Data Protection Impact Assessment AFAS Profit (HRM en Payroll)

SURF Vendor Compliance

This is a non-binding translation. In the event of any discrepancies between this translation and the original document, the original document shall prevail.

Authors: Daisy Brugman, Jan Landsaat & Sophia Gelpke
Version: 1.1
Date: 16 July 2026

Summary

This document is a Data Protection Impact Assessment (DPIA) concerning the use of the SaaS application Profit by Dutch educational institutions (hereinafter: institutions), provided by AFAS B.V. (AFAS). This DPIA is an umbrella DPIA carried out by the sector organisation SURF, which provides institutions with a general framework for assessing data protection risks within Profit.

About the software
Profit is an integrated ERP system that automates and links business processes such as finance, HRM, CRM, project management and stock management within a single application.

Scope
SURF has carried out both legal and technical research to identify general data protection risks arising from the data processing activities that organisations carry out in Profit. This DPIA relates to the AFAS Profit ERP software package, with a specific focus on the HRM and Payroll modules. The native mobile application AFAS Pocket also falls within the scope, as it acts as a lightweight client that synchronises with the AFAS Online backend to provide HR and payroll functionalities on smartphones and tablets. In addition, support requests and the portals klant.afas.nl and help.afas.nl form an integral part of the assessment. Supporting functionalities such as Workflow & Document Management and CRM are only within the scope as far as they directly support the HR and payroll processes.

Outside the scope
The specific AFAS modules ‘Subscriptions’, ‘Finance’, ‘Tax’, ‘Order Management’ and ‘Projects’ fall entirely outside the scope of this DPIA, as do all external applications to which Profit may be linked, such as those of the occupational health and safety service. Furthermore, this DPIA assumes that the processing of personal data relating to minors in AFAS constitutes an exceptional situation, given that most people in the workforce are adults. Finally, the AI assistant ‘Jonas’ has also been excluded from the scope

As this is an umbrella DPIA, it does not contain an assessment of the lawfulness of specific processing activities, nor of risks specific to individual institutions. Instead, a more general assessment is made based on the intended use of Profit by institutions. Institutions wishing to use Profit may take this DPIA as a starting point, but must supplement, expand and/or adapt it based on the specific context in which they intend to use Profit.

Methodology
SURF has used the following methods to carry out the assessment:

- Legal research and assessment of AFAS's contracts, certifications and other documentation.
- Technical examination of the in-browser application, carried out in a test environment created by AFAS for SURF, including the use of a specialised monitoring tool (man-in-the-middle proxy).
- Requests for access from the parties involved, submitted after the technical investigation had been carried out.
- Questionnaires sent to AFAS representatives.

Result: 14 high-risk issues and 2 risks whose severity has yet to be determined
This DPIA has identified fourteen high risks to data subjects and two risks whose severity has yet to be determined. Five of the high risks relate to the division of roles under data protection law and contractual risks. Three of the high risks relate to the rights of data subjects. Six of the high risks are general risks, caused either by the way in which organisations (are likely to) use Profit, or by the design of AFAS. Two of the risks relate to the use of the mobile app. These two risks apply to any app that uses a third-party app store and push notifications. As SURF is conducting a further investigation into the impact of these risks, the risk level will be determined at a later stage.

Finally, SURF emphasises that the majority of the identified risks appear to relate to diagnostic data, rather than to the data that institutions themselves enter into Profit.

Measures
Implementing these measures will mitigate all high risks, leaving only low residual risks.

A timetable has been drawn up for the implementation of the measures for all these risks. Institutions can therefore continue to use Profit. Once the high risks have been mitigated, prior consultation with the data protection authority will not be required. SURF will publish an update on this DPIA in 2027, including a conclusion on the implementation of the remaining measures.

An overview of all identified risks and proposed measures is set out in the table below. The risks and measures sometimes apply to AFAS, as the supplier of Profit, and sometimes to the educational institutions as users of Profit. The status of the measures to be taken by AFAS is shown in the right-hand column.

#	Risk	Measures for educational institutions	AFAS measures	Status of AFAS measures
Division of roles and contractual risks				
1	Loss of control by AFAS as the data controller	Review and sign AFAS's revised data processing agreement.	Update the data processing agreement between AFAS and institutions to include, amongst other things: all categories of personal data, including diagnostic data where applicable, which AFAS and sub-processors process on behalf of institutions; legitimate purposes for which AFAS and sub-processors may process personal data and under what conditions; purposes for which AFAS and sub-processors may not process personal data.	AFAS will update its agreements by 31 December 2026 at the latest.
2	Loss of control and confidentiality due to incomplete data processing agreements	Review and sign AFAS's revised data processing agreement.	Update the data processing agreement between AFAS and institutions to include, amongst other things: all categories of personal data, including diagnostic data where applicable, which AFAS and sub-processors process on behalf of institutions; legitimate purposes for which AFAS and sub-processors may process personal data and under what conditions; purposes for which AFAS and sub-processors may	AFAS will update its agreements by 31 December 2026 at the latest.

#	Risk	Measures for educational institutions	AFAS measures	Status of AFAS measures
			not process personal data.	
3	Loss of control due to the absence of sub-processor agreements	Assess the sub-processors identified in the DPIA.[1] If you have any objections, submit a request to AFAS.	Regarding the support pages klant.afas.nl and help.afas.nl, which in practice are mainly visited by functional administrators: Enter into data processing agreements with LinkedIn, Google and Vimeo that incorporate the terms of the data processing agreement with institutions, including clear instructions on the personal data to be processed and a list of sub-processors.	
		-	With regard to the support pages klant.afas.nl and help.afas.nl, which in practice are mainly visited by functional administrators: Include a specification of the processing activities in the sub-processor agreements with Cookiebot, Cloudflare and Hunt & Hackett.	AFAS will update the agreements by 31 December 2026 at the latest.

[1] At the time the agreement was entered into and throughout its duration, these sub-processors were unknown to the institutions. Consequently, the institutions were unable to assess the parties at the time, and it was impossible to exercise the contractual right of objection.

#	Risk	Measures for educational institutions	AFAS measures	Status of AFAS measures
		-	With regard to AFAS Online: Conclude data processing agreements with Leaseweb that incorporate the terms of the data processing agreement with institutions, including clear instructions on the personal data to be processed and a list of sub-processors.	AFAS will update the agreements by 31 December 2026 at the latest.
4	Loss of control and confidentiality due to unauthorised access in third countries[2]	-	Contractually exclude transfers outside the EEA in the (sub-)processor agreements.	AFAS will update the agreements by 31 December 2026 at the latest.
Data subjects' rights				
5	Inability to exercise GDPR rights due to incomplete access requests	-	Provide full access to processing activities in response to an access request, either by enabling data controllers to access the information themselves or by implementing a clear procedure for handling access requests.	AFAS states that it has already implemented this measure. SURF has not yet verified this. The institution can request all logs directly via https://login.afasonline.com or, if necessary, submit

2 Although, from a legal perspective, no additional measures are required of the institution whilst the Data Privacy Framework remains in force, it is advisable to periodically review the geopolitical situation – particularly with regard to the likelihood of risks materialising – to determine whether an adjustment to the risk assessment is necessary.

#	Risk	Measures for educational institutions	AFAS measures	Status of AFAS measures
				a request via https://klant.afas.nl.
6	Inability to exercise GDPR rights and loss of control due to a lack of transparency regarding sub-processors	Regular checks on the list of sub-processors.	Depending on the sub-processor: update the SLA (data processing agreement), privacy notice and/or cookie policy with the relevant sub-processors.	AFAS will carry out a review of the (new) sub-processors for each version of the documents (SLA, General Terms and Conditions and Data Processing Agreement) by 31 December 2026 at the latest.
			Conclude master agreements and data processing agreements with all sub-processors, incorporating the terms set out in the data processing agreement with institutions, including clear instructions regarding the personal data to be processed and a list of sub-processors.	AFAS will update the agreements by 31 December 2026 at the latest.
7	It is not possible to exercise GDPR rights due to an unclear division of roles	Review and sign AFAS's revised data processing agreement.	Update the data processing agreement between AFAS and institutions to include, amongst other things: all categories of personal data, including diagnostic data where applicable, which AFAS and sub-processors process on behalf of institutions; legitimate purposes for which AFAS and sub-processors may process personal data and under what	AFAS will update its agreements by 31 December 2026 at the latest.

#	Risk	Measures for educational institutions	AFAS measures	Status of AFAS measures
			conditions; purposes for which AFAS and sub-processors may not process personal data.	
General Risks				
8	Loss of control due to self-built workflows	Ensure that HR staff are properly instructed and trained in the organisations' procedures for the careful recording of personal data. Periodically check the workflows, using random sampling, for effectiveness, proportionality, data minimisation, access and retention periods.	Implement a clear strategy to alert clients and users (in the context of data processing) to the data protection risks associated with these workflows.	AFAS states that it has already implemented this measure. SURF has not yet verified this. There are numerous (free) training programmes and courses available to institutions, both as part of the implementation process and independently of it.
9	Loss of control and confidentiality	Only use free-text fields with a clear purpose.	Implement a clear strategy to warn customers and users (in	AFAS states that it has already implemented this

#	Risk	Measures for educational institutions	AFAS measures	Status of AFAS measures
	due to other free-text fields	When creating free-text fields, the functional management team must tick a box to indicate whether these fields (may) contain sensitive or special-category personal data.	the context of data processing) not to enter (sensitive) personal data in open fields and to clarify the data protection risks associated with free-text fields.	measure. SURF has not yet verified this. There are numerous (free) training programmes and courses on this subject, which form part of the implementation process and are also available to institutions independently of the implementation.
		Ensure that staff are properly instructed and trained in the institutions' procedures for the careful recording of personal data.		
		Monitor the effectiveness of this policy through spot checks.		
10	Loss of confidentiality and control due to manual data entry	Ensure that HR staff are properly instructed and trained in the organisations' procedures for the careful recording of personal data.	-	-
		Automate data entry wherever possible.		
11	Loss of control due to failure to automatically configure retention periods	Establish and manage retention periods for personal data in AFAS.	Facilitate organisations in maintaining their retention periods by improving the options for the technical configuration and management of retention periods per group of personal data in AFAS.	AFAS has submitted this measure as a request on the (public) wish list to the Product Development department. AFAS will provide feedback on this by 31 December 2026 at the latest.
		Establish compliance with retention periods in processes.		

#	Risk	Measures for educational institutions	AFAS measures	Status of AFAS measures
12	Loss of confidentiality and control due to retention periods not being configured automatically within logging	Establish and manage retention periods for personal data in AFAS.	AFAS as a data processor: Enable automatic retention periods for logging and monitoring under the responsibility of organisations.	AFAS has submitted this measure as a request to the (public) wish list held by the Product Development department. AFAS will provide feedback on this by 31 December 2026 at the latest.
		Establish compliance with retention periods in processes.	AFAS as data controller: Establish, justify and manage retention periods for logging and monitoring under AFAS's responsibility.	AFAS has submitted this measure as a request on the (public) wish list with the Product Development department. AFAS will provide feedback on this by 31 December 2026 at the latest.
			AFAS as data controller: Configure automatic retention periods for logging and monitoring under AFAS's responsibility.	AFAS has submitted this measure as a request on the (public) wish list to the Product Development department. AFAS will provide feedback on this by 31 December 2026 at the latest.
13	Loss of control due to further processing of personal data via general	-	Set up the process in such a way that no personal data ends up in the general statistics.	AFAS will take measures. AFAS will provide feedback on this

#	Risk	Measures for educational institutions	AFAS measures	Status of AFAS measures
	statistics from the client environment			by 31 December 2026 at the latest.
			Review and improve the process relating to requests for these reports by AFAS staff. Establish a procedure for handling personal data and set retention periods.	AFAS states that it has already implemented this measure. SURF has not yet verified this. AFAS has set a retention period of one year. This retention period is also being adhered to and safeguarded within the process.
			Monitor this process in the event that personal data is processed.	AFAS states that it has already implemented this measure. SURF has not yet verified this. Every request is subject to at least the four-eyes principle.
14	Loss of control due to an incorrect cookie statement	-	Review the procedure relating to the cookie statement and the option to manage it independently.	AFAS states that it has already implemented this measure. SURF has not yet verified this. AFAS will evaluate the cookie notice periodically.
Mobile app risks				

#	Risk	Measures for educational institutions	AFAS measures	Status of AFAS measures
15	Loss of control over personal data due to the installation of applications via app stores	Enable access via the mobile web browser.	Make the app available via sideloading.	AFAS has decided that the Pocket App will not be offered via sideloading.
		Carry out a proportionality and subsidiarity assessment on making the mobile app available via app stores or as a 'side-load' and implement the results.	Enable access via the mobile web browser.	AFAS has decided that the Pocket App will not be made available via a mobile web browser.
16	Loss of control due to the processing of push notifications by Google and Apple	Do not include personal data in the content of the notifications.	*Optional:* implement Unified Push for Android users.	AFAS has decided not to implement this optional measure.
		Carry out a proportionality and subsidiarity assessment of sending push notifications via Google and Apple, or via Unified Push, and implement the results.		

Part C Description and assessment of risks to data subjects

This section concerns the description and assessment of the risks to data subjects. These are the risks identified during testing and analysis, prior to the implementation of risk mitigation measures. The risks are then categorised based on the likelihood of their occurrence and the impact on the rights and freedoms of data subjects should they occur.

The model used in this DPIA is based on 'the Government Model' and utilises the risk categories and risk model of the UK data protection authority, the ICO. The ICO identifies the following main categories of risks:

- inability to exercise rights (including, but not limited to, privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- damage to reputation;
- physical injury;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage.

These main categories provide guidance when identifying specific risks. By classifying risks based on their potential impact on the rights and freedoms of data subjects, a picture emerges of high, medium and low risks. This is illustrated in the risk chart developed by the UK regulator, the ICO, as follows:

Severity of impact	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood/probability		

In this DPIA, the following definitions of 'probability of the risk occurring' and 'severity of the consequences' are used to assess the risks:

Probability of the risk occurring	**Meaning**
Remote	It is unlikely that this risk will occur
Reasonable possibility	It is conceivable that this risk will occur
More likely than not	It is likely or certain that the risk will occur

Severity of the consequences	Significance
Minimal impact	If the risk materialises, it will have little or no impact on the rights and freedoms of the data subject
Some impact	If the risk materialises, it will have some impact on the rights and freedoms of the data subject
Serious harm (severe impact)	If the risk materialises, it will have serious consequences for the rights and freedoms of the data subject

Risk assessment

The following risks were identified during the conduct of this DPIA:[3]

Division of roles and contractual risks

C.1 Loss of control by AFAS as the data controller

AFAS does not, under any circumstances, act as the data controller for the personal data processed within the AFAS software. However, the contractual division of roles does not reflect the actual situation. The technical investigation revealed that AFAS actually carries out (further) processing operations that are not explicitly described or limited in the SLA, namely

- Monitoring to prevent malfunctions or resolve them at an early stage
- Collecting general user statistics
- Collecting anonymous statistics from the customer environment
- Measuring and analysing system response times
- Collecting, monitoring and analysing log data to prevent misuse

SURF takes the view that AFAS, at least for these specific processing activities, qualifies as an independent data controller, as it effectively exercises influence over the purpose and means of this (further) processing. See**Error! Reference source not found. Error! Reference source not found.** for a more detailed analysis of the division of roles. As a result, institutions have insufficient control over the manner in which data subjects' personal data are processed, leading to a loss of control for the data subjects themselves. If this further processing does not satisfy the compatibility test set out in Article 6(4) of the GDPR, it cannot be regarded as lawful.

The likelihood of this risk materialising is assessed as more likely than not, given that the actual situation already shows that AFAS carries out these processing operations outside the contractually agreed division of roles. If the risk materialises, the consequences for the

[3] SURF emphasises that the majority of the identified risks relate to diagnostic data, and explicitly not to the data that institutions themselves enter into Profit.

rights and freedoms of data subjects are potentially serious, as there is a loss of control. For this reason, this risk is classified as a high risk.

C.2 Loss of control and confidentiality due to incomplete data processing agreements

Under Article 28(3) of the GDPR, data processing agreements must specify the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, and the rights and obligations of the data controller. Due to the division of roles and the nature of Profit as generic standard software, AFAS has deliberately chosen not to include, either within or alongside the SLA[4] , a description of: categories of personal data, categories of data subjects, processing purposes, data subjects and retention periods. If desired, the categories of personal data may be attached to the agreement at the customer's request. Furthermore, not all relevant sub-processors (including LinkedIn, Vimeo and Google) are included in the data processing agreement.

As the categories of personal data, categories of data subjects, purposes of processing, data subjects, retention periods and (all) sub-processors involved are not included in the data processing agreement, there is no explicit instruction from the institution to AFAS. For example, without a clear, documented definition of purposes, it cannot be determined whether there is purpose limitation and compatible further processing. This results in a loss of control over the processing of personal data.

Furthermore, the SLA lacks an annex or further details regarding the technical and organisational security measures to be implemented. A mere reference to an ISO or NEN certification and the customer portal is insufficient in this context. Although the reference to the AFAS Customer Portal is practical, it constitutes a 'dynamic' source. This entails the risk that the SLA will be unilaterally amended as soon as the page is updated. Article 28(3)(c) of the GDPR requires the processor to implement appropriate measures in accordance with Article 32 of the GDPR, which necessitates a concrete approach tailored to the processing. Without further specification, the institutions cannot assess whether an appropriate level of security is actually in place, nor can they effectively manage or monitor this.

The risk is more likely to materialise than not, given that the data processing agreements are currently incomplete. Should the risk materialise, this would have serious consequences for the rights and freedoms of data subjects, as it could lead to misuse or incorrect processing of their personal data, unauthorised transfer and limited ability to exercise their rights. For this reason, this risk is classified as a high risk.

C.3 Loss of control due to the absence of sub-processor agreements

Under Article 28 of the GDPR, the data controller is obliged to engage only processors who provide sufficient guarantees regarding compliance with the GDPR. If a processor engages sub-processors, these may only be involved with the prior (specific or general) authorisation

[4] AFAS uses a Service Level Agreement (SLA), rather than a specific Data Processing Agreement.

of the controller, and binding agreements must be entered into with these sub-processors imposing the same data protection obligations as those set out in the agreement between the controller and the processor.[5] This contractual pass-through is essential to ensure that the institution retains control over the processing of personal data.[6]

SURF's investigation reveals the following:

- The sub-processor agreement with Leaseweb is no longer valid (has expired);
- The sub-processor agreements with, amongst others, Cookiebot, Cloudflare and Hunt&Hackett are incomplete, as they lack a specification of the processing operations;
- The necessary agreements with sub-processors such as LinkedIn, Google and Vimeo are missing.

The absence of (valid) contracts between AFAS and other parties leads to a lack of transparency regarding the data processed by the parties and to a loss of control over this data. It is more likely than not that this will occur, as the documentation is currently missing. This could cause serious harm to data subjects, as the absence of agreements means there is absolutely no control over this data. For this reason, this risk is classified as high.

C.4 Loss of control and confidentiality due to unauthorised access in third countries

The SLA stipulates that the processing of personal data by AFAS and the sub-processors it engages takes place exclusively within the EEA.[7] However, the technical investigation and the cookie policy identify sub-processors with 'parent companies' in the United States. This raises the question of whether data is being transferred outside the EEA.

Although the SLA contractually stipulates that data remains within the EEA, SURF cannot independently verify this guarantee in the absence of (complete) sub-processor agreements with all parties involved. This means that there may be a transfer of personal data to a third country within the meaning of Chapter V of the GDPR, for which appropriate safeguards are required.

Furthermore, certain parties (such as Vimeo and LinkedIn) are mentioned in the cookie policy, but are not listed in the SLA and did not emerge from the technical investigation. With regard to these parties, it is also the case that these companies (or at least their parent companies) are established in the United States. This means that here too, there may be a transfer of personal data to a third country within the meaning of Chapter V of the GDPR, for which appropriate safeguards are required.

[5] Article 28(2) and (4) of the GDPR.

[6] Article 24 of the GDPR.

[7] AFAS Service Licence Agreement April 2026, clause 5.7, accessed on 9 June 2026 via https://klant.afas.nl/sla-av.

Given that SURF is unable to verify this guarantee due to the absence of (complete) sub-processing agreements, the likelihood of a loss of control is greater than not. Should this occur, the consequences for the rights and freedoms of data subjects could entail serious harm, depending on the type of personal data disclosed and the party to whom it is disclosed. This therefore constitutes a high risk.

Rights of data subjects

C.5 Inability to exercise GDPR rights due to incomplete access requests

SURF has not received a response to the access requests. However, SURF does have the option of manually exporting data from the test environment where the technical analysis took place. This concerns content data, application logs and account data that are available to the data controller. However, to date, the access requests have been incomplete insofar as they relate to personal data in processing operations that are not visible to the institution. This applies in any case to the processing operations carried out by AFAS as the data controller, as further described in risk0 .

Failure to fully comply with requests for access means that data subjects are unable to exercise their rights and do not have a complete understanding of what data is being processed about them and how it is being used.

The likelihood that data subjects will be unable to exercise their right of access (and other GDPR rights) is therefore likely, given that AFAS was unable to provide one data subject with full access in a timely manner. Should this risk materialise, it would have serious consequences for the data subject's rights and freedoms, as the ability to exercise the right of access is necessary in order to exercise other GDPR rights. All these rights are fundamental rights of data subjects. For this reason, this risk is classified as a high risk.

C.6 Inability to exercise GDPR rights and loss of control due to a lack of transparency regarding sub-processors

Several sub-processors are not included in the SLA[8] . These include, amongst others, Cookiebot, Cloudflare, Hunt & Hackett, Google, LinkedIn and Vimeo. Furthermore, Microsoft is listed as a sub-processor, although AFAS states that Microsoft is not, in fact, a sub-processor for the processing operations covered by this DPIA. Microsoft is only used as a sub-processor in the specific context of the AI Assistant 'Jonas' (which falls outside the scope of this DPIA). However, this information is not evident from the SLA. This makes it difficult for the institutions, as data controllers, to obtain the necessary insight into the recipients and to provide this to data subjects.

For data subjects, this means that it is more difficult for them to exercise their right of access, as an overview of recipients may not be available (in a timely manner). Furthermore, this means that data subjects' data may be processed by parties over which there is no

[8] AFAS uses a Service Level Agreement (SLA) rather than a specific Data Processing Agreement.

control, as a result of which their data may be used for other purposes and a breach of confidentiality may occur.

The likelihood of this risk occurring is higher than not, as there is currently no complete list of AFAS's sub-processors. The impact is severe, as this risk may potentially affect all data processed in Profit, including special categories of personal data. Furthermore, the exercise of GDPR rights is a fundamental right of data subjects. The inability to exercise these rights therefore has a significant impact. For this reason, this risk is classified as a high risk.

C.7 Inability to exercise GDPR rights due to unclear division of roles

The unclear division of roles and the lack of transparency (as described in more detail in Chapter**Error! Reference source not found.** and risk C.1) mean that data subjects are unable to exercise their rights (effectively). In practice, data subjects will therefore be unable to exercise their right to object (Article 21 of the GDPR) to this further processing, as they are not sufficiently informed about its existence and nature.

The likelihood of this risk materialising is assessed as more likely than not, given that the actual situation already shows that AFAS carries out these processing operations outside the contractually defined division of roles. Should the risk materialise, the consequences for the rights and freedoms of data subjects are potentially serious, as the unclear division of roles and lack of transparency mean that data subjects are unable to exercise their fundamental rights. The inability to exercise these rights therefore has a significant impact. For this reason, this risk is classified as a high risk.

General Risks

C.8 Loss of control due to self-built workflows

AFAS offers the data controller the option to design and configure workflows themselves. Within these workflows, the organisation can make its own decisions regarding which roles, users and departments are granted access to which data and which steps they are permitted to carry out. In practice, this may result in more staff having access to (sensitive) personnel information than is necessary for their work and/or in more personal data being processed than is necessary.

As the institution sets up the workflows itself, there is a risk that 'privacy by design' and data minimisation are not applied consistently. Workflows may be set up in such a way that large groups of users are granted access or editing rights to files, documents or alerts without this being strictly necessary for their role. This increases the risk of the unauthorised dissemination or misuse of personal data within the organisation.

The likelihood of this risk materialising is higher than not, given the many options and possibilities for making incorrect choices when setting up the numerous workflows; this also takes into account the level of maturity of institutions, which varies considerably. If the risk materialises, it will have serious consequences for the rights and freedoms of the data subject, as there is a loss of control. For this reason, this risk is classified as a high risk.

C.9 Loss of control and confidentiality due to other free-text fields

It is possible to add comments to data subjects' files using free-text fields. These free-text fields serve no specific purpose, and organisations are therefore free to use them as they see fit. When creating free-text fields, the functional management team can tick a box to indicate whether they may contain sensitive or special categories of personal data.[9]

The existence of these free-text fields carries the risk that users may enter personal data into them for which organisations have no legal basis for processing or grounds for an exception special categories of personal data. This may result in a loss of control over the data – for example, because the data is retained for too long – and to a loss of confidentiality.

The likelihood of this risk materialising is higher than not, as there is no further guidance from the organisations to prevent the above and it depends on human fallibility. If the risk materialises, this will have serious consequences for the rights and freedoms of the data subject, as special categories of personal data may be processed. For this reason, this risk is classified as a high risk.

C.10 Loss of control and confidentiality due to manual data entry

Users can manually enter and edit personal data in Profit. This manual processing takes place via direct entry into the system, whereby new personal data can be added, and existing data can be amended or enriched. As a result, data subjects run the risk of their personal data being processed incorrectly, which could, for example, result in a performance review or salary details being entered for the wrong employee.

Where validation is possible, AFAS applies it to open fields. When entering, for example, email addresses, telephone numbers, Chamber of Commerce numbers and personally identifiable numbers (e.g. BSN), the system automatically checks whether the input consists of legitimate values that meet the criteria.

The likelihood of this risk materialising is higher than not, as data entry is subject to human error. Should the risk materialise, it would have some negative consequences for the rights and freedoms of data subjects, as the consequences would be directly felt in their lives. An example of this is financial loss resulting from incorrect salary processing. For this reason, this risk is classified as a high risk.

C.11 Loss of control and confidentiality due to the failure to automatically configure retention periods

AFAS does not offer any functionality that enables personal data to be automatically deleted once the retention period has expired, or that triggers a notification upon the expiry of a retention period. Consequently, there is a risk that personal data will be retained for

[9] AFAS Help Centre Netherlands, *'Marking free-text fields as personal data'*, accessed on 11 December 2025 via https://help.afas.nl/help/NL/SE/Crm_Config_PerOrg_Relat_AVG.htm#o93144.

longer than necessary, in breach of the principles of data minimisation and storage limitation.

It is more likely than not that this risk will materialise, as retention periods are not currently enforced by the system. Should the risk materialise, it would have serious consequences for the rights and freedoms of data subjects, as it affects all personal data held by Profit, including special categories of personal data. For this reason, this risk is classified as high.

C.12 Loss of control and confidentiality due to the failure to automatically configure retention periods within logging

AFAS generates and retains various types of log files, including transaction logging, read access logging, authorisation logging, etc. See **Error! Reference source not found. Error! Reference source not found.** &**Error! Reference source not found. Error! Reference source not found.** for a detailed explanation. Most log files must be manually deleted by the organisation once the specified retention periods have expired. In addition, there are logging layers in which activities relating to the consultation of logs themselves are recorded (so-called *'logging of logging'*). This specific data cannot be deleted or can only be deleted to a very limited extent, for technical reasons.

Due to the reliance on manual actions and the lack of automatic deletion options, there is a real risk that not all log files will be deleted in a timely manner or in full. This creates the risk that personal data will be retained for longer than necessary, in breach of the principles of data minimisation and storage limitation. Although the sensitivity of the logged personal data is relatively low, even such data must not be processed beyond the permitted retention period.

The likelihood of this risk materialising is greater than the likelihood of it not materialising. Should the risk materialise, it would have serious consequences for the rights and freedoms of the data subject, as there would be a loss of control and confidentiality. For this reason, this risk is classified as a high risk.

C.13 Loss of control due to further processing of personal data via general statistics from the customer environment

AFAS is able to generate general usage statistics from client environments on request. These reports are not based on pre-defined, standardised reports, but are requested on an ad hoc basis via a ticketing system. A Software Engineer assesses each request to determine whether the requested report will be prepared and provided. AFAS cannot rule out the possibility that personal data may be included (directly or indirectly) in these reports. AFAS states that this employee is qualified to carry out this assessment of data classification, but the actual basis for this remains unknown.

AFAS's Data Protection Officer and Privacy Officer have access to the request system and can view requests and intervene, if necessary, but have no formal decision-making role in the process. There are no documented procedural arrangements on how to deal with situations in which personal data appears in these reports, nor have specific retention periods been agreed with the recipient of the report or for storage within the request system itself. This means that reports which may contain personal data can be retained indefinitely.

This creates a risk that the supplier may carry out further processing that is not explicitly described or restricted in the SLA and about which the data controller (and the data subjects) have not been informed or have been insufficiently informed. The purposes, legal basis and retention periods for this further processing are not clearly defined, and there is no certainty that this further processing is compatible with the original purposes.

The likelihood of this risk materialising is reasonable, given that staff have the option to request such reports. Should the risk materialise, this will have serious consequences for the rights and freedoms of the data subject, as there is a loss of control due to further processing where limited measures have been put in place to regulate these reports. For this reason, this risk is classified as a high risk.

Cookies

C.14 Loss of control due to an incorrect cookie policy

The cookie statement for klant.afas.nl (help.afas.nl) is managed by Cookiebot and is therefore not entirely under the direct control of AFAS. In the current cookie statement, certain cookies are classified as 'necessary', whilst they are not strictly necessary for the technical operation or security of the service.

In addition, there are cookies for which no description is yet available. The provider is unable to specify the purpose or content of these cookies. As a result, users are given an incomplete and partly inaccurate picture of which cookies are set, for what purpose and on what basis. This lack of clarity creates a risk that non-essential cookies may be set without valid and/or informed consent, or that consent may be sought on the basis of incomplete information.

It is more likely than not that this risk will materialise. If the risk materialises, it will have serious consequences for the rights and freedoms of the data subject, as the lack of transparency constitutes a breach of a principle of the GDPR, particularly when tracking cookies or similar technologies are used. For this reason, this risk is classified as a high risk.

Risks arising from the provision of a mobile app via the Google and Apple app stores

At the time of publication, SURF has not yet reached a conclusion regarding the impact of the following two risks, which relate to data processing by Google and Apple when using mobile apps. The considerations and measures identified by SURF are described below. However, SURF is conducting further research into the impact of these risks and the effect of available measures on them. A publication on this subject will appear at a later stage. In the meantime, organisations can take measures based on their own assessments.

C.15 Loss of control over processed personal data due to the installation of a mobile app via a third-party app store

The risk associated with offering the Pocket app via the Apple App Store and Google Play Store lies in the automatic link established between the use of the app and the user's personal Apple or Google account. This link enables these platform providers to gain insight into the installation of the app, which may lead to the indirect identification of the user's relationship with AFAS. As this processing is not strictly necessary for the functioning of the app, it contravenes the 'Privacy by Default' principle and results in a loss of control over personal data.

The likelihood of this risk materialising is higher than not, given that control is lost as soon as the app is downloaded via an app store. Consequently, personal data relating to employees inevitably flows to third parties such as Apple and Google, which may compromise confidentiality and increase the risk to employees' rights and freedoms. This leads to the potential exposure of personal data without this being strictly necessary and to the involvement of major platform providers.

Alternatives that infringe less on privacy must be considered in order to better protect users' data and ensure compliance with data minimisation requirements.

C.16 Loss of control due to the processing of push notifications by Google and Apple

This is a risk that generally applies to all applications using Google's or Apple's push notification infrastructure.

The Pocket mobile app sends push notifications. The push notifications result in the transfer of both metadata and content to Google and Apple. The metadata comprises data such as device IDs, IP addresses and, potentially, the student's Google or Apple account. The content comprises the messages, provided that such content is not sent in encrypted form, as is necessarily the case with the 'notification messages' component of the push notifications. The content of these messages is visible to and processed by Google and Apple. As it is not necessary to include personal data in notifications, this constitutes a breach of the principle of subsidiarity. Educational institutions determine the content of the messages themselves and can make privacy-friendly choices by not including personal data.

Regardless of the content of the messages, the use of notification messages means that the content of the messages is systematically processed by Google. It is possible to limit this processing by using an encrypted data payload, either on top of the notification message or separately. If a student has access to Unified Push, an alternative push infrastructure for Android, the app can also make use of this and fall back on Google if it is unavailable. As both of these mitigating measures are absent, the use of notifications does not meet the subsidiarity requirement.

The likelihood of a loss of control is greater than not, as notifications are a standard feature of the Pocket app and the loss of control occurs as soon as Google or Apple receives the notification.

Part D Description of proposed measures

D.1 Restrictive measures

Loss of control by AFAS as the data controller						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	**Current risk**
C.1	AFAS carries out (further) processing operations as a data controller without contractual arrangements.	Loss of control.	**More likely than not**	**Serious**	**High**	**Current risk**
	Organisational measure	**Vendor measure**	**Probability**	**Severity**	**Risk score**	**Residual risk**
	Review and sign AFAS's revised data processing agreement.	Update the data processing agreement between AFAS and institutions to include, amongst other things: all categories of personal data, including diagnostic log data where applicable, which AFAS and sub-processors process on behalf of institutions; legitimate purposes for which AFAS and sub-processors may process personal data and under what conditions; purposes for which AFAS and sub-processors may not process personal data.	**Remote**	**Serious**	**Low**	**Residual risk**

Loss of control and confidentiality due to incomplete data processing agreements						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	
C.2	There is no comprehensive data processing agreement between institutions and AFAS, as AFAS does not use a separate data processing agreement and the provisions included in the SLA in this regard are incomplete.	Loss of control.	**More likely than not**	**Serious**	**High**	**Current risk**
	Institution's measure	**Vendor measure**	**Probability**	**Severity**	**Risk score**	
	Review and sign AFAS's revised data processing agreement.	Update the data processing agreement between AFAS and institutions to include, amongst other things: all categories of personal data, including diagnostic log data where applicable, which AFAS and sub-processors process on behalf of institutions; legitimate purposes for which AFAS and sub-processors may process personal data and under what conditions; purposes for which AFAS and sub-processors may not process personal data.	**Remote**	**Serious**	**Low**	**Residual risk**

Loss of control due to the absence of sub-processor agreements						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	**Current risk**
C.3	Contracts with sub-processors are missing or do not meet the requirements.	Loss of control.	**More likely than not**	**Serious**	**High**	
	Institutional measure	**Vendor measure**	**Probability**	**Severity**	**Risk score**	**Residual risk**
	Assess the sub-processors identified in the DPIA.[10] In the event of an objection, submit a request to AFAS.	With regard to AFAS Online and the support pages klant.afas.nl and help.afas.nl, which in practice are mainly visited by functional administrators: Enter into data processing agreements with LinkedIn, Google and Vimeo that incorporate the terms of the data processing agreement with institutions, including clear instructions on the personal data to be processed and a list of sub-processors.	**Remote**	**Serious**	**Low**	
		With regard to AFAS Online and the support pages klant.afas.nl and help.afas.nl, which in practice are mainly visited by functional administrators: Include a specification of the processing activities in the sub-processor agreements				

[10] At the time the agreement was entered into and throughout its duration, these sub-processors were unknown to the institutions. Consequently, they were unable to assess the parties at the time, and it was impossible to exercise the contractual right to object.

		with Cookiebot, Cloudflare and Hunt & Hackett. With regard to AFAS Online: Conclude data processing agreements with Leaseweb that incorporate the terms of the data processing agreement with institutions, including clear instructions regarding the personal data to be processed and a list of sub-processors.				

Loss of control and confidentiality due to unauthorised access in third countries[11]						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	
C.4	Transfer of personal data to parties based in the US or having a parent company there.	Loss of control and confidentiality.	**More likely than not**	**Serious**	**High**	**Current risk**
	Institutional measure	**Vendor measure**	**Probability**	**Severity**	**Risk score**	
	-	Contractually prohibit transfers outside the EEA in the (sub-)processor agreements.	**Remote**	**Serious**	**Low**	**Residual risk**

[11] Although, from a legal perspective, no additional measures are required of the institution whilst the Data Privacy Framework remains in force, it is advisable to periodically review the geopolitical situation – particularly with regard to the likelihood of risks materialising – to determine whether an update to the risk assessment is necessary.

Data subjects' rights

Inability to exercise GDPR rights due to a lack of response to requests for access						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	
C.5	Incomplete response to a data subject access request due to the absence of processing operations that are invisible to organisations.	It is not possible for data subjects to exercise their GDPR rights.	**More likely than not**	**Serious**	**High**	**Current risk**
	Institution's remedial action	**Vendor measure**	**Probability**	**Severity**	**Risk score**	**Residual risk**
	-	Provide full access to processing activities in response to an access request, either by enabling data controllers to access the information themselves or by implementing a clear procedure to process access requests.	**Remote**	**Serious**	**Low**	

Inability to exercise GDPR rights and loss of control due to a lack of transparency regarding sub-processors						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	
C.6	Contracts with sub-processors are missing or do not meet the requirements.	It is not possible for data subjects to fully exercise their GDPR rights, and there is a loss of control over processing activities.	**More likely than not**	**Serious**	**High**	**Current risk**
	Institutional measure	**Vendor measure**	**Chance**	**Severity**	**Risk score**	**Residual risk**
	Regular review of the list of sub-processors.	Depending on the sub-processor: update the SLA (data processing agreement), privacy notice and/or cookie policy with relevant sub-processors.	**Remote**	**Serious**	**Low**	
		Conclude main and data processing agreements with all sub-processors, incorporating the terms of the data processing agreement with organisations, including clear instructions on the personal data to be processed and a list of sub-processors.				

It is not possible to exercise GDPR rights due to an unclear division of roles						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	
C.7	The unclear division of roles and the lack of transparency (as described in more detail in risk C.1.) mean that data subjects are unable to exercise their rights (effectively).	It is not possible for data subjects to fully exercise their GDPR rights, and supervisory authorities lose control.	**More likely than not**	**Serious**	**High**	**Current risk**
	Organisational measure	**Vendor measure**	**Probability**	**Severity**	**Risk score**	
	Review and sign AFAS's revised data processing agreement.	Update the data processing agreement between AFAS and institutions to include, amongst other things: all categories of personal data, including diagnostic data where applicable, which AFAS and sub-processors process on behalf of institutions; legitimate purposes for which AFAS and sub-processors may process personal data and under what conditions; purposes for which AFAS and sub-processors may not process personal data.	**Remote**	**Serious**	**Low**	**Residual risk**

General risks

Loss of control due to self-built workflows						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	
C.8	Designing and configuring workflows yourself.	Loss of control because more staff members are granted access to (sensitive) personnel information than is necessary for their work and/or because more personal data is processed than is necessary.	**More likely than not**	**Serious**	**High**	**Current risk**
	Organisational measure	**Vendor measure**	**Probability**	**Severity**	**Risk score**	
	Ensure that HR staff are properly briefed and trained in the organisations' procedures for the careful recording of personal data.	Implement a clear strategy to alert customers and users (in the context of data processing) to make the risks associated with the workflows clear.	**Remote**	**Serious**	**Low**	**Residual risk**
	Periodically check the workflows by means of spot checks for effectiveness, proportionality, data 30inimization, access and retention periods.					

Loss of control and confidentiality due to other free-text fields						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	
C.9	Filling in free-text fields.	Loss of control and confidentiality.	**More likely than not**	**Serious**	**High**	**Current risk**
	Organisational measure	**Vendor measure**	**Probability**	**Severity**	**Risk score**	
	Only use open text fields with a clear purpose.	Implement a clear strategy to warn customers and users (in the context of the processing) not to enter any (sensitive) personal data into open fields and to make the risks associated with free-text fields clear.	**Remote**	**Serious**	**Low**	**Residual risk**
	When creating free-text fields, the functional management team must tick the box to indicate whether these fields may contain sensitive or special categories of personal data.					

	Ensure that staff are properly briefed and trained in the organisations' procedures for the careful recording of personal data. Monitor the effectiveness of this policy through spot checks.					

Loss of confidentiality and control due to manual data entry						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	**Current risk**
C.10	Manual entry of incorrect information.	Loss of confidentiality and control.	**More likely than not**	**Serious**	**High**	
	Organisational control	**Vendor measure**	**Probability**	**Severity**	**Risk score**	**Residual risk**
	Ensure that HR staff are properly briefed and trained in the organisations' procedures for the careful recording of personal data. Automate data entry where possible.	-	**Remote**	**Serious**	**Low**	

Loss of control due to retention periods not being configured automatically						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	**Current risk**
C.11	No automatic retention periods.	Loss of control.	**More likely than not**	**Serious**	**High**	
	Institutional measure	**Vendor measure**	**Probability**	**Severity**	**Risk score**	**Residual risk**
	Establishing and managing retention periods for personal data in AFAS. Establishing compliance with retention periods in processes.	To assist organisations in maintaining their retention periods by improving the options for the technical configuration and management of retention periods per group of personal data in AFAS.	**Remote**	**Serious**	**Low**	

Loss of confidentiality and control due to retention periods not being configured automatically within logging						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	**Current risk**
C.12	No automatic retention periods can be configured within logging.	Loss of control	**More likely than not**	**Serious**	**High**	
	Remedy: configuration	**Vendor measure**	**Probability**	**Severity**	**Risk score**	**Residual risk**
	Establishing and managing retention periods for personal data in AFAS. Establish compliance with retention periods in processes.	AFAS as a data processor: Enable automatic retention periods for logging and monitoring under the responsibility of institutions. AFAS as data controller: Establish, justify and manage retention periods for logging and monitoring under AFAS's responsibility. AFAS as the data controller: Configure automatic retention periods for logging and monitoring under AFAS's responsibility.	**Remote**	**Serious**	**Low**	

Loss of control due to further processing of personal data via general statistics from the client environment						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	**Current risk**
C.13	Further processing of personal data via general statistics from the customer portal.	Loss of control.	**More likely than not**	**Serious**	**High**	
	Organisational measure	**Vendor measure**	**Probability**	**Severity**	**Risk score**	**Residual risk**
		Set up the process in such a way that no personal data ends up in the general statistics.	**Remote**	**Serious**	**Low**	
		Review and improve the process for AFAS staff requesting these reports. Establish a procedure for handling personal data and set retention periods.				
		Monitor this process in case personal data is processed.				

Loss of control due to an incorrect cookie statement						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	**Current risk**
C.14	The unclear cookie statement for klant.afas.nl (help.afas.nl) is managed by Cookiebot and is therefore not (entirely) under the direct control of AFAS.	Loss of control.	**More likely than not**	**Serious**	**High**	
	Organisational measure	**Vendor measure**	**Probability**	**Severity**	**Risk score**	**Residual risk**
	-	Assess the procedure relating to the cookie policy and the option to manage it independently.	**Remote**	**Serious**	**Low**	

Mobile app risks

Loss of control over personal data due to the installation of an application via app stores						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	**Current risk**
C.15	The need to download the Pocket app via the Google and/or Apple mobile app stores	Loss of control.	**More likely than not**	**Serious**	**TBD**	
	Organisational countermeasure	**Vendor measure**	**Probability**	**Severity**	**Risk score**	**Residual risk**
	Enable access via the mobile web browser.	Make the app available via sideloading.	**Remote**	**Minimal**	**Low**	
	Carry out a proportionality and subsidiarity assessment of making the mobile app available via app stores or as a 'side-load' and implement the results.	Enable access via the mobile web browser.				

Loss of control due to push notifications being processed by Google and Apple						
Reference	**Cause**	**Consequence**	**Probability**	**Severity**	**Risk score**	**Current risk**
C.16	Sending push notifications via Google and Apple.	Loss of control.	**More likely than not**	**TBD**	**TBC**	
	Measure: organisation	**Vendor measure**	**Probability**	**Severity**	**Risk score**	**Residual risk**
	Do not include personal data in the content of notifications.	Optional: implement Unified Push for Android users.	**TBC**	**TBC**	**TBC**	
	Carry out a proportionality and subsidiarity assessment on sending push notifications via Google and Apple, or via Unified Push, and implement the results.					