussen het gebruik van de app en het persoonlijke Apple- of Google-account van de betrokkene. Dit betekent dat het hebben van een Apple-account of een Google-account noodzakelijk is om de app te gebruiken, waardoor deze platforms inzicht krijgen in het feit dat de app is geïnstalleerd. Deze vorm van gegevensverwerking is niet strikt noodzakelijk voor het aanbieden van de app.

[87] AFAS maakt gebruik van een Service Level Agreement (SLA), en geen gespecificeerde Verwerkingsovereenkomst.

[88] AFAS Service License Agreement April 2026, paragraaf 5.7, geraadpleegd op 9 juni 2026 via https://klant.afas.nl/sla-av.

B.4.2 Proportionaliteit

Om de evenredigheid van de verwerkingsactiviteiten te beoordelen, moet worden afgewogen of de inbreuk van de activiteiten in verhouding staat tot de doeleinden ervan. Bij de beoordeling van de inbreuk moet rekening worden gehouden met de (privacy)belangen van de betrokkenen. Om deze afweging te maken, worden vijf van de beginselen uit artikel 5 van de AVG gebruikt.

B.4.2.1 Rechtmatigheid, behoorlijkheid en transparantie

Rechtmatigheid houdt in dat aan alle wettelijke voorwaarden voor gegevensverwerking wordt voldaan. De instellingen beschikken over hun eigen grondslag en AFAS heeft wel verwerkersovereenkomsten. De verwerkersovereenkomsten zijn echter onvolledig, omdat AFAS ervoor heeft gekozen om in de SLA[89] geen omschrijving op te nemen van: categorieën persoonsgegevens, categorieën betrokkenen, verwerkingsdoeleinden, betrokkenen en bewaartermijnen. Indien gewenst kunnen de categorieën persoonsgegevens op verzoek van de klant worden opgeslagen bij de overeenkomst. Ook zijn niet alle betrokken subverwerkers opgenomen in de verwerkersovereenkomst. Daarnaast ontbreekt een bijlage of nadere uitwerking van de te treffen technische en organisatorische beveiligingsmaatregelen in de SLA. Tot slot is er is in de SLA geen regeling opgenomen over wanneer doorgifte van persoonsgegevens naar buiten de EER is toegestaan, noch een beschrijving van de bestaande doorgiftes.

Het beginsel van *transparantie* zorgt er niet alleen voor dat toestemming op de hoogte moet zijn, maar ook dat volledige transparantie van gegevenspraktijken en rechten voor gebruikers wordt gewaarborgd. Door het gebrek aan informatie over alle verwerkingen, kunnen AFAS en instellingen niet aan deze eis voldoen. Er heerst ook onduidelijkheid rond de verwerking voor eigen doeleinden.

Behoorlijkheid is een overkoepelend beginsel dat vereist dat persoonsgegevens niet worden verwerkt op een manier die nadelig, discriminerend, onverwacht of misleidend is voor de betrokkene.[13] Vanwege het gebrek aan transparantie kan niet worden beoordeeld of verdere verwerking eerlijk is ten opzichte van de betrokkenen en in overeenstemming is met hun redelijke verwachtingen ten aanzien van de (metadata over de) verwerking van hun HRM- en payrollgegevens.

Conclusie: Zonder dat kan worden uitgesloten dat AFAS persoonsgegevens verder verwerken voor doeleinden die niet in overeenstemming zijn met de doeleinden van de instellingen, kunnen zij AFAS niet gebruiken op een manier die in overeenstemming is met de beginselen van rechtmatigheid, behoorlijkheid en transparantie. Zie voor een uitgebreide toelichting B.13 Grondslagen AFAS (verwerkingsverantwoordelijke).

[89] AFAS maakt gebruik van een Service Level Agreement (SLA), en geen gespecificeerde Verwerkingsovereenkomst.

B.4.2.2 Minimale gegevensverwerking

De beginselen van minimale gegevensverwerking en privacy by design vereisen dat de verwerking van persoonsgegevens beperkt blijft tot wat noodzakelijk is. De gegevens moeten *'toereikend, ter zake dienend en beperkt zijn tot hetgeen nodig is voor de doeleinden waarvoor zij worden verwerkt'*.[90] Dit betekent dat de verwerkingsverantwoordelijke geen gegevens mag verzamelen en opslaan die niet rechtstreeks verband houden met een legitiem doel. Volgens dit beginsel moeten de standaardinstellingen voor de gegevensverzameling zodanig worden ingesteld dat de gegevensverzameling tot een minimum wordt beperkt door gebruik te maken van de meest privacyvriendelijke instellingen.

AFAS biedt tal van mogelijkheden om workflows voor verschillende processen te ontwerpen met verschillende soorten velden, waaronder open tekstvelden. Het is aan de instellingen om ervoor te zorgen dat zij alleen de gegevens verwerken die nodig zijn voor hun processen en dat zij open tekstvelden zodanig gebruiken dat het doel ervan duidelijk is, zodat zij gebruikers niet aanmoedigen om meer persoonsgegevens te delen dan nodig is. Omdat de inrichting van workflows door de instelling zelf gebeurt, bestaat het risico dat privacy-by-design en dataminimalisatie niet consequent worden toegepast.

De cookieverklaring voor klant.afas.nl (help.afas.nl) staat onder beheer van Cookiebot en is daardoor niet volledig onder directe controle van AFAS. In de cookieverklaring zijn bepaalde cookies als "noodzakelijk" aangemerkt, terwijl deze niet strikt noodzakelijk zijn voor de technische werking of beveiliging van de dienst. Daarnaast zijn er cookies waarvoor nog geen beschrijving beschikbaar is. Hierdoor is het moeilijk om te beoordelen of de gegevens die ze verzamelen noodzakelijk zijn voor legitieme doeleinden. Dit leidt mogelijk tot een inbreuk op het beginsel van minimale gegevensverwerking.

Conclusie: Instellingen hebben grotendeels zelf de controle over hun praktijken inzake minimale gegevensverwerking met betrekking tot de persoonsgegevens die zij in AFAS vastleggen. Of het beginsel van minimale gegevensverwerking wordt nageleefd bij de verwerking van door AFAS bij het plaatsen van cookies, kan echter niet worden beoordeeld vanwege een gebrek aan informatie.

B.4.2.3 Juistheid

Het beginsel van juistheid vereist dat de persoonsgegevens juist zijn en, waar nodig, worden bijgewerkt. Er moeten alle redelijke maatregelen worden genomen om ervoor te zorgen dat persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld worden gewist of gerectificeerd.[91]

AFAS biedt koppelingen om gegevens automatisch uit andere systemen te importeren, waardoor de juistheid van de gegevens bij het invoeren in de applicatie wordt gewaarborgd. Daarnaast kunnen gebruikers handmatig persoonsgegevens invoeren en bewerken in Profit.

[90] Artikel 5, lid 1, onder c, AVG.

[91] Artikel 5, lid 1, onder d, AVG.

Om onjuiste gegevens te voorkomen, past AFAS waar mogelijk datavalidatie toe. Mocht er toch sprake zijn van onjuiste gegevens in de applicatie, dan kan de gebruiker deze aanpassen.

Conclusie: Binnen Profit zijn geen technische of functionele beperkingen zijn aangetroffen die instellingen beletten om aan het juistheidsbeginsel te voldoen.

B.4.2.4 Opslagbeperking

Het beginsel van opslagbeperking vereist dat persoonsgegevens slechts zo lang worden bewaard als nodig is voor het betreffende doel. Gegevens moeten worden "*bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren, en dit niet langer dan nodig is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt.*"[92] Dit beginsel vereist daarom dat persoonsgegevens worden gewist zodra ze niet langer nodig zijn om het door de verwerkingsverantwoordelijke nagestreefde doel te bereiken.

AFAS biedt geen functionaliteit aan die het mogelijk maakt om persoonsgegevens na het verstrijken van de bewaartermijn geautomatiseerd te verwijderen of om een melding te krijgen na het verstrijken van een bewaartermijn. Hierdoor bestaat het risico dat persoonsgegevens langer bewaard blijven dan noodzakelijk.

Daarnaast genereert en bewaart AFAS verschillende vormen van logbestanden, zie ook A.6.6 Monitoren door AFAS & A.6.7 Applicatielogging. De meeste logbestanden moeten handmatig door de instelling worden verwijderd na het verstrijken van de gestelde bewaartermijnen. Daarnaast bestaan er loggingslagen waarin activiteiten rond het raadplegen van logs zelf worden vastgelegd (zogeheten *logging van logging*). Deze specifieke gegevens kunnen technisch niet of slechts zeer beperkt worden verwijderd.

Voor eventuele verdere verwerking door AFAS is het onduidelijk welke bewaartermijnen zij hanteren en of deze in overeenstemming zijn met het beginsel van opslagbeperking.

Conclusie: Door de afhankelijkheid van handmatige acties en het ontbreken van automatische verwijdermogelijkheden is de kans reëel dat niet alle logbestanden tijdig of volledig worden verwijderd. Hierdoor bestaat het risico dat persoonsgegevens langer bewaard blijven dan noodzakelijk, in strijd met de beginselen van minimale gegevensverwerking en opslagbeperking.

Er kan echter niet worden beoordeeld of dit ook geldt voor de verwerkingen door AFAS als verwerkingsverantwoordelijke, zoals nader beschreven in A.3 Door AFAS vastgestelde doeleinden.

[92] Artikel 5, lid 1, onder e, eerste zin AVG.

B.4.2.5 Integriteit en vertrouwelijkheid

Persoonsgegevens moeten verwerkt worden op een dusdanige manier dat passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.[93]

Read access logging

AFAS ondersteunt read access logging zoals beschreven in A.6.7.8 Read Access logging. Het ondersteunen van *read access logging* verkleint het risico dat bij een autorisatiefout of incident niet kan worden vastgesteld of onbevoegde personen persoonsgegevens hebben ingezien. Daardoor is het bij een mogelijk datalek mogelijk om vast te stellen of, en wiens, persoonsgegevens door onbevoegde gebruikers zijn ingezien. Dit betekent dat instellingen adequate en gerichte maatregelen kunnen nemen.

Beheer gebruikersrechten

AFAS biedt een autorisatie-tool aan waardoor een instelling de autorisaties kan inrichten, zoals beschreven in A.5.3.9 Beheer gebruikersrechten**.** Daarnaast heeft Profit een functionaliteit genaamd 'autorisatie auditor' waarmee extra regels kunnen worden opgesteld om 'te brede' autorisaties te inventariseren, zoals beschreven in A.5.3.9.1 Autorisatie Auditor. Door deze oplossing kan een instelling de functiescheiding in de organisatie beter bewaken.

Versleuteling

AFAS beheert de encryptiesleutel zelf, die is opgeslagen op SQL-servers, met een back-up sleutel onder een wachtwoordoplossing. De sleutels zijn toegankelijk voor geautoriseerd personeel van AFAS, zoals systeemingenieurs en productbeheerders. Gegevens worden zowel in rust als tijdens verzending versleuteld volgens de geldende industrienormen. Zie bijlage 3 (Beveiligingsgaranties) voor een uitgebreide toelichting.

Speciale en gevoelige categorieën gegevens

Aangezien de verwerking van gevoelige en speciale categorieën gegevens inherent een hoger risiconiveau met zich meebrengt, zijn er aanvullende beveiligingsmaatregelen nodig om een passend beveiligingsniveau te waarborgen.

De informatie over versleuteling is onvolledig. AFAS merkt op dat klantomgevingen binnen 72 uur na aanmaak worden versleuteld en dat nieuwe back-ups worden versleuteld, maar details over bredere versleutelingscontroles ontbreken, waaronder:

- Versleuteling van persoonsgegevens tijdens het transport
- Volledige versleuteling van gegevens in rust in alle omgevingen, gegevens tijdens het transport. Wat wordt er precies geïmplementeerd?
- Procedures en verantwoordelijkheden voor sleutelbeheer

Conclusie: Gezien de verwerking van bijzondere en gevoelige persoonsgegevens in Profit, is aanvullende verduidelijking noodzakelijk om vast te stellen of de toegepaste versleuteling een passend beveiligingsniveau waarborgt.

[93] Artikel 5, lid 1, onder f AVG jo. artikel 32 lid 1 en 2 AVG.

B.5 Rechten van betrokkenen

Betrokkenen hebben onder de AVG diverse rechten met betrekking tot hun persoonsgegevens. Dit betreft onder andere het recht op inzage, rectificatie en het recht op gegevenswissing (vergetelheid).

Het is de verantwoordelijkheid van de verwerkingsverantwoordelijke om informatie te verstrekken en deze verzoeken naar behoren en tijdig te behandelen. Indien de verwerkingsverantwoordelijke een verwerker heeft ingeschakeld, schrijft de AVG voor dat in de verwerkersovereenkomst moet worden opgenomen dat de verwerker de verwerkingsverantwoordelijke zal bijstaan bij het voldoen aan verzoeken van betrokkenen met betrekking tot hun rechten.

In dit hoofdstuk wordt onderzocht of instellingen en AFAS voldoen aan de AVG-vereisten met betrekking tot de rechten van betrokkenen en of betrokkenen deze rechten daadwerkelijk kunnen uitoefenen.

Het uitvoeren van het recht op beperking van de verwerking (artikel 18 AVG) zal in de praktijk resulteren in het rectificeren en wissen van gegevens. Daarom wordt deze niet apart besproken in dit hoofdstuk.

B.5.1 Recht op informatie

Het recht op transparante informatie (artikel 12 AVG) houdt in dat betrokkenen op een begrijpelijke en toegankelijke manier moeten worden geïnformeerd over de verwerking van hun persoonsgegevens. Dit stelt hen in staat om hun rechten onder de AVG effectief uit te oefenen.

Er ontbreekt essentiële informatie (zoals informatie over de categorieën persoonsgegevens, categorieën betrokkenen, verwerkingsdoeleinden, betrokkenen en bewaartermijnen) over de verwerkingen met betrekking tot Profit en niet alle betrokken subverwerkers worden niet vermeld in de SLA. Hierdoor kan de instelling als verwerkingsverantwoordelijke betrokkenen niet op transparante wijze informeren over de gegevensverwerking.

Daarnaast ontbreekt essentiële informatie over de (verdere) verwerkingen die AFAS als verwerkingsverantwoordelijke uitvoert, zoals nader omschreven in A.3.3 Door AFAS vastgestelde doeleinden. Deze verwerkingen zijn niet expliciet omschreven in de SLA.[94]

Instellingen die Profit gebruiken kunnen op dit moment niet voldoen aan hun transparantieverplichting onder de AVG.

[94] AFAS Service License Agreement januari 2026, *paragraaf 2.3.6*, geraadpleegd op 27 maart 2026 via https://klant.afas.nl/sla-av.. Zie voor de specifieke verwerkingsactiviteiten de volgende paragrafen in de DPIA: A.5.6.1, A.5.6.2, A.5.6.3 en A.5.6.4 en de A.5.6.5.

B.5.2 Recht op inzage

Het recht op inzage (artikel 15 AVG) geeft betrokkenen het recht om te weten welke persoonsgegevens over hen worden verwerkt en om hiervan een kopie te ontvangen. Op verzoek moeten verwerkingsverantwoordelijken de betrokkenen meedelen of zij persoonsgegevens over hen verwerken (rechtstreeks of via een verwerker). Indien dit het geval is, moeten zij de betrokkenen een kopie verstrekken van de verwerkte persoonsgegevens, samen met informatie over de doeleinden van de verwerking, de ontvangers aan wie de gegevens zijn doorgegeven, de bewaartermijn(en) en informatie over hun verdere rechten als betrokkenen, zoals het indienen van een klacht bij de AP.

Als verwerkingsverantwoordelijken moeten instellingen voldoen aan verzoeken om inzage die door betrokkenen worden ingediend. AFAS moet instellingen hierbij ondersteunen.

Als onderdeel van het technische onderzoek zijn is een inzageverzoek ingediend bij de leverancier. SURF heeft geen reactie op haar inzageverzoek ontvangen.

B.5.3 Recht van bezwaar (artikel 21 AVG)

Betrokkenen hebben het recht bezwaar te maken tegen verwerking op basis van gerechtvaardigde belangen of openbare taken, evenals tegen direct marketing (artikel 21 AVG).

Voor zover instellingen verwerkingsactiviteiten uitvoeren op basis van hun gerechtvaardigde belang(en), moeten zij het recht van bezwaar faciliteren. AFAS is verplicht om instellingen, voor zover redelijkerwijs mogelijk, bij te staan bij het faciliteren van dergelijke bezwaren.

B.5.4 Recht op rectificatie en gegevenswissing

Betrokkenen hebben het recht om onjuiste of verouderde gegevens te laten corrigeren, onvolledige gegevens te laten aanvullen (artikel 16 AVG) en onder bepaalde omstandigheden persoonsgegevens te laten verwijderen (artikel 17 AVG).

AFAS biedt de mogelijkheid om gegevens eenvoudig in de applicatie te corrigeren en te verwijderen. Indien onjuiste of onvolledige persoonsgegevens in logbestanden worden verwerkt, is dit te wijten aan een onjuistheid of onvolledigheid in de brongegevens, d.w.z. de persoonsgegevens die bij het aanmaken van het account zijn geregistreerd.

Logbestanden registreren per definitie de persoonsgegevens zoals deze in de brongegevens zijn vastgelegd. Daarom moet elk verzoek tot rectificatie van deze gegevens gericht zijn op de brongegevens, en niet op de gegevens in logbestanden. Verzoeken tot verwijdering van persoonsgegevens in logbestanden zijn doorgaans niet van toepassing, aangezien geen van de gronden in artikel 17, lid 1, AVG van toepassing is. Het doel van de verwerking van deze persoonsgegevens is het waarborgen van de veiligheid van persoonsgegevens en, meer in het algemeen, van de AFAS-omgeving. De in logbestanden vastgelegde persoonsgegevens blijven voor dit doel noodzakelijk totdat deze logbestanden worden verwijderd in overeenstemming met het toepasselijke bewaarbeleid. Bovendien zou het corrigeren of verwijderen van persoonsgegevens uit logbestanden dit doel ondermijnen en de door de AVG vereiste bescherming van de persoonsgegevens van de betrokkene in gevaar brengen.

Indien de betrokkene een complete verwijdering verzoekt, en de instelling voert dit uit met de functie voor het verwijderen van een persoon[95], dan moeten eerst alle rolgebonden gegevens verwijderd worden voordat de persoon als entiteit kan worden gewist. Indien bepaalde gegevens niet kunnen worden verwijderd, worden deze binnen Profit verplaatst naar een speciaal aangemaakte anonieme entiteit (“Anoniem persoon” of “Anoniem medewerker”), waarna aanvullende opschoning nodig kan zijn door de instelling om te waarborgen dat daar niet te veel informatie aanwezig is.

Bij een verwijderverzoek zullen ook de persoonsgegevens nog in de verschillende back-ups terug te vinden zijn. De back-ups zijn versleuteld en zolang er geen *restore* dient plaats te vinden, worden deze gegevens niet actief verwerkt of geraadpleegd en worden ze geschoond na het aflopen van de bewaartermijn.

B.5.5 Recht op dataportabiliteit

Het recht op dataportabiliteit houdt in dat betrokkenen het recht hebben om hun persoonsgegevens te laten overdragen (artikel 20 AVG). Profit bevat geen technische of functionele beperkingen die instellingen belemmeren bij het honoreren van verzoeken om dataportabiliteit (indien de betrokkene daarvoor in aanmerking komt). In Profit is eenvoudig een machine-leesbare export te downloaden van de persoonsgegevens per medewerker.

B.5.6 Recht om niet te worden onderworpen aan geautomatiseerde besluitvorming

Er vindt geen automatische besluitvorming plaats in AFAS.

[95] AFAS Help Center Nederland, *Persoonsgegevens stapsgewijs verwijderen*, geraadpleegd op 5 december 2025 via https://help.afas.nl/help/NL/SE/Crm_PerOrg_Relat_Delete_AVG.htm.

Part C Beschrijving en beoordeling risico's voor de betrokkenen

Dit deel betreft de beschrijving en beoordeling van de risico's voor betrokkenen. Het gaat hierbij om de risico's die tijdens het testen en analyseren zijn vastgesteld, voordat risicobeperkende maatregelen zijn genomen. De risico's worden vervolgens ingedeeld op basis van de waarschijnlijkheid dat ze zich voordoen en de gevolgen voor de rechten en vrijheden van de betrokkenen wanneer ze zich voordoen.

Het model dat in deze DPIA wordt gebruikt, is gebaseerd op 'het Rijksmodel' en maakt gebruik van de risicocategorieën en het risicomodel van de Britse gegevensbeschermingsautoriteit, de ICO. De ICO noemt de volgende hoofdcategorieën van risico's:

- onvermogen om rechten uit te oefenen (met inbegrip van, 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
- enig ander significant economisch of sociaal nadeel.

Deze hoofdcategorieën bieden houvast bij het vaststellen van specifieke risico's. Door de risico's weer te geven op basis van hun potentiële impact op de rechten en vrijheden van betrokkenen, ontstaat een beeld van de hoge, medium en lage risico's. Dit wordt weergegeven in de risicografiek die is ontwikkeld door de Britse toezichthouder ICO, als volgt:

Ernst van de gevolgen voor de betrokkene(n)	Ernstige gevolgen	Laag risico	Hoog risico	Hoog risico
	Enige negatieve gevolgen	Laag risico	Medium risico	Hoog risico
	Minimale gevolgen	Laag risico	Laag risico	Laag risico
		Heel klein	Redelijke mogelijkheid	Waarschijnlijker dan niet
		Kans (waarschijnlijkheid) dat het risico zich voordoet		

In deze DPIA worden de volgende definities van 'kans dat het risico zich voordoet' en 'ernst van de gevolgen gehanteerd om de risico's te beoordelen:

Kans dat het risico zich voordoet	Betekenis
Heel klein	Het is onwaarschijnlijk dat dit risico zal optreden
Redelijke mogelijkheid	Het is denkbaar dat dit risico zal optreden
Waarschijnlijker dan niet	Het is waarschijnlijk of zeker dat het risico zal optreden

Ernst van de gevolgen	Betekenis
Minimale gevolgen	Als het risico zich voordoet heeft dit weinig of geen gevolgen voor de rechten en vrijheden van betrokkene
Enige negatieve gevolgen	Als het risico zich voordoet heeft dit enige invloed op de rechten en vrijheden van betrokkene
Ernstige gevolgen	Als het risico zich voordoet heeft dit ernstige gevolgen voor de rechten en vrijheden van betrokkene

C.1 Risico-inventarisatie

Bij de uitvoering van deze DPIA zijn de volgende risico's geïdentificeerd:[96]

Rolverdeling en contractuele risico's

C.1.1 Verlies van controle door AFAS als verwerkingsverantwoordelijke

AFAS stelt zich contractueel in geen enkele situatie op als verwerkingsverantwoordelijke voor de persoonsgegevens die binnen de AFAS-software worden verwerkt. De contractuele rolverdeling sluit echter niet aan bij de feitelijke situatie. Tijdens het technisch onderzoek is gebleken dat AFAS feitelijk (verdere) verwerkingen uitvoert die niet expliciet zijn omschreven of begrensd in de SLA, namelijk

- Monitoring om storingen voorkomen of in een vroeg stadium op lossen
- Algemene gebruikersstatistieken verzamelen
- Anonieme statistieken uit de klantomgeving verzamelen
- Het meten en analyseren van systeemreactietijden
- Het verzamelen, monitoren en analyseren van loggegevens om misbruik te voorkomen

SURF stelt zich op het standpunt dat AFAS, althans voor deze specifieke verwerkingsactiviteiten, kwalificeert als zelfstandig verwerkingsverantwoordelijke, nu zij feitelijk invloed uitoefent op het doel en de middelen van deze (verdere) verwerkingen. Zie A.7 Betrokken partijen voor een uitgebreidere analyse van de rolverdeling. Als gevolg hiervan hebben instellingen onvoldoende controle over de wijze waarop persoonsgegevens van betrokkenen worden verwerkt, hetgeen leidt tot een verlies van controle voor betrokkenen

[96] SURF benadrukt dat het merendeel van de geïdentificeerde risico's betrekking hebben op diagnostische gegevens, en nadrukkelijk niet op de gegevens die instellingen zelf in Profit invoeren.

zelf. Indien deze verdere verwerking niet voldoet aan de verenigbaarheidstoets van artikel 6 lid 4 AVG, kan deze niet als rechtmatig worden aangemerkt.

De kans dat dit risico zich voordoet wordt als waarschijnlijker dan niet ingeschat, aangezien de feitelijke situatie reeds laat zien dat AFAS deze verwerkingen uitvoert buiten de contractueel vastgelegde rolverdeling. Indien het risico zich verwezenlijkt, zijn de gevolgen voor de rechten en vrijheden van betrokkenen potentieel ernstig, omdat er een verlies van controle is. Om die reden wordt dit risico gekwalificeerd als een hoog risico.

C.1.2 Verlies van controle en vertrouwelijkheid door onvolledige verwerkersovereenkomsten

Verwerkersovereenkomsten dienen volgens artikel 28 lid 3 AVG het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke te omschrijven. Vanwege de rolverdeling en het karakter van Profit als generieke standaardsoftware, heeft AFAS er bewust voor gekozen om in of naast de SLA[97] geen omschrijving op te nemen van: categorieën persoonsgegevens, categorieën betrokkenen, verwerkingsdoeleinden, betrokkenen en bewaartermijnen. Indien gewenst kunnen de categorieën persoonsgegevens op verzoek van de klant worden opgeslagen bij de overeenkomst. Ook zijn niet alle betrokken subverwerkers (waaronder LinkedIn, Vimeo en Google) opgenomen in de verwerkersovereenkomst.

Doordat de categorieën persoonsgegevens, categorieën betrokkenen, verwerkingsdoeleinden, betrokkenen, bewaartermijnen en (alle) betrokken subverwerkers niet zijn opgenomen in de verwerkersovereenkomst ontbreekt een expliciete instructie van de instelling aan AFAS. Bijvoorbeeld zonder een duidelijke, gedocumenteerde afbakening van doeleinden kan niet worden vastgesteld of sprake is van doelbinding en verenigbare verdere verwerking. Hierdoor ontstaat een verlies van controle over de verwerking van persoonsgegevens.

Daarnaast ontbreekt een bijlage of nadere uitwerking van de te treffen technische en organisatorische beveiligingsmaatregelen in de SLA. Een enkele verwijzing naar een ISO- of NEN-certificering en het klantportaal is in dit kader onvoldoende. Hoewel de verwijzing naar de AFAS Klantportal praktisch is, vormt dit een ‘dynamische’ bron. Dit brengt het risico met zich mee dat de SLA eenzijdig wijzigt zodra de pagina wordt aangepast. Artikel 28 lid 3 sub c AVG vereist dat de verwerker passende maatregelen treft conform artikel 32 AVG, hetgeen een concrete, op de verwerking toegesneden invulling vergt. Zonder nadere specificatie kunnen de instellingen niet beoordelen of daadwerkelijk sprake is van een passend beveiligingsniveau, noch hier effectief op sturen of toezicht houden.

De kans dat het risico zich voordoet is waarschijnlijker dan niet, aangezien de verwerkersovereenkomsten momenteel onvolledig zijn. Als het risico zich voordoet heeft dit ernstige gevolgen voor de rechten en vrijheden van betrokkene aangezien dit kan leiden tot

[97] AFAS maakt gebruik van een Service Level Agreement (SLA), en geen gespecificeerde Verwerkingsovereenkomst.

misbruik of onjuiste verwerking van hun persoonsgegevens, onrechtmachtige doorgifte en beperkte mogelijkheden om hun rechten uit te oefenen. Om die reden wordt dit risico gekwalificeerd als een hoog risico.

C.1.3 C.1.Verlies van controle door het ontbreken van subverwerkersovereenkomsten

Volgens artikel 28 AVG is de verwerkingsverantwoordelijke verplicht om uitsluitend verwerkers in te schakelen die voldoende garanties bieden ten aanzien van de naleving van de AVG. Indien een verwerker subverwerkers inschakelt, mogen deze slechts worden betrokken met voorafgaande (specifieke of algemene) toestemming van de verwerkingsverantwoordelijke en moeten met deze subverwerkers bindende afspraken worden gemaakt waarin dezelfde gegevensbeschermingsverplichtingen worden opgelegd als in de overeenkomst tussen verwerkingsverantwoordelijke en verwerker.[98] Deze contractuele doorlegging is essentieel om te waarborgen dat de instelling controle houdt over de verwerking van persoonsgegevens.[99]

Uit het onderzoek van SURF blijkt het volgende:

- De subverwerkersovereenkomst met Leaseweb is niet langer geldig (verlopen);
- De subverwerkersovereenkomsten met onder meer Cookiebot, Cloudflare en Hunt&Hackett zijn onvolledig, aangezien een specificatie van de verwerkingen ontbreekt;
- Met subverwerkers zoals LinkedIn, Google en Vimeo ontbreken de benodigde overeenkomsten.

Het ontbreken van (geldige) contracten tussen AFAS en andere partijen leidt tot een gebrek aan transparantie over de gegevens die door de partijen worden verwerkt en tot een verlies van controle over deze gegevens. De kans dat dit gebeurt, is waarschijnlijker dan niet, aangezien de documentatie momenteel ontbreekt. Dit kan ernstige schade toebrengen aan de betrokkenen, aangezien het ontbreken van overeenkomsten betekent dat er helemaal geen controle is over deze gegevens. Om die reden wordt dit risico gekwalificeerd als een hoog risico.

Rechten van betrokkenen

C.1.4 Niet uit kunnen oefenen van AVG-rechten door incomplete inzageverzoeken

SURF heeft geen reactie op de inzageverzoeken ontvangen. Wel heeft SURF de mogelijkheid om handmatig data te exporteren vanuit de testomgeving waar de technische analyse heeft plaatsgevonden. Dit betreft contentdata, applicatielogs en accountdata die beschikbaar zijn voor de verwerkingsverantwoordelijke. De inzageverzoeken zijn tot op heden echter onvolledig voor zover het gaat om persoonsgegevens in verwerkingen die onzichtbaar zijn voor de instelling. Dit geldt in ieder geval voor de verwerkingen die AFAS verricht als verwerkingsverantwoordelijke, zoals nader omschreven in risico C.1.2.

[98] Art. 28 lid 2 en 4 AVG.

[99] Art. 24 AVG.

Het niet volledig voldoen aan inzageverzoeken maakt dat betrokkenen hun rechten niet kunnen uitoefenen en geen volledig inzicht hebben in welke gegevens over hen worden verwerkt en hoe deze worden gebruikt.

De kans dat betrokkenen hun inzagerecht (en andere AVG-rechten) niet kunnen uitoefenen is waarschijnlijk dan niet, aangezien AFAS niet in staat was voor één betrokkene tijdig complete inzage te bieden. Als het risico zich voordoet heeft dit ernstige gevolgen voor de rechten en vrijheden van betrokkene, aangezien het kunnen uitoefenen van het inzagerecht noodzakelijk is om andere AVG-rechten te kunnen uitoefenen. Al deze rechten zijn fundamentele rechten van betrokkenen. Om die reden wordt dit risico gekwalificeerd als een hoog risico.

C.1.5 Niet mogelijk om AVG-rechten uit te oefenen en verlies van controle door gebrek aan transparantie subverwerkers

In de SLA[100] zijn meerdere subverwerkers niet opgenomen. Dit betreft onder meer Cookiebot, Cloudflare, Hunt & Hackett, Google, LinkedIn en Vimeo. Daarnaast staat Microsoft vermeld als subverwerker, hoewel AFAS stelt dat Microsoft voor de verwerkingen in deze DPIA juist niet is. Alleen bij specifieke inzet van AI-Assistent ‘Jonas’ (die buiten de scope van deze DPIA valt) wordt Microsoft als subverwerker ingezet. Uit de SLA blijkt deze informatie echter niet. Dit maakt het voor de instellingen als verwerkingsverantwoordelijken moeilijk om het benodigde inzicht in de ontvangende partijen te verkrijgen en te verstrekken aan betrokkenen.

Voor betrokkenen heeft dit het gevolg dat ze hun recht op inzage moeilijker kunnen uitoefenen, doordat een overzicht van ontvangers mogelijk niet (tijdig) beschikbaar is. Daarnaast kunnen de gegevens van betrokkenen hierdoor verwerkt worden door partijen waar geen controle op is, waardoor hun gegevens voor andere doeleinden gebruikt kunnen worden en er een verlies van vertrouwelijkheid kan optreden.

De waarschijnlijkheid dat dit risico optreedt is waarschijnlijker dan niet, aangezien er momenteel geen compleet overzicht is van de subverwerkers van AFAS. De impact ernstig, omdat het mogelijk gaat om alle gegevens die in Profit verwerkt worden onder dit risico vallen, waaronder bijzondere persoonsgegevens. Daarnaast is het uitoefenen van AVG-rechten een fundamenteel recht van betrokkenen. Het niet kunnen uitoefenen hiervan heeft dus een grote impact. Om die reden wordt dit risico gekwalificeerd als een hoog risico.

C.1.6 Niet mogelijk om AVG-rechten uit te oefenen door onduidelijke rolverdeling

De onduidelijke rolverdeling en het ontbreken van transparantie (zoals nader beschreven in hoofdstuk B.5 en risico C.1.1) hebben tot gevolg dat betrokkenen hun rechten niet (effectief) kunnen uitoefenen. Zo zullen betrokkenen in de praktijk niet in staat zijn hun recht

[100] AFAS maakt gebruik van een Service Level Agreement (SLA), en geen gespecificeerde Verwerkingsovereenkomst.

van bezwaar (artikel 21 AVG) uit te oefenen tegen deze verdere verwerking, omdat zij onvoldoende geïnformeerd zijn over het bestaan en de aard daarvan.

De kans dat dit risico zich voordoet wordt als waarschijnlijker dan niet ingeschat, aangezien de feitelijke situatie reeds laat zien dat AFAS deze verwerkingen uitvoert buiten de contractueel vastgelegde rolverdeling. Indien het risico zich verwezenlijkt, zijn de gevolgen voor de rechten en vrijheden van betrokkenen potentieel ernstig, omdat de onduidelijke rolverdeling en gebrekkige transparantie ertoe leiden dat betrokkenen niet hun fundamentele rechten uit kunnen oefenen. Het niet kunnen uitoefenen hiervan heeft dus een grote impact. Om die reden wordt dit risico gekwalificeerd als een hoog risico.

Algemene Risico's

C.1.7 Verlies van controle door zelfbouw workflows

AFAS biedt de verwerkingsverantwoordelijke de mogelijkheid om zelf workflows te ontwerpen en configureren. Binnen deze workflows kan de instelling eigen keuzes maken over welke rollen, gebruikers en afdelingen toegang krijgen tot welke gegevens en welke stappen zij mogen uitvoeren. In de praktijk kan dit ertoe leiden dat meer medewerkers toegang krijgen tot (gevoelige) personeelsinformatie dan noodzakelijk is voor hun werkzaamheden en/of dat er meer persoonsgegevens verwerkt worden dan nodig.

Omdat de inrichting van workflows door de instelling zelf gebeurt, bestaat het risico dat privacy-by-design en dataminimalisatie niet consequent worden toegepast. Workflows kunnen zo worden opgezet dat grote groepen gebruikers inzage of bewerkingsrechten krijgen in dossiers, documenten of signalen zonder dat dit strikt noodzakelijk is voor hun rol. Dit vergroot de kans op ongewenste verspreiding of oneigenlijk gebruik van persoonsgegevens binnen de organisatie.

De kans dat het risico zich voordoet is waarschijnlijker dan niet doordat er veel opties en mogelijkheden zijn om verkeerde keuzes te maken tijdens het inrichten van de vele workflows, hierbij is ook het niveau van volwassenheid van instellingen meegenomen wat nogal uiteenloopt. Als het risico zich voordoet heeft dit ernstige gevolgen voor de rechten en vrijheden van betrokkene aangezien er een verlies van controle is. Om die reden wordt dit risico gekwalificeerd als een hoog risico.

C.1.8 Verlies van controle en vertrouwelijkheid door overige vrije velden

Het is mogelijk om door middel van vrij in te vullen velden opmerkingen toe te voegen aan dossiers van betrokkenen. Deze vrije velden dienen geen bepaald doel en instellingen zijn dus vrij hier zelf invulling aan te geven. Bij het aanmaken van vrije velden kan het functioneel beheer aanvinken of deze gevoelige of bijzondere persoonsgegevens (mogen) bevatten.[101]

[101] AFAS Help Center Nederland, *Vrije velden kenmerken als Privacygegevens*, geraadpleegd op 11 december 2025 via https://help.afas.nl/help/NL/SE/Crm_Config_PerOrg_Relat_AVG.htm#o93144.

Het bestaan van deze vrije velden leidt tot het risico dat gebruikers hier persoonsgegevens in registreren waarvoor instellingen geen verwerkingsgrondslag en uitzonderingsgrond voor bijzondere persoonsgegevens hebben. Dit kan leiden tot een verlies van controle over de gegevens, doordat de gegevens bijvoorbeeld te lang bewaard worden, en tot een verlies van vertrouwelijkheid.

De kans dat het risico zich voordoet is waarschijnlijker dan niet, omdat er verder geen sturing is vanuit de instellingen om bovenstaande te voorkomen én afhankelijk is van menselijke feilbaarheid. Als het risico zich voordoet heeft dit ernstige gevolgen voor de rechten en vrijheden van betrokkene aangezien er mogelijk bijzondere persoonsgegevens worden verwerkt. Om die reden wordt dit risico gekwalificeerd als een hoog risico.

C.1.9 Verlies van controle en vertrouwelijkheid door handmatige invoer

Gebruikers kunnen handmatig persoonsgegevens invoeren en bewerken in Profit. Deze handmatige verwerking vindt plaats via directe invoer in het systeem, waarbij nieuwe persoonsgegevens kunnen worden toegevoegd en bestaande gegevens kunnen worden gewijzigd of verrijkt. Hierdoor lopen betrokkenen het risico dat hun persoonsgegevens onjuist worden verwerkt, wat er bijvoorbeeld in kan resulteren dat een beoordeling of salarisgegevens bij de verkeerde medewerker worden ingevoerd.

Waar validatie mogelijk is wordt dat door AFAS toegepast op open velden. Bij de invoer van bijvoorbeeld e-mailadressen, telefoonnummers, KvK-nummers en persoonlijk identificeerbare nummers (bv. BSN) controleert het systeem automatisch of de invoer bestaat uit legitieme waarden die aan de criteria voldoen.

De kans dat dit risico zich realiseert is waarschijnlijker dan niet, omdat het invoeren afhankelijk is van menselijke feilbaarheid. Als het risico zicht voordoet heeft dit enige negatieve gevolgen voor de rechten en vrijheden van betrokken aangezien de gevolgen direct merkbaar in het leven van betrokkenen zijn. Een voorbeeld hiervan is de financiële benadeling door een incorrecte salarisverwerking. Om die reden wordt dit risico gekwalificeerd als een hoog risico.

C.1.10 Verlies van controle en vertrouwelijkheid door niet automatisch te configureren bewaartermijnen

AFAS biedt geen functionaliteit aan die het mogelijk maakt om persoonsgegevens na het verstrijken van de bewaartermijn geautomatiseerd te verwijderen of om een melding te krijgen na het verstrijken van een bewaartermijn. Hierdoor bestaat het risico dat persoonsgegevens langer bewaard blijven dan noodzakelijk, in strijd met de beginselen van minimale gegevensverwerking en opslagbeperking.

De kans dat dit risico zich realiseert is waarschijnlijker dan niet, omdat momenteel de bewaartermijnen niet worden afgedwongen door het systeem. Als het risico zich voordoet heeft dit ernstige gevolgen voor de rechten en vrijheden van betrokkene aangezien dit alle persoonsgegevens Profit raakt, waaronder de bijzondere persoonsgegevens. Om die reden wordt dit risico gekwalificeerd als een hoog risico.

C.1.11 Verlies van controle en vertrouwelijkheid door niet automatisch te configureren bewaartermijnen binnen logging

AFAS genereert en bewaart verschillende vormen van logbestanden waaronder mutatielogging, read access logging, logging op autorisaties, etc. Zie A.6.6 Monitoren door AFAS & A.6.7 Applicatielogging voor een uitgebreide toelichting. De meeste logbestanden moeten handmatig door de instelling worden verwijderd na het verstrijken van de gestelde bewaartermijnen. Daarnaast bestaan er loggingslagen waarin activiteiten rond het raadplegen van logs zelf worden vastgelegd (zogeheten *logging van logging*). Deze specifieke gegevens kunnen technisch niet of slechts zeer beperkt worden verwijderd.

Door de afhankelijkheid van handmatige acties en het ontbreken van automatische verwijdermogelijkheden is de kans reëel dat niet alle logbestanden tijdig of volledig worden verwijderd. Hierdoor bestaat het risico dat persoonsgegevens langer bewaard blijven dan noodzakelijk, in strijd met de beginselen van minimale gegevensverwerking en opslagbeperking. Hoewel de gevoeligheid van de gelogde persoonsgegevens relatief laag is, mogen ook dergelijke gegevens niet buiten de toegestane bewaartermijn verwerkt worden.

De kans dat het risico zich voordoet is waarschijnlijker dan niet. Als het risico zich voordoet heeft dit ernstige gevolgen voor de rechten en vrijheden van betrokkene aangezien er een verlies van controle en vertrouwelijkheid is. Om die reden wordt dit risico gekwalificeerd als een hoog risico.

C.1.12 Verlies van controle door verdere verwerking van persoonsgegevens via algemene statistieken uit klantomgeving

AFAS heeft de mogelijkheid om op aanvraag algemene gebruiksstatistieken uit klantomgevingen te genereren. Deze rapportages worden niet gebaseerd op vooraf gedefinieerde, gestandaardiseerde rapporten, maar worden op ad hoc basis aangevraagd via een ticketsysteem. Een Software Engineer beoordeelt per aanvraag of het gevraagde rapport wordt opgesteld en verstrekt. AFAS kan niet uitsluiten dat in deze rapportages (direct of indirect) persoonsgegevens terechtkomen. AFAS stelt dat deze medewerker gekwalificeerd is om deze beoordeling van datakwalificatie te doen, maar de feitelijke onderbouwing hiervan blijft onbekend.

De Functionaris Gegevensbescherming en Privacy Officer van AFAS hebben inzage in het aanvraagsysteem en kunnen meekijken met aanvragen en zo nodig interveniëren, maar hebben geen formele beslisrol in het proces. Er zijn geen vastgelegde procedurele afspraken over hoe om te gaan met situaties waarin persoonsgegevens in deze rapportages voorkomen, noch zijn specifieke bewaartermijnen afgesproken met de ontvanger van de rapportage of voor de opslag in het aanvraagsysteem zelf. Dit betekent dat rapportages die mogelijk persoonsgegevens bevatten voor onbepaalde tijd kunnen worden bewaard.

Hierdoor ontstaat het risico dat de leverancier een verdere verwerking uitvoert die niet expliciet is omschreven of beperkt in de SLA en waarvan de verwerkingsverantwoordelijke (en de betrokkenen) niet of onvoldoende zijn geïnformeerd. De doeleinden, grondslag en bewaartermijnen van deze verdere verwerking zijn niet duidelijk afgebakend en er is geen zekerheid dat deze verdere verwerking verenigbaar is met de oorspronkelijke doeleinden.

De kans dat het risico zich voordoet is redelijk aangezien er een mogelijkheid is voor medewerkers om deze rapportage is om aan te vragen. Als het risico zich voordoet heeft dit ernstige gevolgen voor de rechten en vrijheden van betrokkene aangezien er een verlies van controle is door een verdere verwerking waar beperkte maatregelen zijn getroffen om deze rapportages te kaderen. Om die reden wordt dit risico gekwalificeerd als een hoog risico.

C.1.13 Verlies van controle en vertrouwelijkheid door ongeoorloofde toegang in derde landen

In de SLA is vastgelegd dat de verwerking van persoonsgegevens door AFAS en de door haar ingeschakelde subverwerkers uitsluitend plaatsvindt binnen de EER.[102] Het technische onderzoek en de cookieverklaring identificeren echter subverwerkers met 'moeders' in de Verenigde Staten. Dit roept de vraag op of er sprake is van doorgifte buiten de EER.

Hoewel de SLA contractueel bepaalt dat data binnen de EER blijft, kan SURF deze garantie bij het ontbreken van (volledige) subverwerkersovereenkomsten met alle betrokken partijen niet onafhankelijk verifiëren. Dit betekent dat er mogelijk sprake is van doorgifte van persoonsgegevens naar een derde land in de zin van hoofdstuk V AVG, waarvoor passende waarborgen vereist zijn.

Daarnaast zijn bepaalde partijen (zoals Vimeo en LinkedIn) wel vermeld in de cookieverklaring, maar ontbreken zij in de SLA én zijn deze partijen niet naar voren gekomen uit het technisch onderzoek. Ten aanzien van deze partijen geldt eveneens dat deze ondernemingen (althans hun moedermaatschappijen) in de Verenigde Staten zijn gevestigd. Dit betekent dat ook hier mogelijk sprake is van doorgifte van persoonsgegevens naar een derde land in de zin van hoofdstuk V AVG, waarvoor passende waarborgen vereist zijn.

Aangezien SURF deze garantie niet kan verifiëren door het ontbreken van (volledige) subvewerkersovereenkomsten, is de kans op verlies van controle waarschijnlijker dan niet. De gevolgen voor de rechten en vrijheden van betrokkenen kunnen, indien dit gebeurt, ernstige schade inhouden, afhankelijk van het soort persoonsgegevens dat wordt bekendgemaakt en de partij waaraan deze worden bekendgemaakt. Daarom is dit een hoog risico.

Cookies

C.1.14 Verlies van controle door incorrecte cookieverklaring

De cookieverklaring voor klant.afas.nl (help.afas.nl) staat onder beheer van Cookiebot en is daardoor niet volledig onder directe controle van AFAS. In het huidige cookiestatement zijn bepaalde cookies als “noodzakelijk” aangemerkt, terwijl deze niet strikt noodzakelijk zijn voor de technische werking of beveiliging van de dienst.

[102] AFAS Service License Agreement April 2026, paragraaf 5.7, geraadpleegd op 9 juni 2026 via https://klant.afas.nl/sla-av.

Daarnaast zijn er cookies waarvoor nog geen beschrijving beschikbaar is. De leverancier kan niet aangeven wat het doel of de inhoud van deze cookies is. Gebruikers krijgen hierdoor een onvolledig en deels onjuist beeld van welke cookies worden geplaatst, met welk doel en op welke grondslag. Door deze onduidelijkheid bestaat het risico dat niet-noodzakelijke cookies worden geplaatst zonder geldige en/of geïnformeerde toestemming of dat toestemming wordt gevraagd op basis van onvolledige informatie.

De kans dat het risico zich voordoet is waarschijnlijker dan niet. Als het risico zich voordoet heeft dit ernstige gevolgen voor de rechten en vrijheden van betrokkene aangezien het gebrek aan transparantie een schending vormt van een beginsel van de AVG, met name wanneer trackingcookies of soortgelijke technologieën worden gebruikt. Om die reden wordt dit risico gekwalificeerd als een hoog risico.

Risico's als gevolg van het aanbieden van een mobiele app via de app-winkels van Google en Apple

Op het moment van publicatie heeft SURF nog geen conclusie getrokken over de impact van de volgende twee risico's, die verband houden met de gegevensverwerking door Google en Apple bij het gebruik van mobiele apps. De overwegingen en maatregelen die SURF heeft geïdentificeerd, staan hieronder beschreven. SURF doet echter verder onderzoek naar de impact van deze risico's en het effect van beschikbare maatregelen op de risico's. Hierover zal op een later tijdstip een publicatie verschijnen. In de tussentijd kunnen instellingen maatregelen nemen op basis van hun eigen beoordelingen.

C.1.15 Verlies van controle over verwerkte persoonsgegevens door installatie van mobiele app via app-winkel van derden

Het risico dat gepaard gaat met het aanbieden van de Pocket-app via de Apple App Store en Google Play Store ligt in de automatische koppeling die tot stand komt tussen het gebruik van de app en het persoonlijke Apple- of Google-account van de gebruiker. Deze koppeling stelt deze platformaanbieders in staat om inzicht te krijgen in de installatie van de app, wat kan leiden tot indirecte identificatie van de relatie met AFAS. Aangezien deze verwerking niet strikt noodzakelijk is voor de werking van de app, is dit in strijd met het Privacy by Default-principe en leidt dit tot verlies van controle over persoonsgegevens.

De kans dat dit risico zich voordoet, is waarschijnlijker dan niet, aangezien er sprake is van een verlies van controle zodra de app via een app-store wordt gedownload. Bijgevolg stromen persoonsgegevens over werknemers onvermijdelijk naar derden zoals Apple en Google, wat de vertrouwelijkheid in gevaar kan brengen en het risico voor de rechten en vrijheden van werknemers vergroot. Dit leidt tot de mogelijke blootstelling van persoonsgegevens zonder dat dit strikt noodzakelijk is en tot de betrokkenheid van grote platformaanbieders.

Er moeten alternatieven met minder inbreuken op de privacy worden overwogen om de gegevens van gebruikers beter te beschermen en naleving van de vereisten inzake gegevensminimalisatie te waarborgen.

C.1.16 Verlies van controle door de verwerking van pushmeldingen door Google en Apple

Dit is een risico dat in het algemeen geldt voor alle applicaties die gebruikmaken van de push-infrastructuur van Google of Apple.

De mobiele Pocket-app verstuurt pushmeldingen. De pushmeldingen leiden tot zowel de overdracht van metadata als inhoud naar Google en Apple. De metadata betreft gegevens zoals apparaat-ID's, IP-adressen en mogelijk het Google- of Apple-account van de student. De inhoud betreft de berichten, indien die inhoud niet versleuteld wordt verzonden, zoals noodzakelijkerwijs het geval is bij het onderdeel "meldingsberichten" van de pushmeldingen. De inhoud van deze berichten is zichtbaar voor en wordt verwerkt door Google en Apple. Aangezien het niet noodzakelijk is om persoonsgegevens in meldingen op te nemen, vormt dit een inbreuk op het subsidiariteitsbeginsel. Onderwijsinstellingen bepalen zelf de inhoud van de berichten en kunnen privacyvriendelijke keuzes maken door geen persoonsgegevens op te nemen.

Ongeacht de inhoud van de berichten betekent het gebruik van meldingsberichten dat de inhoud van de berichten systematisch door Google wordt verwerkt. Het is mogelijk om deze verwerking te beperken door gebruik te maken van een versleutelde datapayload, hetzij bovenop het meldingsbericht, hetzij afzonderlijk. Als een student beschikt over Unified Push, een alternatieve push-infrastructuur voor Android, kan de app hier ook gebruik van maken en terugvallen op Google als dit niet beschikbaar is. Aangezien beide mitigerende maatregelen ontbreken, voldoet het gebruik van meldingen niet aan de subsidiariteitsvereiste.

De kans dat er sprake is van verlies van controle is waarschijnlijker dan niet, aangezien meldingen een standaardonderdeel zijn van de Pocket-app en het controleverlies optreedt zodra Google of Apple de melding ontvangt.

Part D Beschrijving voorgenomen maatregelen

D.1 Beperkende maatregelen

Verlies van controle door AFAS als verwerkingsverantwoordelijke						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	**Huidig risico**
C.1.1	AFAS voert (verdere) verwerkingen uit als verwerkingsverantwoordelijke zonder contractuele afspraken.	Verlies van controle.	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	**Rest risico**
	Herziene verwerkersovereenkomst van AFAS beoordelen en ondertekenen.	Update de verwerkersovereenkomst tussen AFAS en instellingen o.a. met: alle categorieën persoonsgegevens, inclusief diagnostische loggegevens indien van toepassing, die AFAS en subverwerkers namens instellingen verwerken; legitieme doeleinden waarvoor AFAS en subverwerkers persoonsgegevens mogen verwerken en onder welke voorwaarden; doeleinden waarvoor AFAS en subverwerkers geen persoonsgegevens mogen verwerken.	**Heel klein**	**Ernstig**	**Laag**	

Verlies van controle en vertrouwelijkheid door onvolledige verwerkersovereenkomsten						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	**Huidig risico**
C.1.2	Er is geen volledige verwerkersovereenkomst tussen instellingen en AFAS, doordat AFAS geen losse verwerkersovereenkomst hanteert en wat er in dit kader in de SLA is opgenomen niet compleet is.	Verlies van controle.	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	**Rest risico**
	Herziene verwerkersovereenkomst van AFAS beoordelen en ondertekenen.	Update de verwerkersovereenkomst tussen AFAS en instellingen o.a. met: alle categorieën persoonsgegevens, inclusief diagnostische loggegevens indien van toepassing, die AFAS en subverwerkers namens instellingen verwerken; legitieme doeleinden waarvoor AFAS en subverwerkers persoonsgegevens mogen verwerken en onder welke voorwaarden; doeleinden waarvoor AFAS en subverwerkers geen persoonsgegevens mogen verwerken.	**Heel klein**	**Ernstig**	**Laag**	

Verlies van controle door het ontbreken van subverwerkersovereenkomsten						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	**Huidig risico**
C.1.3	Contracten met subverwerkers ontbreken of voldoen niet aan de eisen.	Verlies van controle.	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	**Rest risico**
	Beoordeel de in de DPIA geïdentificeerde subverwerkers.[103] Dien bij bezwaar conform de SLA een verzoek in bij de (directie van) AFAS.	Ten aanzien van AFAS Online en de supportpagina's klant.afas.nl en help.afas.nl, die in de praktijk hoofdzakelijk door functioneel beheerders worden bezocht: Verwerkersovereenkomsten met LinkedIn, Google en Vimeo afsluiten waarin de afspraken in de verwerkersovereenkomst met instellingen worden doorgezet, met een duidelijke instructie over de te verwerken persoonsgegevens en een lijst met subverwerkers.	**Heel klein**	**Ernstig**	**Laag**	
		Ten aanzien van AFAS Online en de supportpagina's klant.afas.nl en help.afas.nl, die in de praktijk hoofdzakelijk door functioneel beheerders worden bezocht:				

[103] Bij het aangaan van de overeenkomst en gedurende de overeenkomst waren deze subverwerkers onbekend bij de instellingen. Hierdoor hebben zij de partijen destijds niet kunnen beoordelen en was het onmogelijk om gebruik te maken van het contractuele bezwaarrecht.

		Specificatie van de verwerkingen opnemen in de subverwerkersovereenkomsten met Cookiebot, Cloudflare en Hunt & Hackett.				
		Ten aanzien van AFAS Online: Verwerkersovereenkomsten met Leaseweb afsluiten waarin de afspraken in de verwerkersovereenkomst met instellingen worden doorgezet, met een duidelijke instructie over de te verwerken persoonsgegevens en een lijst met subverwerkers.				

Niet uit kunnen oefenen van AVG-rechten door het uitblijven van een reactie op inzageverzoeken						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	**Huidig risico**
C.1.4C.1.3	Geen volledige reactie op inzageverzoek door ontbreken verwerkingen die onzichtbaar zijn voor instellingen.	Niet mogelijk om AVG- rechten uit te oefenen voor betrokkenen.	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	**Rest risico**
	-	Volledige inzage in verwerkingen verschaffen bij een inzageverzoek, ofwel door beheerders de mogelijkheid te bieden zelf inzage te krijgen of door een duidelijke procedure te implementeren om inzageverzoeken te verwerken.	**Heel klein**	**Ernstig**	**Laag**	

Niet mogelijk om AVG-rechten uit te oefenen en verlies van controle door gebrek aan transparantie subverwerkers						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	**Huidig risico**
C.1.5C.1.3	Contracten met subverwerkers ontbreken of voldoen niet aan de eisen.	Niet mogelijk om AVG- rechten volledig uit te oefenen voor betrokkenen en verlies van controle instellingen.	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	**Rest risico**
	Periodieke controle op overzicht subverwerkers.	Afhankelijk van de subverwerker: SLA (verwerkersovereenkomst), privacyverklaring en/of cookieverklaring updaten met relevante subverwerkers.	**Heel klein**	**Ernstig**	**Laag**	
		Hoofd- en verwerkersovereenkomsten met alle subverwerkers afsluiten waarin de afspraken in de verwerkersovereenkomst met instellingen worden doorgezet, met een duidelijke instructie over de te verwerken persoonsgegevens en een lijst met subverwerkers.				

Niet mogelijk om AVG-rechten uit te oefenen door onduidelijke rolverdeling						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	**Huidig risico**
C.1.6C.1.3	De onduidelijke rolverdeling en het ontbreken van transparantie (zoals nader beschreven in risico C.1.1.) hebben tot gevolg dat betrokkenen hun rechten niet (effectief) kunnen uitoefenen.	Niet mogelijk om AVG- rechten volledig uit te oefenen voor betrokkenen en verlies van controle instellingen.	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	**Rest risico**
	Herziene verwerkersovereenkomst van AFAS beoordelen en ondertekenen.	Update verwerkersovereenkomst tussen AFAS en instellingen o.a. met: alle categorieën persoonsgegevens, inclusief diagnostische gegevens indien van toepassing, die AFAS en subverwerkers namens instellingen verwerken; legitieme doeleinden waarvoor AFAS en subverwerkers persoonsgegevens mogen verwerken en onder welke voorwaarden; doeleinden waarvoor AFAS en subverwerkers geen persoonsgegevens mogen verwerken.	**Heel klein**	**Ernstig**	**Laag**	

Algemene risico's

Verlies van controle door zelfbouw workflows						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	
C.1.7C.1.3	Zelf workflows ontwerpen en configureren.	Verlies van controle doordat meer medewerkers krijgen toegang tot (gevoelige) personeelsinformatie dan noodzakelijk is voor hun werkzaamheden en/of doordat er meer persoonsgegevens verwerkt worden dan nodig.	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	**Huidig risico**
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	
	Zorg ervoor dat HR-medewerkers goed zijn geïnstrueerd en opgeleid in de procedures van de instellingen voor het zorgvuldig registreren van persoonsgegevens.	Duidelijke strategie implementeren om klanten en gebruikers (in de context van de verwerking) te waarschuwen om de risico's van de workflows helder te maken.	**Heel klein**	**Ernstig**	**Laag**	**Rest risico**
	Controleer periodiek door middel van steekproeven de workflows op doelmatigheid, proportionaliteit, data minimalisatie, toegang en bewaartermijnen.					

Verlies van controle en vertrouwelijkheid door overige vrije tekstvelden						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	**Huidig risico**
C.1.8C.1.3	Invullen vrije tekstvelden.	Verlies van controle en vertrouwelijkheid.	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	**Rest risico**
	Gebruik alleen open tekstvelden met een duidelijk doel.	Duidelijke strategie implementeren om klanten en gebruikers (in de context van de verwerking) te waarschuwen geen (bijzondere) persoonsgegevens in open velden op te nemen en om de risico's van de vrije tekstvelden helder te maken.	**Heel klein**	**Ernstig**	**Laag**	
	Bij het aanmaken van vrije tekstvelden moet het functioneel beheer aanvinken of deze gevoelige of bijzondere persoonsgegevens (mogen) bevatten.					
	Zorg ervoor dat medewerkers goed zijn geïnstrueerd en opgeleid in de procedures van de instellingen voor het zorgvuldig registreren van persoonsgegevens.					
	Monitoring van de effectiviteit van dit beleid door middel van steekproeven.					

Verlies van vertrouwelijkheid en controle door handmatige invoer						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	**Huidig risico**
C.1.9C.1.3	Handmatige invoer van verkeerde informatie.	Verlies van vertrouwelijkheid en controle.	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	**Rest risico**
	Zorg ervoor dat HR-medewerkers goed worden geïnstrueerd en opgeleid in de procedures van de instellingen voor het zorgvuldig registreren van persoonsgegevens.	-	**Heel klein**	**Ernstig**	**Laag**	
	Automatiseren invoer waar mogelijk.					

Verlies van controle door niet automatisch te configuren bewaartermijnen						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	**Huidig risico**
C.1.10C.1.3	Geen automatische bewaartermijnen.	Verlies van controle.	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	**Rest risico**
	Vaststellen en beheren bewaartermijnen persoonsgegevens in AFAS.	Instellingen faciliteren bij het handhaven van hun bewaartermijnen door de mogelijkheden voor de technische configuratie en het beheer van bewaartermijnen per groep persoonsgegevens in AFAS te verbeteren.	**Heel klein**	**Ernstig**	**Laag**	
	Naleving bewaartermijnen vastleggen in processen.					

Verlies van vertrouwelijkheid en controle door niet automatisch te configureren bewaartermijnen binnen logging						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	**Huidig risico**
C.1.11C.1.3	Geen automatische bewaartermijnen te configureren binnen logging.	Verlies van controle	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	**Rest risico**
	Vaststellen en beheren bewaartermijnen persoonsgegevens in AFAS.	AFAS als verwerker: Automatische bewaartermijnen op logging en monitoring mogelijk maken onder verantwoordelijkheid instellingen.	**Heel klein**	**Ernstig**	**Laag**	
	Naleving bewaartermijnen vastleggen in processen.	AFAS als verwerkingsverantwoordelijke: Vastellen, motiveren en beheren bewaartermijnen op logging en monitoring onder verantwoordelijkheid AFAS.				
		AFAS als verwerkingsverantwoordelijke: Automatische bewaartermijnen inregelen op logging en monitoring onder verantwoordelijkheid AFAS.				

Verlies van controle door verdere verwerking van persoonsgegevens via algemene statistieken uit klantomgeving						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	**Huidig risico**
C.1.12C.1.3	Verdere verwerking van persoonsgegevens via algemene statistieken uit klantomgeving.	Verlies van controle.	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	**Rest risico**
		Richt het proces zo in dat er geen persoonsgegevens in de algemene statistieken terechtkomen.	**Heel klein**	**Ernstig**	**Laag**	
		Evalueer en verbeter het proces rond de uitvraag van deze rapportages door medewerkers van AFAS. Stel een procedure vast voor de omgang met persoonsgegevens en stel bewaartermijnen vast.				
		Houd toezicht op dit proces voor in het geval dat persoonsgegevens verwerkt worden.				

Verlies van controle en vertrouwelijkheid door ongeoorloofde toegang in derde landen[104]						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	**Huidig risico**
C.1.13C.1.3	Doorgifte van persoonsgegevens naar partijen die gevestigd zijn in de VS of daar een moederbedrijf hebben.	Verlies van controle en vertrouwelijkheid.	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	**Rest risico**
	-	Contractueel uitsluiten van doorgifte buiten de EER in de (sub)verwerkersovereenkomsten.	**Heel klein**	**Ernstig**	**Laag**	

Verlies van controle door incorrecte cookieverklaring						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	**Huidig risico**
C.1.14C.1.3	De onduidelijke cookieverklaring voor klant.afas.nl (help.afas.nl) staat onder beheer van Cookiebot en is daardoor niet (volledig) onder directe controle van AFAS.	Verlies van controle.	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	**Rest risico**
	-	Evalueer de procedure rondom de cookieverklaring en de optie om deze zelfstandig te beheren.	**Heel klein**	**Ernstig**	**Laag**	

104 Hoewel er juridisch gezien geen aanvullende maatregelen van de instelling nodig zijn zolang het Data Privacy Framework van kracht is, is het raadzaam om de geopolitieke situatie periodiek te evalueren – met name wat betreft de waarschijnlijkheid dat risico's zich voordoen – om te bepalen of een aanpassing van de risicobeoordeling nodig is.

Mobiele app risico's

Verlies van controle over persoonsgegevens door installatie van applicatie via app stores						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	**Huidig risico**
C.1.15 C.1.3	Het moeten downloaden van Pocket app via de Google en/of Apple mobiele app winkels	Verlies van controle.	**Waarschijnlijker dan niet**	**Ernstig**	**n.t.b.**	
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	**Rest risico**
	Maak toegang via de mobiele webbrowser mogelijk.	Maak de app beschikbaar via side load.	**Heel klein**	**Minimaal**	**Laag**	
	Voer proportionaliteits- en subsidiariteitsbeoordeling uit op beschikbaar stellen mobiele app via app stores of als 'side-load' en implementeer resultaten.	Maak toegang via de mobiele webbrowser mogelijk.				

Verlies van controle door verwerken van push notificaties door Google en Apple						
Referentie	**Oorzaak**	**Gevolg**	**Kans**	**Ernst**	**Risico score**	**Huidig risico**
C.1.16 C.1.3	Versturen van push notificaties via Google en Apple.	Verlies van controle.	**Waarschijnlijker dan niet**	**n.t.b**	**n.t.b.**	
	Maatregel instelling	**Maatregel vendor**	**Kans**	**Ernst**	**Risico score**	**Rest risico**
	Neem geen persoonsgegevens op in de inhoud van de notificaties.	Optioneel: implementeer Unified push voor Androidgebruikers.	**n.t.b**	**n.t.b**	**n.t.b**	
	Voer proportionaliteits- en subsidiariteitsbeoordeling uit op versturen pushnotificatie via Google en Apple, of via Unified Push en implementeer resultaten.					

Bijlage 1 Technisch onderzoek

Use case / scenario's

Als onderdeel van het onderzoek zijn er scenario's/use cases uitgevoerd in het systeem. Deze scenario's dienen als basis voor verschillende elementen van het onderzoek:

- Data onderscheppen
- Inzage verzoek(en)
- Privacy by Design
- Privacy by Default
- Algemene kennis over gebruik van systeem

Scenario's / Use cases

HR Manager

- Login traject doorlopen
- Nieuwe werknemer (medewerker 1) aanmaken
- Het formulier met persoonlijke gegevens invullen (inclusief naam, adres, contactgegevens, contactpersonen in noodgevallen)
- Vereiste documenten uploaden (kopieën paspoort/ID-kaart, werkvergunningen, CV, belastingformulier)
- Een nieuwe gebruikersaccount (medewerker 1) aanmaken activeren
- Rapport exporteren naar PDF
- Rapport exporteren naar Excel
- Klant.afas.nl zonder cookie consent
- Klant.afas.nl met cookie consent
- Dient een supportverzoek in bij AFAS.

Werknemer 1

- Login traject doorlopen
- Toegang tot persoonlijke gegevens record
- Contactpersoon in noodgevallen toevoegen
- Loonstrook downloaden
- Verlofdagen controleren
- Gewenste taal wijzigen
- Mobiliteitsformulier invullen

Inzageverzoek (Data Subject Access Request)

Inzageverzoek

Beste Surf (AFAS),

Ik ben medewerker bij uw bedrijf en ik heb een account op AFAS acceptatieomgeving van uw bedrijf (T35602AA).

Bij deze wil ik, conform artikel 15 van de AVG, een inzage verzoek indienen voor mijn persoonsgegevens. Dit inzageverzoek betreft alle gegevens die naar mij herleidbaar zijn, inclusief, maar niet beperkt tot, de gegevens opgeslagen in AFAS, logbestanden, auditlogs,

gebruiksinteracties en technische foutrapportages. Dit alles van zowel de Profit applicatie, AFAS Pocket app en de Insite omgeving. Aanvullend daarop verzoek ik ook:

- *de verwerkingsdoeleinden;*
- *de betrokken categorieën van persoonsgegevens;*
- *de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen*
- *worden verstrekt, met name ontvangers in derde landen of internationale organisaties;*
- *indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen*
- *worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;*
- *welke mogelijkheden er zijn om mijn persoonsgegevens te rectificeren of te wissen, om*
- *bezwaar te maken tegen de verwerking en welke procedure daar dan voor gevolgd moet*
- *worden;*
- *van gegevens die ik niet zelf heb verstrekt, alle beschikbare informatie over de bron van die*
- *gegevens;*
- *het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.*

NB: ik sta bij u geregistreerd onder onderstaand e-mailadres. U kunt dat adres gebruiken om mijn identiteit vast te stellen.

Veel dank en met vriendelijke groet,

Renate de Vries

Account e-mail adres: #########@surf.nl
Relevante parameters
Personeelscode: 000##
IP adres: 62.250. ##.###
Periode: 6 - 11 - 2025 tot 19 - 11 - 2025

U kunt mij bereiken op: #########@surf.nl

Respons inzageverzoek

We hebben geen reactie op de inzageverzoeken mogen ontvangen. SURF heeft de mogelijkheid om de data (content data, applicatielogs en accountdata) beschikbaar voor de verwerkingsverantwoordelijke handmatig te exporteren, maar op het gebied van persoonsgegevens verwerkt in verwerkingen onzichtbaar voor verwerkingsverantwoordelijke zijn de inzageverzoeken tot op heden onvolledig.

Onderschepte data

Tijdens het onderzoek is de data tussen de gebruiker en de dienstverlener onderschept. Hier volgen de relevante resultaten.

End points

hostname	land	ip	ip registrant	
35602.insitetest.afas.online	NL	185.46.182.93	JS4840-MNT, AFAS Software BV	AFAS Online, testomgeving
fonts.googleapis.com	US	142.251.36.42	Google LLC	Gekoppeld aan Googlemaps
fonts.gstatic.com	US	142.251.36.3	Google LLC	Gekoppeld aan Googlemaps
hcaptcha.com	US	104.19.229.21	Cloudflare, Inc.	Leverancier van de captcha die gebruikt wordt bij activeren van account.
idp.afasonline.com	NL	185.46.182.13	JS4840-MNT, AFAS Software BV	AFAS Online
login.afasonline.com	NL	185.46.182.11	JS4840-MNT, AFAS Software BV	AFAS Online
maps.googleapis.com	US	216.58.214.10	Google LLC	Google maps integratie
maps.googleapis.com	US	142.251.39.138	Google LLC	Google maps integratie
maps.googleapis.com	US	142.250.179.202	Google LLC	Google maps integratie
maps.googleapis.com	US	142.251.36.10	Google LLC	Google maps integratie
maps.gstatic.com	US	172.217.168.195	Google LLC	Google maps integratie
maps.gstatic.com	US	142.250.179.163	Google LLC	Google maps integratie
portal.afasonline.com	NL	185.46.182.121	JS4840-MNT, AFAS Software BV	AFAS Online
region1.google-analytics.com	US	216.239.32.36	Google LLC	Gekoppeld aan afasstatus.nl
statuspal.eu	US	104.26.14.146	Cloudflare, Inc.	Gekoppeld aan afasstatus.nl
sts.afasonline.com	NL	185.46.182.12	JS4840-MNT, AFAS Software BV	AFAS Online
www.afasstatus.nl	FR	162.19.237.189	OVH GmbH, OVH-MNT	Gekoppeld aan afasstatus.nl

www.googletagmanager.com	US	216.58.208.104	Google LLC	Gekoppeld aan afasstatus.nl

Tabel D-1, alle endpoints die gezien zijn tijdens uitvoeren scenarios in de Insite testomgeving.

Cookies

Host	Cookie name	Expiry	Beschrijving
35602.insitetest.afas.online	__Host-.auth	Session	Vereist voor de beveiliging van de website.
	__Host-.cache	Session	Vereist voor de beveiliging van de website.
	__Host-.contextmenu	Session	Noodzakelijk voor de algemene functionaliteit van de website.
	__Host-.lastactivetabs	Session	Gebruikt in samenhang met gedrag van de bezoeker, door de website - De cookie registreert het gedrag en de navigatie van de bezoeker over meerdere websites en zorgt ervoor dat er geen volgfouten optreden wanneer de bezoeker meerdere browsertabs heeft geopend.
	__Host-.nonce.$id	Session	
	__Host-.secureclient	Session	Vereist voor de beveiliging van de website.
	__Host-.securesession	Session	Vereist voor de beveiliging van de website.
	__Host-.storedviews	Session	Bevat gegevens over de laatste producten die door de bezoeker worden bekeken. Gebruikt voor interne statistieken door de exploitant van de website.
hcaptcha.com	__cf_bm	Session	Deze cookie wordt gebruikt om onderscheid te maken tussen mensen en bots. Dit is gunstig voor de website om juiste rapporten over het gebruik van de website te maken.
idp.afasonline.com	__Host-.AFAS.IdP.Nonce-$id	Session	
sts.afasonline.com	__Host-.AFAS.Csrf	Session	In afwachting

Tabel D-2, cookies AFAS Online.

Host	Cookie name	Expiry	Beschrijving
klant.afas.nl	__Host-.anon	Session	Vereist voor de beveiliging van de website.
	__Host-.auth	Session	Vereist voor de beveiliging van de website.

	__Host-.cache	Session	Vereist voor de beveiliging van de website.
	__Host-.contextmenu	Session	Noodzakelijk voor de algemene functionaliteit van de website.
	__Host-.secureclient	Session	Vereist voor de beveiliging van de website.
	__Host-.securesession	Session	Vereist voor de beveiliging van de website.

Tabel D-3, cookies klant.afas.nl geen consent.

Host	Cookie name	Domain	Expiry	Beschrijving
bat.bing.com	MUID		Sessie	Veel gebruikt door Microsoft als een unieke gebruikers-ID. De cookie maakt het volgen van gebruikers mogelijk door de ID in veel Microsoft-domeinen te synchroniseren.
consent.A.7.com	ak_bmsc	.cookiebot.com	2 uur	Slaat de cookiestatus van de gebruiker op voor het huidige domein
googleads.g.doubleclick.net	IDE		Sessie	Gebruikt door Google DoubleClick om de acties van de websitegebruiker te registreren en te rapporteren na het bekijken of klikken op een van de advertenties van de adverteerder met het doel de effectiviteit van een advertentie te meten en om gerichte advertenties aan de gebruiker te presenteren.
	test_cookie		Sessie	Gebruikt om te controleren of de browser van de gebruiker cookies ondersteunt.
help.afas.nl	ARRAffinity	afashelp.abna.appserviceenvironment.net	Sessie	Gebruikt om verkeer naar de website te distribueren op verschillende servers om de responstijden te optimaliseren.
	ARRAffinitySameSite	afashelp.abna.appserviceenvironment.net	Sessie	Gebruikt om verkeer naar de website te distribueren op verschillende servers om de responstijden te optimaliseren.
klant.afas.nl	__Host-.anon		Sessie	Vereist voor de beveiliging van de website.
klant.afas.nl **www.afas.nl**	__Host-.auth		Sessie	Vereist voor de beveiliging van de website.
	__Host-.cache		Sessie	Vereist voor de beveiliging van de website.

	__Host-.contextmenu		Sessie	Noodzakelijk voor de algemene functionaliteit van de website.
	__Host-.csrf.$id		Sessie	In afwachting
	__Host-.lastactivetabs		Sessie	Gebruikt in samenhang met gedrag van de bezoeker, door de website - De cookie registreert het gedrag en de navigatie van de bezoeker over meerdere websites en zorgt ervoor dat er geen volgfouten optreden wanneer de bezoeker meerdere browsertabs heeft geopend.
	__Host-.secureclient		Sessie	Vereist voor de beveiliging van de website.
	__Host-.securesession		Sessie	Vereist voor de beveiliging van de website.
	__Host-.storedviews		Sessie	Bevat gegevens over de laatste producten die door de bezoeker worden bekeken. Gebruikt voor interne statistieken door de exploitant van de website.
online.afas.nl	FPAU	afas.nl	2 maanden	Wijst een specifieke ID toe aan de bezoeker - Hiermee kan de website het aantal specifieke gebruikersbezoeken voor analyse en statistieken bepalen.
px.ads.linkedin.com	bcookie	.linkedin.com	1 jaar	Gebruikt om spam te detecteren en de beveiliging van de website te verbeteren.
	li_gc	.linkedin.com	½ jaar	Slaat de cookiestatus van de gebruiker op voor het huidige domein
	lidc		1 dag	Registreert welk servercluster de bezoeker bedient. Dit wordt gebruikt in samenhang met trafficverdeling, om de gebruikerservaring te optimaliseren.
segments.optinadserving.com	viewer	optinadserving.com	1 jaar	Gebruikt om de bezoeker relevante inhoud en advertenties te presenteren - De service wordt geleverd door advertentieshubs van derden, waardoor realtime bieden voor adverteerders wordt vergemakkelijkt.
www.youtube.com	VISITOR_INFO1_LIVE	.youtube.com	½ jaar	Probeert de bandbreedte van gebruikers te schatten op pagina's met geïntegreerde YouTube-video's.

	VISITOR_PRIVACY_METADATA	½ jaar	½ jaar	*"Used by YouTube to store the user's privacy and consent settings for embedded videos. It helps ensure that user privacy choices (like consent for personalized ads or tracking) are respected when watching embedded YouTube content."*
	YSC	.youtube.com	Sessie	Registreert een unieke ID om statistieken bij te houden van welke video's van YouTube de gebruiker heeft gezien.
	__Secure-ROLLOUT_TOKEN	youtube.com	½ jaar	In afwachting
	__Secure-YEC	.youtube.com	4 maanden	Bewaart de voorkeuren van de videospeler van de gebruiker met ingesloten YouTube-video
	__Secure-YNID		Sessie	In afwachting

Tabel D-4, cookies klant.afas.nl met consent.

Logging & Monitoring

Systeemresponsetijden log InSite

Veld	Waarde
ClientIP	Ip adres
Deelnemer	Deelnemer id / klant / instelling
Duration	miliseconden
Login	gebruikersnaam
Logtime	YYYY-MM-DD HH:MM:SS.MS
SourcePath	/
TargetPath	url - domein
Url	url
Index	
Label	categorienaam event of de pagina
SessionId	identificatienummer gebruikerssessie
SiteUrl	domain

TraceId	Uniek ID om een request of transactie end-to-end te volgen
User Agent	identificatiestring van browser/app en besturingssysteem
id	unieke sleutel
_time	tijdstip waarop het event heeft plaatsgevonden
host	
linecount	
punct	
source	oorsprong van het event, bijvoorbeeld *InSiteStatistics*
sourcetype	oorsprong van het event type, bijvoorbeeld *InSiteStatistics*
splunkserver	splunk-server die event verwerkt

Tabel D-5, overzicht systeemreactietijden logging AFAS InSite.

Read Access Logging Profit

Veldnaam	Beschrijving
Id	Unieke identificatie van het logrecord of de gebeurtenis.
OrgId	
TimeStamp	Datum en tijd waarop de actie is uitgevoerd of vastgelegd.
MemberId	Identifier van de instelling
EnvironmentId	Identifier van de specifieke omgeving
UserIdIn	Identifier van de instelling + gebruikersnaam
UserId	Hashed user id
Action	Omschrijving van de uitgevoerde actie
ActionId	Technische code of ID die de soort actie uniek identificeert
FormType	Type formulier of scherm dat is gebruikt
FormName	Technische aanduiding van scherm
Properties	Parameters die horen bij de actie
AdminMode	True of false

Version	Versie van de applicatie
View	
TabSheetId	Identifier van de specifieke tab of sectie binnen het scherm
Name	Naam van het object of record waarop de actie betrekking heeft
Code	Functionele of technische code van het object
name1	Aanvullende naam- of omschrijvingsveld
PrimaryKey	leeg
Title	Titel of beschrijvende naam van het scherm, formulier of object.

Tabel D-6, overzicht van verwerkte gegevens bij read access logging vanuit Profit.

Read Access Logging AFAS InSite

Veldnaam	Beschrijving
TimeStamp	Moment waarop de HTTP-aanvraag naar InSite is gedaan (datum en tijd van de gebruikersactie)
MemberId	Identifier van de instelling
EnvironmentId	Identifier van de AFAS-omgeving
UserId	Identifier van de instelling + gebruikersnaam
Verb	HTTP-methode van de request (bijv. GET, POST)
Url	Volledige URL die is aangeroepen, inclusief domein, pad en querystring
StatusCode	HTTP-statuscode van de response (bijv. 200 voor succesvol, 401/403/500 bij fouten)
IPAddress	Extern IP-adres van de client waarmee de gebruiker InSite heeft benaderd
DomainName	Domeinnaam van de InSite-omgeving (instellingid.afasinsite.nl)
VirtualPath	Virtueel pad naar de InSite-pagina
AppRelativePath	Applicatierelatief pad binnen InSite/Profit naar de opgevraagde resource

QueryString	Parameters achter de '?' in de URL die de specifieke aanvraag identificeren
Version	Versie van de InSite/Profit
Properties	Browser informatie

Tabel D-7, overzicht van verwerkte gegevens bij read access logging vanuit AFAS InSite.

Read Access Logging AFAS PocketApp

Veldnaam	Beschrijving
Id	Unieke identificatie van het logrecord of de gebeurtenis.
OrgId	
TimeStamp	Datum en tijd waarop de actie is uitgevoerd of vastgelegd.
MemberId	Identifier van de instelling
EnvironmentId	Identifier van de AFAS-omgeving
UserIdIn	Hashed user id
UserId	Identifier van de instelling + gebruikersnaam
ConnectorAppId	Identifier van de applicatie of client die de connector gebruikt
ConnectorType	Type connector
Verb	HTTP-methode van de request (bijv. GET, POST)
Path	Pad/endpoint van de aangeroepen connector-URL binnen de API
MethodName	Naam van de specifieke operatie binnen de connector
AdminMode	True of false
Version	Versie van de applicatie
ExtractedProperties	Uit de request of response afgeleide metadata

Tabel D-8, overzicht van verwerkte gegevens bij read access logging vanuit AFAS PocketApp.

Bijlage 2 Categorieën van persoonsgegevens

Direct identificeerbare gegevens
Dit zijn gegevens die worden gebruikt om een persoon op unieke wijze te identificeren (en te authentiseren/autoriseren). Voorbeelden hiervan zijn naam (voornaam, achternaam), geboortedatum en -plaats, burgerservicenummer (BSN), paspoort- of identiteitskaartnummer en biometrische gegevens (zoals vingerafdrukken of gezichtsherkenning).

Contactgegevens
Deze gegevens worden gebruikt om contact op te nemen met een persoon. Voorbeelden hiervan zijn: e-mailadres, telefoonnummer (vast en mobiel), postadres en sociale media-accounts.

Demografische gegevens
Dit zijn gegevens die de algemene kenmerken van een persoon beschrijven. Voorbeelden hiervan zijn leeftijd, geslacht, nationaliteit, burgerlijke staat, opleidingsniveau en beroep of functie.

Organisatiegegevens
Deze gegevens hebben betrekking op de organisatie waaraan een persoon verbonden is. Voorbeelden hiervan zijn bedrijfsnaam, functietitel, afdeling, werkadres, zakelijk e-mailadres en telefoonnummer.

Diagnostische gegevens
Deze gegevens hebben betrekking op de technische aspecten van het gebruik van apparaten en diensten. Voorbeelden hiervan zijn apparaat-ID's, browsertype en -versie, besturingssysteem, cookiegegevens, logbestanden en gebruiksstatistieken van apps of websites.

Financiële gegevens
Gegevens die informatie onthullen over iemands financiële situatie.

Bijzondere categorieën van gegevens
Persoonsgegevens die ras of etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen of lidmaatschap van een vakvereniging onthullen, en de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, gegevens betreffende de gezondheid of gegevens betreffende het seksleven of de seksuele geaardheid van een natuurlijke persoon. Deze gegevens zijn zeer gevoelig en worden in de AVG apart geïnterpreteerd.

Bijlage 3 Beveiligingsgaranties

Auteur: Shiyona Keenakkottil, Security Expert

Samenvatting van de beveiligingsgaranties

AFAS heeft meerdere vormen van beveiligingsgaranties verstrekt, waaronder certificeringen, auditrapporten en beschrijvingen van interne processen.

ISO/IEC 27001-certificering

AFAS heeft een bijgewerkt ISO/IEC 27001:2022-certificaat en een herziene Verklaring van Toepasbaarheid (SoA) opgeleverd. Hieruit blijkt dat de betreffende diensten nu binnen de scope vallen. Alle beheersmaatregelen uit Bijlage A zijn van toepassing verklaard, behalve controlemaatregel 8.30 (uitbestede ontwikkeling). Deze uitsluiting is naar behoren onderbouwd: AFAS ontwikkelt alle software en systemen volledig in eigen beheer met eigen medewerkers. Dat betekent dat er geen externe partijen erbij zijn betrokken. Het bijgewerkte certificaat en de SoA geven geen aanleiding tot opmerkingen of zorgpunten met betrekking tot de toepasbaarheid van de ISO/IEC 27001:2022-controlemaatregelen.

ISAE 3402 Type II-rapport

Tijdens het schrijven van de DPIA heeft SURF een ISAE 3402 Type II-rapport uit 2025 ontvangen; daaruit blijkt volgens de accountant dat de interne controles over het algemeen goed zijn ontworpen, maar dat er enkele afwijkingen in de uitvoering zijn geconstateerd. Belangrijke afwijkingen zijn onder meer:

- Ontbrekende of vertraagde monitoring van dagelijkse patch-tests
- Onvolledige documentatie van projecttestactiviteiten voor bepaalde soorten wijzigingen

De accountant concludeerde dat alle patches met succes zijn getest en dat de vereiste goedkeuringen uiteindelijk zijn verkregen. Deze afwijkingen worden beschouwd als een laag tot gemiddeld risico, voornamelijk vanwege problemen met de timing en de documentatie en niet zozeer vanwege fundamentele tekortkomingen in de controles. Het verstrekte rapport uit 2025 heeft veel van de eerder vastgestelde afwijkingen weggenomen, waardoor de bovengenoemde afwijkingen nog openstaan. AFAS heeft verduidelijkt dat deze auditbevindingen het gevolg waren van de starheid van het proces ten opzichte van de operationele uitvoering, waaronder buitensporige documentatievereisten. Volgens AFAS heeft het procesverbeteringsplannen in gang gezet om de auditcontroles beter af te stemmen op de praktische uitvoering, met behoud van de controledoelstellingen, in de hoop de bevindingen te verminderen en op te lossen.

SURF heeft voor publicatie het nieuwe ISAE 3402 Type II-rapport ontvangen van AFAS. Een uitgebreide analyse van dit rapport kon voor de publicatiedatum niet meer worden meegenomen en volgt bij de eerstvolgende update.

Back-up, RTO/RPO en continuïteitsmaatregelen

AFAS hanteert een uitgebreid back-up- en herstelprogramma, waarbij dagelijkse, maandelijkse en jaarlijkse back-ups consequent worden uitgevoerd. Back-ups worden

opgeslagen op een aparte locatie en maken gebruik van WORM-opslag (Write Once Read Many) om manipulatie te voorkomen. De herstelmogelijkheden van AFAS dragen bij aan de operationele betrouwbaarheid. Disaster Recovery-plannen zijn duidelijk gedefinieerd met RPO (Recovery Point Objective) en RTO (Recovery Time Objective) voor verschillende uitvalscenario's, samen met een beschrijving van stand-by servers en failover-mechanismen. AFAS vermeldt in de documentatie dat back-ups tot 7 jaar worden bewaard voordat ze worden verwijderd en dat de verwijdering gebaseerd is op beleid. Als het verwijderingsbeleid niet correct wordt gehandhaafd, kunnen persoonsgegevens langer bewaard blijven dan de huidige termijn van 7 jaar. Back-ups worden versleuteld met behulp van TDE (Transparent Data Encryption). Volgens de AFAS ISAE3402-controle worden, zodra een omgeving is versleuteld, alle daaropvolgende back-ups ook versleuteld.

Versleuteling
De leverancier geeft aan dat hij standaardversleutelingsmechanismen gebruikt om klantgegevens te beveiligen. Gegevens in rust worden versleuteld met Transparent Data Encryption (TDE) met AES-256 op Microsoft SQL Server en werkstations worden versleuteld met BitLocker. Inkomend verkeer wordt beveiligd met TLS 1.3. Volgens de uitgaande TLS-configuratie van AFAS worden de protocolversies TLS 1.0 en TLS 1.1 nog steeds ondersteund, wat de transportversleuteling kan verzwakken indien deze worden gebruikt.[105] Volgens de richtlijnen van het National Cyber Security Centre worden deze protocolversies aangemerkt als ‘ontoereikend’ en niet veilig voor gebruik, waarbij TLS 1.2 de aanbevolen minimumversie is en TLS 1.3 de voorkeur geniet.[106] AFAS heeft verklaard dat TLS 1.0/1.1 alleen wordt gebruikt voor een beperkt aantal bestaande klanten met technische afhankelijkheden en geen onderdeel vormt van de standaardconfiguratie. AFAS geeft aan dat deze protocollen niet van toepassing zijn op instellingen, ervan uitgaande dat instellingen geen verouderde systemen gebruiken die van deze protocollen afhankelijk zijn. AFAS geeft tevens aan dat de toegang tot eindpunten wordt gecontroleerd. Uitgaand verkeer wordt geregeld via een op een allow-list gebaseerd mechanisme, waarbij alleen vooraf goedgekeurde bestemmingen zijn toegestaan. Indien een benodigde verbinding niet beschikbaar is, moet er een incident worden gemeld bij AFAS om goedkeuring en vrijgave van het adres aan te vragen. AFAS bevestigt verder dat er jaarlijks evaluaties worden uitgevoerd om het gebruik opnieuw te beoordelen en ervoor te zorgen dat klanten die zijn gemigreerd van verouderde systemen, worden verwijderd uit de toegangslijst voor verouderde systemen, waarbij de bijbehorende toegang wordt uitgeschakeld.

Onafhankelijke tests van de publieke omgeving van AFAS geven aan dat deze uitsluitend TLS 1.2 en TLS 1.3 afdwingt. Er werd geen ondersteuning voor TLS 1.0 of TLS 1.1 waargenomen op de geteste eindpunten. De omgeving maakt gebruik van sterkere cipher suites, een geldig certificaat uitgegeven door GlobalSign en forward secrecy ingeschakeld, wat ervoor

[105] AFAS help webpage: https://help.afas.nl/help/NL/SE/plv2_Config_SysReq.htm?query=encryptie

[106] NCSC Netherlands TLS Guidelines 2025: https://www.ncsc.nl/transport-layer-security/ICT-beveiligingsrichtlijnen-voor-TLS , last read on 4th May 2026.

zorgt dat sleutels tijdelijk zijn en niet hergebruikt kunnen worden voor het decoderen van eerder verkeer.

Instellingen wordt aangeraden ervoor te zorgen dat alle systemen en koppelingen gebruikmaken van TLS 1.2 of hoger en geen gebruik maken van verouderde protocollen zoals TLS 1.0 of TLS 1.1, aangezien het voortgezette gebruik van verouderde systemen het beveiligingsrisico kan vergroten en de bescherming van gegevens tijdens het transport kan verzwakken.

AFAS beheert de versleutelingssleutels via een gecentraliseerd sleutelbeheerproces, waarbij privésleutels automatisch worden gegenereerd, opgeslagen en geroteerd. De SQL-hoofdsleutel valt echter niet onder de standaardrotatiecyclus vanwege de complexiteit van het systeem en de aanzienlijke inspanning die nodig is voor het opnieuw versleutelen, aldus AFAS. In plaats daarvan past AFAS compenserende maatregelen toe rond deze sleutel, waaronder opslag in een wachtwoordkluis, strikte beperkingen op de toegangscontrole en periodieke externe beoordeling van het toegangsbeheer. Bevoegde medewerkers, zoals systeemingenieurs en productbeheerders, hebben toegang tot de versleutelingssleutels, maar deze toegang is beperkt tot geautoriseerd personeel van de leverancier en wordt verleend op basis van just-in-time-toegang met volledige logboekregistratie en monitoring. Eventuele resterende insiderrisico's worden beperkt door strikte toegangscontrolemechanismen, beveiliging van de kluis en continue auditlogboekregistratie, wat resulteert in een laag risicoprofiel.

Logisch toegangsbeheer
AFAS beschrijft een logisch toegangsproces dat bestaat uit toegangsbeheer voor medewerkers, rolgebaseerde toewijzing van toegangsrechten via de ICT-manager en verplichte meervoudige authenticatie (MFA) voor medewerkers en klanten. Er worden regelmatig audits en controles uitgevoerd. AFAS voegde hieraan toe dat MFA standaard wordt afgedwongen, behalve wanneer klanten hun eigen authenticatieprovider gebruiken. Daarnaast wordt de inlogbeveiliging gewaarborgd door gelaagde controles bij mislukte authenticatiepogingen, waaronder progressieve beperking na meerdere mislukkingen (bijv. een CAPTCHA-uitdaging na enkele pogingen, gevolgd door strengere snelheidsbeperking en accountblokkering na een drempelwaarde van mislukte pogingen).

AFAS biedt geen speciale ‘Privilage access management’ module, maar volgens AFAS wordt dit geregeld via op rollen gebaseerde toegangscontrole in combinatie met tijdgebonden toewijzing van privileges. Verhoogde toegang kan tijdelijk worden verleend en wordt na een bepaalde periode automatisch ingetrokken, waardoor het risico van langdurige geprivilegieerde toegang wordt verminderd.

Veranderingsbeheer
AFAS beschikt over een proces voor verandermanagement dat serverupdates, wijzigingen in applicaties en de documentatie van geautomatiseerde workflows omvat. Standaardwijzigingen worden automatisch doorgevoerd, terwijl complexere wijzigingen goedkeuring van het management en tests vereisen voordat ze in productie worden genomen. Geautomatiseerde controles na updates controleren de integriteit van het systeem, en afwijkingen leiden tot vervolgacties.

Resultaten van penetratietests

Er is een rapport van een penetratietest voor twee diensten van AFAS – insite en outsite (niet alle diensten) – beoordeeld.[107] Er zijn verschillende kwetsbaarheden vastgesteld, waaronder onveilige communicatieconfiguraties, openbaar toegankelijke niet-productieomgevingen, IDOR, XSS, XML-injectie, tekortkomingen in de sessiebeveiliging, ontbrekende beveiligingsheaders, onvoldoende rate limiting en lacunes in de logboekregistratie en monitoring. AFAS heeft aangegeven dat alle bevindingen uit deze rapporten zijn aangepakt en opgevolgd binnen hun gecentraliseerde interne systeem. AFAS heeft ook het meest recente penetratietestrapport gedeeld met SURF en SURF voorzien van updates over de maatregelen die zijn genomen om de hoge risico's die in het penetratietestrapport zijn vastgesteld, te beperken.[108]

[107] Pen test report from AFAS 2024, *AFAS Public Report 2024 - Third Party Memo v1.2.* geraadpleegd op 23 april 2026.

[108] Pen test report from AFAS 2025, *AFAS public Report 2025*, geraadpleegd op 29 april 2026.