Driving innovation together

DPIA Ans Exam

Data Protection Impact Assessment on the processing of personal data in Ans Exam

Author(s): Sanne Ouburg, Mike Noordermeer

Version: 1.0
Date: 12 December 2025

Table of contents

Version history

Version	Date	Summary of changes
0.1	23 April 2025	Draft part A for SURF.
0.2	22 July 2025	Feedback from Ans incorporated into part A. Full draft.
0.3	25 July 2025	Feedback SURF incorporated – structural and textual changes.
0.4	3 November 2025	Feedback and measures Ans incorporated. Review of risks and resulting risks.
0.9	3 December 2025	Further measures Ans incorporated. Final version for NDA check.
1.0	12 December 2025	Final version.

Summary

This report is a data protection impact assessment (hereinafter: DPIA) on the use of the SaaS application Ans Exam by educational institutions (hereinafter: institutions), offered by Ans Exam B.V. (formerly Ans Delft). This DPIA is a central DPIA, carried out by Privacy Company on behalf of SURF, the ICT cooperative of Dutch education and research institutions, which provides institutions with a general framework for assessing data protection risks within Ans Exam.

Scope

This DPIA focuses on the Ans SaaS solution and its API. It reviews the main functions, such as creating tests, grading, and performing analyses. This DPIA assumes that the use of the standard SURF DPA, therefore the provisions of the standard Ans DPA are not assessed. Only Schedule 1 of the Ans DPA is used as a reference.

Methodology

Privacy Company combined a legal fact-finding strategy with a technical examination of the data processed through the use of Ans. The technical assessment identifies how personal data is processed. These processing operations are reviewed against the available documentation and relevant legal requirements. The assessment also examines which sub-processors are used, for what purposes, and whether any personal data is transferred outside the EU.

Privacy Company conducted its research using public information, the documentation about the system (as supplied by the supplier) and by analysing the possibilities via a (test) licence or licences with three different user roles: administrator, teacher (supervisor) and two participants (students).

Outcome: 13 high risks, 3 medium risks and 1 low risk

The table below shows the 13 high risks, 3 medium risks and 1 low risk for data subjects, with the mitigating measures the institutions can take, as well as the suggested measures for Ans. Table 2 includes an overview of the measures Ans agreed to take and the timelines for the implementation of these measures.

Some measures require changes to the agreement between institutions and Ans. Ans will prepare these changes in Q1 2026 and will contact institutions when the required changes are available for review.

Table 1: Overview risks and measures

Nr.	Risk	Measures institutions	Measures Ans
1	Loss of control – Incomplete description of processing activities in DPA	Update the DPA. Ensure the DPA clearly and comprehensively lists all processing activities,	Update the DPA, so that it is up-to-date and clearly specifies all data processing operations carried out on behalf of

🟥		types of personal data processed, purposes, retention periods, and sub-processors. Implement procedures to periodically verify that the actual data processing aligns with what is documented in the DPA and update the agreement as needed.	the institution, including a comprehensive sub-processor list. Proactively inform the institution about any changes to processing activities and assist with updating the DPA promptly to reflect these changes.
🟥 2	Loss of control – Role division	Together with Ans define and document a clear definition of roles, specifying which data processing operations are performed by Ans as processor and which are undertaken by Ans as independent data controller. Provide clear communication to the data subjects (including where data subjects should direct requests related to their personal data).	Align the descriptions of personal data categories and processing purposes across the DPA, Privacy Policy and other legal documentation to eliminate overlap and clarify the distinction between processor and controller roles. Clearly communicate when Ans processes personal data for its own purposes (including legal basis and contacts for exercising data subject rights). Conduct and document a compatibility assessment under Article 6(4) GDPR for any further processing.
🟩 3	Inability to exercise data subject rights – Right to object direct marketing	Clarify roles and responsibilities in the communication chain. Require Ans to comply with transparency obligations under the GDPR.	Update the privacy policy to explicitly mention the right to object under Article 21 GDPR. Update the privacy policy to inform the data subject what personal data is used for what purpose.

🟩			Clearly label emails with their purpose (e.g. product update, marketing) and indicate who is the sender (controller), so recipients can make informed decisions and exercise their rights appropriately.
🟥 4	Lack of transparency – List of sub-processors is incomplete	Exercise the audit right to regularly audit which sub-processors are used. Ensure all sub-processors are included in the legal framework (including personal data processed by this sub-processor and the processing location).	Provide transparency on the applicable sub-processors and maintain a complete list and ensure that all personal data processed by the sub-processor is listed.
🟥 5	Loss of control – DPA with TransIP lacks clear and specific instructions	Implement strong contractual controls and approval processes for (new) sub-processors.	Ensure the DPA and its annexes (e.g., types of personal data, processing purposes, categories of data subjects) are customized and accurately reflect what processing will occur. Or: Use another supplier for file storage.
🟥 6	Loss of control – Processing location SorryApp	Exercise the audit right to regularly audit which sub-processors are used.	Clarify data processing location(s) and legal transfer mechanism with SorryApp, or alternatively replace processor SorryApp with a different party with a processing location in the EEA or a valid legal transfer mechanism. Or:

🟥			Remove references to status website from the application, limiting exposure of student and staff to SorryApp.
🟥 7	Lack of transparency – User impersonation not visible in UI	Disallow the use of user impersonation by administrators, until proper logging is in place.	Make sure start and end of impersonation is logged, and logs are surfaced in user interface. Log the username of the impersonating user with any actions that used impersonation.
🟧 8	Chilling effect – Email tracking notification emails		Disable open tracking of notification emails.
🟥 9	Chilling effect employees - Insights reviewer alignment	Ensure that there is a legal basis for the insights reviewer alignment. Obtain approval from the Works Council before implementing any form of employee monitoring.	Disable the time spent reviewing insights.
🟧 10	Loss of control due to lack of transparency - Feedback students		Either give students the option to submit feedback anonymously, and/or the interface should clearly state that the comment and the student's name (and other details) will be visible to the instructors.
🟥 11	Lack of transparency – Incomplete cookie information	Regularly audit the web traffic for not listed cookies.	Comply with the legal transparency requirements about cookies and similar technologies. Update complete list of cookies.

12	Lack of data minimisation – Application logging	Re-assess application logging, access and retention periods, together with Ans (in a joint exercise through SURF).	Re-assess application logging, access and retention periods, together with SURF and institutions.
13	Loss of confidentiality – One-time passwords	Develop and enforce clear internal guidelines on when and how one-time passwords can be generated and used, including who is authorised to issue them, for what purposes, and how their use is documented and monitored.	Ensure that one-time passwords are restricted in scope and grant access only to the specific part of the platform necessary for their intended purpose (e.g., accessing a particular exam), and not to broader student data or full student records.
14	Loss of control – Personal data processed longer than needed	Clearly specify retention periods for different categories of personal data and ensure that staff are instructed to initiate permanent deletion within these timelines, particularly for student accounts and results, or automate deletion using API access.	Allow permanent deletion of all entities, including users. Allow users to permanently delete entities within 180-days soft-deletion period. Simplify the deletion model (clear split between soft-deletion (trash) and hard-deletion).
15	Loss of control – Integrated Google Services	Do not implement YouTube videos in the exams.	Replace Google Charts by a different solution, preferably hosted as part of the application.
16	Inability to exercise data subject rights – Administrators not fully able to honour DSARs	Create a procedure to handle a data subject requesting its personal data from Ans to ensure all personal data is included in the response.	Create a support page describing how controllers can fulfil a DSAR, assisting controllers through the support channel where necessary.

			Add additional buttons in the product to more easily export data of users.
17	Lack of adequate procedures for reporting security incidents	Ensure that the DPA with Ans includes explicit obligations regarding breach notifications (in line with Article 28 and 33 GDPR). Periodically audit or request evidence from Ans demonstrating compliance with these requirements to verify they have appropriate measures in place. Subscribe applicable staff to security advisories from Ans.	Create security advisories section in Ans' support portal. Establish and document a clear internal procedure for identifying, assessing, and reporting security vulnerabilities (including criteria for escalation, timelines). Train staff on this protocol.

Conclusion

The DPIA identified 13 high risks, 3 medium risks and 1 low risk for data subjects. The risks arise from contractual factors, the product's functionalities, and the use of subprocessors. If the proposed measures are implemented, all high risks will be reduced to low residual risks. In that case, no prior consultation with the Data Protection Authority is required. Although reducing low risks is not strictly necessary, it is recommended because the measures are easy to implement and help better protect the rights and freedoms of data subjects.

Throughout the DPIA process, Ans has shown a clear commitment to addressing all identified risks and has proactively begun implementing mitigating measures. As a result, risks have already been resolved ahead of the DPIA's completion (See the textboxes in Part A). For the remaining risks, some measures require additional time. Ans commitments are listed at the end of this conclusion.

Some risks originate from the contractual framework. Ans has committed to updating their templates (including Schedule 1) by the end of Q1 2026 (Ans will work closely with SURF on this). However, Ans expressed concerns about fully resolving these risks in a timely manner, noting that institutions are often reluctant (or slow due to lengthy internal processes) to accept changes and sign updated agreements. Although Ans is in the best position to identify and list which personal data is processed and for what purpose, it is ultimately the controller's responsibility to ensure that a data processing agreement meeting the requirements of Article 28 (3) GDPR is in place. Institutions should therefore pay close attention to this and proactively ensure that their agreements are updated and compliant. Ans will send out an updated agreement by the end of Q1 2026.

Other risks relate to features institutions themselves requested in their tenders. An example of this is the dashboard features that allow examinators to closely monitor each student's test progress in detail. It is important that institutions take privacy into account when drafting and issuing their tenders or make feature requests.

As a final note, institutions are recommended to use single sign-on (SSO) and enforce SSO, using a dedicated domain for the Ans application. Although this recommendation does not directly relate to an identified personal data risk, certain classes of risks can be avoided by enforcing single sign-on (e.g., one of the vulnerabilities in this DPIA was not applicable to institutions enforcing SSO).

Following the DPIA, Ans Exam has committed to a set of concrete mitigating measures that were jointly defined and agreed upon by Ans Exam, SURF and Privacy Company. Ans has committed to the following timelines for their measures:

Table 2: Overview commitments Ans

Nr.	Mitigating measures Ans	Timeline
1	Update Schedule 1 with the correct information (with assistance from SURF)	Q1 2026
	Replace Schedule 1 for the existing DPAs with updated versions containing the correct information.	Q1 2026
	Update and use the new template for all future DPAs	Q1 2026
2	Update Schedule 1 with the correct information (with assistance from SURF).	Q1 2026
	Replace Schedule 1 for the existing DPAs with updated versions containing the correct information.	Q1 2026
	Update and use the new template for all future DPAs.	Q1 2026
	Update Privacy Policy with the correct information (with assistance from SURF).	Q1 2026
3	Update Privacy Policy with the correct information (with assistance from SURF).	Q1 2026
	Addition to the emails (short description in the email itself rather than labelling the emails) to indicate the sender (controller).	Q1 2026
4	Update Schedule 1 with the correct information (with assistance from SURF).	Q1 2026

	Replace Schedule 1 for the existing DPAs with updated versions containing the correct information.	Q1 2026
	Update and use the new template for all future DPAs.	Q1 2026
5	Migrate all files containing personal data from TransIP to Amazon S3.	Before the end of Q3 2026
6	Address shortcomings in StatusPal DPA and annexes together with StatusPal.	Q1 2026
	Migrate status website to StatusPal.	Q1 2026
7	Add start and end of user impersonation to the user logs.	Q1 2026
	Log the username of the impersonating user with any actions that used impersonation.	Q1 2026
	Surface impersonation logs in the user interface.	Q1 2026
8	Disable open tracking of notification emails.	Q1 2026
9	Disable the time spent reviewing insights.	Completed in new grading experience, fully removed from the product in Q1 2026
10	Ans will adjust the interface to clearly state that both the comment and the student's name are visible to instructors.	Before the end of Q2 2026
11	Comply with the legal transparency requirements about cookies and similar technologies.	Q1 2026
	Update complete list of cookies.	Q1 2026
12	Re-assess application logging and retention periods, together with SURF and institutions.	Q2 2026
13	Ensure that one-time passwords are restricted in scope and grant access only to the specific part of the platform necessary for their intended purpose.	Before the end of Q2 2026

14	Allow permanent deletion of all entities, including users.	Before the end of Q2 2026
	Allow users to permanently delete entities within 180-days soft-deletion period.	Before the end of Q2 2026
	Simplify the deletion model (clear split between soft-deletion (trash) and hard-deletion).	Before the end of Q2 2026
15	Replace Google Charts by a different solution (transfer the graphs visible to students).	Before the end of Q3 2026
16	Create a support page describing how controllers can fulfil a DSAR.	Before the end of Q3 2026
	Add additional buttons in the product to more easily export data of users.	Before the end of Q3 2026
17	Create security advisories section in support portal.	Q1 2026
	Establish and document internal procedures on security advisories and train staff.	Q1 2026

Introduction

This report is a data protection impact assessment (hereinafter: DPIA) on the use of the SaaS application Ans Exam by educational institutions (hereinafter: institutions), offered by Ans Exam B.V. (formerly Ans Delft). This DPIA is a central DPIA, carried out by Privacy Company on behalf of SURF, the ICT cooperative of Dutch education and research institutions, which provides institutions with a general framework for assessing data protection risks within Ans Exam.

Scope

Ans is an assessment tool used by several educational institutions. Ans is a SaaS solution. Using an API, various processes (such as importing student lists) can be automated. In addition, Ans includes the possibility of integrations with other software services. When using Ans, personal data of students, teachers, administrators and other employees involved in managing or using the assessment tool are processed.

The DPIA focuses on the SaaS solution with its API. The various applications are examined (test construction, assessment, analyses, etc.) and assessed. Integrations with other software are named but are outside the scope of this DPIA.

This DPIA assumes that the standard SURF DPA is being used. As a result, the clauses of the standard Ans DPA are not assessed. Only Schedule 1 of the Ans DPA is used as a reference.

DPIA

Article 35 of the General Data Protection Regulation (GDPR) requires organisations to carry out a Data Protection Impact Assessment (DPIA) in all cases where the processing of personal data is likely to result in high risks to the rights and freedoms of the individuals concerned (hereafter: “privacy risks”). The purpose of a DPIA is to ensure that a data controller has a clear understanding of the privacy risks associated with the intended processing and takes measures to reduce those risks to manageable levels. This is not always entirely possible. If high privacy risks remain after the proposed measures have been applied, a DPIA may lead to the conclusion that prior consultation with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens - AP) is required before the controller can begin the processing.

To determine in advance whether a DPIA is required for a specific processing activity, the cooperating data protection authorities of the European Union have established a list of nine criteria. If a processing activity meets at least two of these criteria, the risk is likely to be high. In the case of Ans, the following criteria are at least potentially applicable. Ans processes data with high frequency (daily) and on a large scale (many data subjects, criterion 5), of students and employees where there is an imbalance of power between the data subject and the controller (criterion 7).

In addition to this list of nine criteria, the AP has published its own list of seventeen types of processing for which a DPIA is mandatory. Some of the processing activities listed may be carried out by institutions through Ans, further emphasizing the necessity of a DPIA. This includes processing type 15: profiling, where the AP specifically refers to *"assessment of [...] student performance"*.

Central DPIA by SURF

This DPIA was carried out by Privacy Company, on behalf of SURF, the ICT cooperative of Dutch education and research institutions. SURF carries out compliance assessments on behalf of the institutions on suppliers that offer technological solutions within the education sector, including DPIAs. The controller for the processing operations assessed in this DPIA is therefore not SURF, but the institutions that use Ans. The DPIA is therefore a "central" or "overarching" DPIA and provides the institutions with a general framework for assessing data protection risks within Ans. In this way, the sector jointly fulfils its legal obligations.

By pooling expertise, SURF achieves cost savings and knowledge sharing and has a stronger negotiating position on behalf of the education and research sector towards suppliers with regard to taking any mitigating measures. This has the advantage for the supplier that it does not have to go through the same DPIA process with every customer and can implement measures in one go that mitigate (high) risks for the entire sector. The AP has endorsed the power of cooperation between educational and research institutions via SURF and emphasises that this contributes significantly to the protection of personal data in education and research.

This central DPIA examines how the personal data of students and employees of the institutions within Ans are processed, what agreements have been made about the processing, what risks exist and what measures can be taken to mitigate these risks. The DPIA provides a starting point but is not sufficient in itself to demonstrate that the controller complies with the GDPR. The institution must carry out their own DPIA to identify organisation-specific risks, take appropriate measures and account for the processing operations. A local DPIA provides the necessary depth and insights into specific circumstances or organisational characteristics that this central DPIA cannot provide.

Methodology

Privacy Company conducted its research using public information, the documentation about the system (as supplied by the supplier) and by analysing the possibilities via a (test) licence or licences with three different user roles: administrator, teacher (supervisor) and two participants (students).

Outline of this DPIA

Privacy Company conducted this DPIA between April and October 2025.

This DPIA uses a structure of four main divisions, which are reflected here as "parts".

A. Description of the factual data processing
B. Assessment of the lawfulness of the data processing
C. Assessment of the risks for data subjects
D. Description of mitigation measures

Part A describes the characteristics and purposes of the data processing. It also addresses the types of personal data, the data subjects, the purposes of the processing, the roles of the parties involved, the interests in the processing, the locations where the data is processed and the retention periods.

Part B assesses the bases, necessity, proportionality and compatibility of the intended processing in relation to the processing purposes. Proportionality is assessed in the light of the principles of data processing as listed in Article 5 of the GDPR, such as transparency, adequate security, privacy by design and purpose limitation. This section also assesses the legitimacy of transferring personal data to countries outside the EU and the way in which the rights of data subjects are guaranteed.

Part C describes and assesses the risks to the rights and freedoms of data subjects arising from the processing of personal data in the software/process/processing/system.

Part D describes the additional technical and organisational measures needed to reduce or eliminate the remaining privacy risks identified. Finally, this part describes whether there is a residual risk of data processing after the application of risk-reducing measures.

A separate Technical Appendix is available describing the results of the technical research.

After delivery of the draft version of Part A, Ans made several changes that improved the privacy posture of the application. Where possible, these changes have been included in the final version of Part A and the (now outdated) privacy risks have been left out of Part B-D. The technical appendix resembles the original situation, but Privacy Company performed retesting of the changes and included the results in Part A where applicable.

Part A. Description of the processing

Part A of this DPIA provides an overview of the relevant facts of the data processing operations. It describes the data processing operations, the processed personal data, and the processing purposes. In addition, Part A provides an overview of the personal data processed, the parties involved, the interests of the parties involved in the processing, and the techniques and methods of data processing. Also covered are the legal and policy framework and retention periods.

1 Ans Exam

Ans is an assessment platform developed and delivered by Ans Exam B.V since 2014. It is offered as a SaaS-solution and is in use by more than 20 educational institutions in the Netherlands. Ans allows institutions to create, deliver and grade exams, including peer-reviewed, group or paper-based exams. This chapter will describe the features of the product at a high-level and discuss the architecture and integrations. It will also touch on the hosting and security of the product.

1.1 Product features

Ans allows staff members to create questions, group these questions in assignments (exams) and publish these assignments to students. This section gives an overview of the features offered by the product.[1]

Exact feature availability depends on the license the customer obtained. Ans offers three license levels: Explore, Collaborate and Campus.[2] Apart from a higher guaranteed uptime and longer retention of results, the more advanced packages also offer specific features like single sign-on, custom domain and custom roles. Additionally, due to specific tender requirements, some customers are provided with a custom package.

1.1.1 Assignments

Assignments are the main building block of the Ans application. Staff members can create different assignment types. These types include:[3]

- Digital assignment: assignments that are created and taken online, either on location or from home. These assignments can optionally be peer-reviewed (reviewed by other students instead of by staff), self-reviewed (reviewed by the test taker themselves) or a group assignment (multiple students work on the same exam and only one of the students submits the exam).
- Written assignment: these assignments are created digitally and then answer forms can be printed. The test is made ‘offline’ on location by students after which the answer forms are digitised and uploaded to Ans for reviewing and grading.
- Hand-in assignment: an assignment type where the student is required to upload one or more files, used for assignments such as papers, essays and theses. These assignments can be group-based as well.
- Bubble sheet: an answer form for paper-based multiple-choice exams. Basically, this is a written assignment but without the exam questions or any open answers.
- Appraisal form: a form to let a staff member grade the performance of a student, for instance during a presentation or oral exam.

Assignments can be formative or summative. Summative assignments are used to evaluate how well students have understood the course material (usually resulting in a grade), whereas formative assignments are used to provide feedback to students and improve their learning of the course material.

[1] Ans – Benefits, URL: https://www.ans.app/benefits, last viewed: 15 April 2025.

[2] Ans – Pricing, URL: https://www.ans.app/pricing, last viewed: 15 April 2025.

[3] Assignment types, URL: https://support.ans.app/hc/en-us/articles/360011744017-Assignment-types, last updated: 30 July 2024.

1.1.2 Exercises and questions

Assignments in Ans consist of exercises, which in turn consist of a description and questions. Descriptions can consist of text, images, video, audio or code samples.[4] Video can be included from Ans' infrastructure or from YouTube (Google). The number of times media (audio or video) can be played back during a test can be limited (this is only possible if the media is stored on Ans' infrastructure).

Ans supports a multitude of question types, including:[5]

- Open questions, optionally limiting the number of words available to the student or starting with a pre-defined answer.
- Multiple-choice questions, with one or more correct answers. Optionally, the answers can be shuffled for every student.
- Code editor questions, where students can provide programming code as their answers.
- File upload questions, where students have to upload a file as answer to the question.
- Fill-in questions, where students have to complete phrases or sentences.
- Hotspot questions, where students have to drop markers in the correct area of an image.
- Mathematical equation questions, where students answer by providing a mathematical equation.
- Order questions, where students have to put several answers in the correct order.

More question types are available, including some types that are still offered as beta features (spreadsheet, statement and drawing questions).

Exercises can be stored in 'question banks', containing a collection of exercises belonging to the same subject, field of education or study.[6] This allows for easy reuse of exercises.

1.1.3 Assignment taking

Once an assignment has been prepared, it can be scheduled for taking.[7] Assignments can be scheduled for all learners, all learners that have the 'extra time' property set, a specific group or a specific class. Taking an assignment can be locked to a specific location (based on IP-address), require an access code, and restrict access to other pages in the application.[8] There are also several integrations available to ensure a secure testing environment, see Section 1.3.

[4] Overview of description types, URL: https://support.ans.app/hc/en-us/articles/360016757277-Overview-of-description-types, last updated: 8 August 2024.

[5] Overview of question types, URL: https://support.ans.app/hc/en-us/articles/360016757257-Overview-of-question-types, last updated: 30 July 2024.

[6] Manage question banks, URL: https://support.ans.app/hc/en-us/articles/360027181474-Manage-question-banks, last updated: 11 October 2024.

[7] Scheduling an assignment, URL: https://support.ans.app/hc/en-us/articles/360011856558-Schedule-an-assignment, last updated: 8 November 2024.

[8] Secure a digital test, URL: https://support.ans.app/hc/en-us/articles/360011857418-Secure-a-digital-test, last updated: 30 December 2024.

When a digital test is active, instructors and invigilators can monitor progress of the participants using a dashboard in Ans.[9] This dashboard shows the participants that still have to start, have started and have completed the test. For all participants together, the progress within the exercises of the test is visible as a percentage. The location where the test is taken is also visible (either an in Ans pre-defined location or an approximate location based on the IP-address of the user). Staff can generate a one-time password for a student, bypassing their user account password or SSO for the test.

Update after completion of Part A

In response to the full draft of this DPIA, Ans stopped showing the approximate location based on the IP-address of the user in the progress dashboard with the release of 7 December 2025. [10]

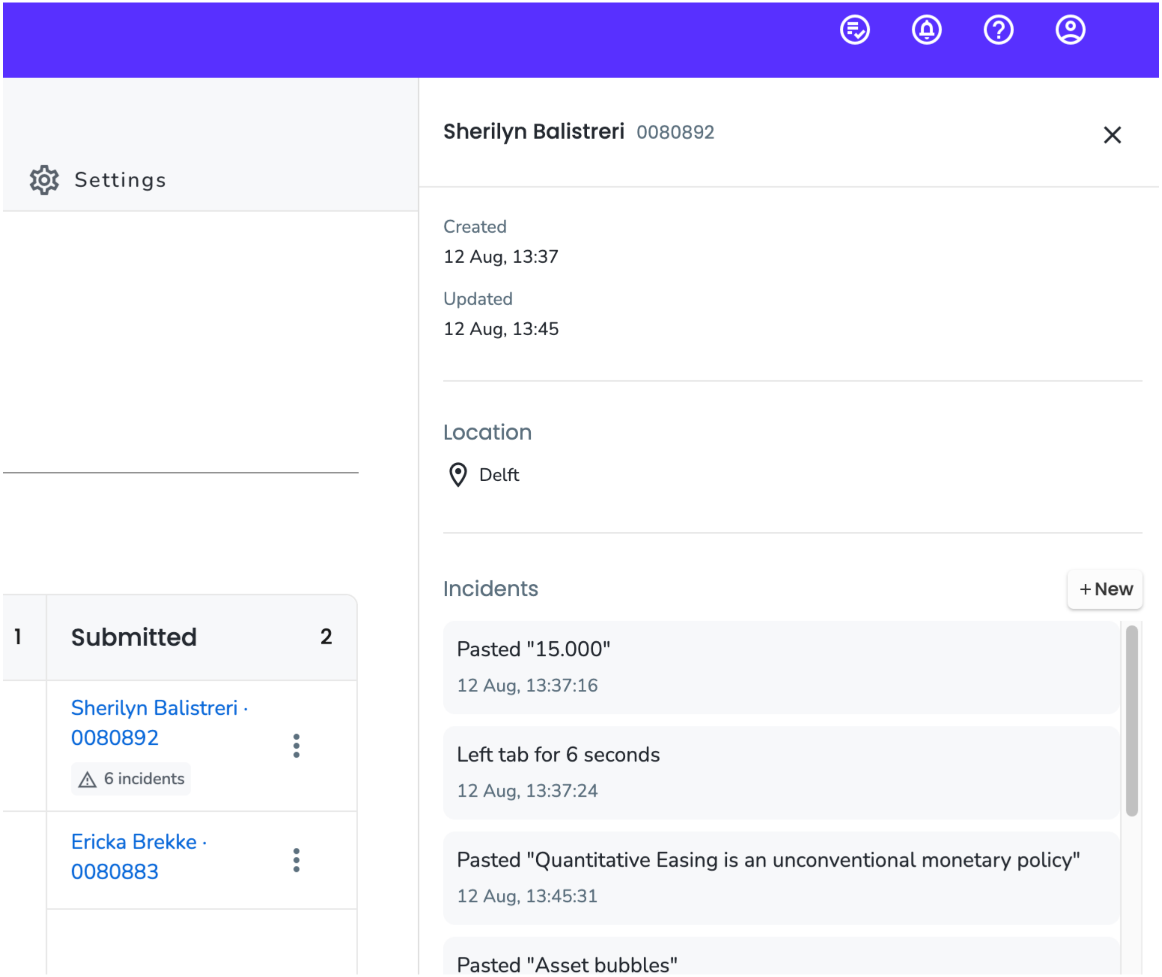
During tests, Ans can monitor for users leaving the browser tab or copy-pasting contents into the test. These are reported as incidents on the test overview page (see Figure 1).[11] Incidents can also be reported by instructors or invigilators manually and added to the overview.

[9] Monitor the progress during a digital test, URL: https://support.ans.app/hc/en-us/articles/360032438894-Monitor-the-progress-during-a-digital-test, last updated: 1 April 2025.

[10] Feedback Ans 1 December 2025.

[11] Add proctoring settings to your digital test, URL: https://support.ans.app/hc/en-us/articles/27332580148241-Add-proctoring-settings-to-your-digital-test, last updated: 13 August 204.

Figure 1: Incidents reported in Ans interface during test taking



Settings

1 Submitted 2

Sherilyn Balistreri · 0080892
6 incidents

Ericka Brekke · 0080883

Sherilyn Balistreri 0080892

Created
12 Aug, 13:37

Updated
12 Aug, 13:45

Location
Delft

Incidents
+ New

Pasted "15.000"
12 Aug, 13:37:16

Left tab for 6 seconds
12 Aug, 13:37:24

Pasted "Quantitative Easing is an unconventional monetary policy"
12 Aug, 13:45:31

Pasted "Asset bubbles"

Instructors and invigilators can send announcements to participants during an assignment. If live chat is enabled for the assignment, participants can send questions to staff or respond to announcements in a one-on-one chat. In group assignments, chat history will be visible for the whole group.

In the assignment settings, instructors can enable a calculator (basic or scientific) or digital notebook for use during the test.[12] The contents of the notebook are not visible for staff members. The browser's built-in spell check functionality can also be controlled. For closed-questions, immediate feedback as soon as the student answers a question can be automatically provided.

1.1.4 Grading, feedback and student interactions

Ans offers staff members a way to digitally review exam questions, grading them using one of three grading methods: (1) points per criterion, (2) a slider or (3) a rubric with levels.[13] Reviewing can be divided by different staff members, where optionally staff can be assigned

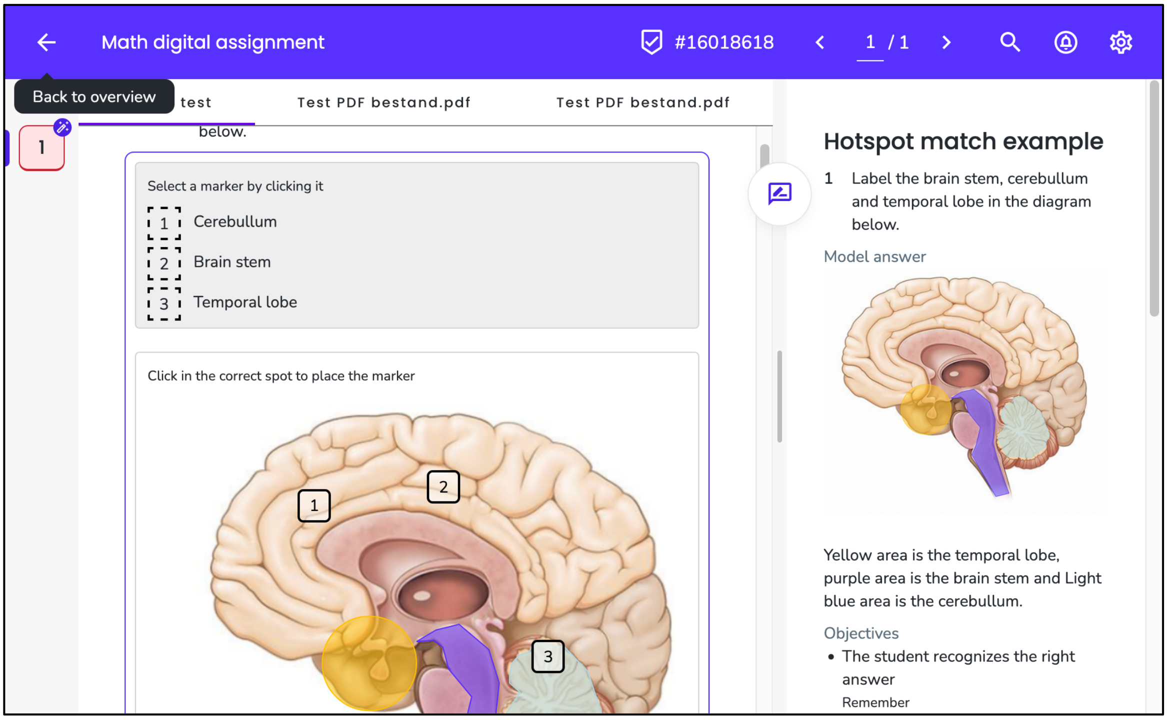
[12] Add accessibility options to your digital test, URL: https://support.ans.app/hc/en-us/articles/6003838086033-Add-accessibility-options-to-your-digital-test, last updated: 9 August 2024.

[13] Start reviewing, URL: https://support.ans.app/hc/en-us/articles/360033652094-Start-reviewing, last updated: 9 April 2025.

to specific exercises or groups of users. Staff members can leave comments while grading or can leave annotations on specific places in the answer of the student. They can also flag an answer to another colleague if they are unsure about grading a question.

By default, anonymous grading is enabled. This means that during reviewing, staff members do not see the name or student number of the student they are reviewing (see Figure 2). If a user has the role of reviewer in the course, they will not be able to see student details by visiting other pages in Ans. This is different for instructors, that can click on the result number in the review dialog and then immediately see all student details (see Figure 3).

Figure 2: Screen shown to reviewer during anonymous grading



below.

Select a marker by clicking it

1 Cerebullum

2 Brain stem

3 Temporal lobe

Click in the correct spot to place the marker

Hotspot match example

1 Label the brain stem, cerebullum and temporal lobe in the diagram below.

Model answer

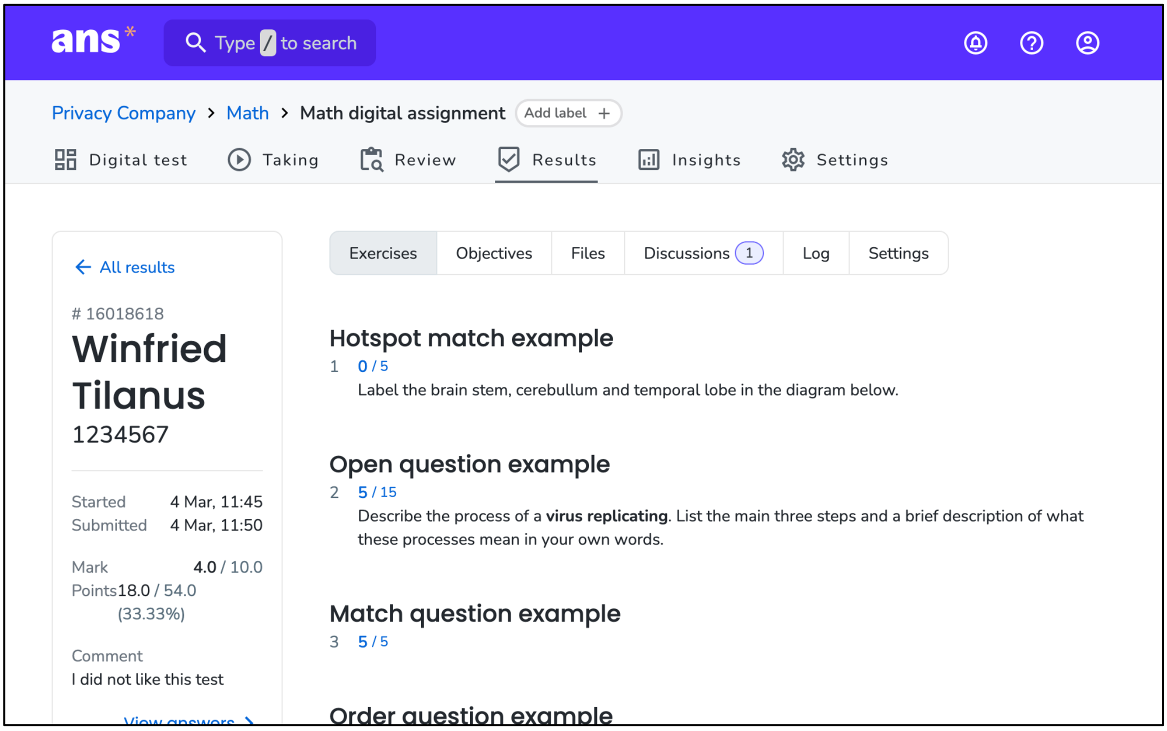
Yellow area is the temporal lobe, purple area is the brain stem and Light blue area is the cerebullum.

Objectives

- The student recognizes the right answer

Remember

Figure 3: Student details shown to instructor after clicking on the result number during reviewing



16018618

Winfried Tilanus

1234567

Started	4 Mar, 11:45
Submitted	4 Mar, 11:50
Mark	4.0 / 10.0
Points	18.0 / 54.0 (33.33%)

Comment

I did not like this test

Hotspot match example

1 0 / 5

Label the brain stem, cerebullum and temporal lobe in the diagram below.

Open question example

2 5 / 15

Describe the process of a **virus replicating**. List the main three steps and a brief description of what these processes mean in your own words.

Match question example

3 5 / 5

Order question example

Closed-ended questions, like multiple-choice or order questions, can be automatically graded by the software. For these questions, the staff member does not have to review the questions. Optionally, the staff member can however view the answer and change the grading.

In case of written assignments made on paper, scans of the answers can be uploaded to Ans and are automatically recognised using a QR-code.[14] After uploading, the scans are assigned to the correct student automatically (based on the student number filled in by the student) and the answers can be reviewed digitally in the same way as any other exam.

Ans can automatically calculate the mark of a test, using a formula or a pre-defined table with grades.[15] Rounding or a guess correction can optionally be applied when calculating the mark. Optionally, results of students can be approved or disapproved by an instructor.[16] Unmarked or approved results are displayed to students (when the result is published), disapproved results are not displayed to students.

After reviewing, the exam results can be published to students digitally.[17] Publication can be limited to a specific timeframe and depending on the wishes of the institution the mark,

[14] Upload & process your scans, URL: https://support.ans.app/hc/en-us/articles/360027215333-Upload-process-your-scans, last updated: 2 March 2025.

[15] Calculate a mark, URL: https://support.ans.app/hc/en-us/articles/360032871713-Calculate-a-mark, last updated: 26 February 2025.

[16] Approve, disapprove, remove or restore results, URL: https://support.ans.app/hc/en-us/articles/360013431397-Approve-disapprove-remove-or-restore-results, last updated: 18 March 2025.

[17] Publish results, URL: https://support.ans.app/hc/en-us/articles/360027351093-Publish-results, last updated: 24 March 2025.

points scored, questions and answers can be displayed. Optionally, students can start discussions to ask questions about the grading, which can be answered by staff members. Publication can also be limited to specific locations.

Staff members can export results (mark, points per question or points per criterion) from the results overview page.[18] This export can then be used to enter information into other systems, like a student information system (SIS). Results can also be archived, making them read-only.[19]

Results can also be synchronised to a SIS through a custom API-integration. For learning management systems (LMS) Ans offers standard integrations based on LTI version 1.3 to synchronise grades to these systems. See Section 1.3 for more details on these integrations.

1.1.5 Data-driven analysis

Ans offers staff members further insights into tests on multiple levels. Insights are split between assignments, questions, objectives and reviewer alignment. These insights are also available on question-level if a question is part of a question bank.

On assignment level, insight is given into:[20]

- Characteristics of the test: the number of assignments, maximum number of points, maximum score obtainable by guessing and whether assignments were randomly generated.
- Metrics of the test: number of participants, pass rate and reliability metrics (KR-20, standard deviation, standard measurement error).
- Obtained marks: minimum, maximum, average and median marks and a graphical view of obtained results.
- Obtained points: minimum, maximum, average and median number of points and a graphical view of the obtained points on student-level.
- Duration: minimum, maximum, average and median time participants took to complete the test and a graphical view of the test duration on student-level.

Per question, insight is given into:[21]

- Quality indicators: these insights consist of various statistical indicators (e.g., P-value, Rit-value, Rir-value), combined with an overall quality indication of the question and the average duration it took participants to finish the question.
- Group comparison: if the course consists of multiple groups of students, the differences between groups can be analysed.
- Rank correlation: a graphical view showing the obtained score versus the total test score.

[18] Export results, URL: https://support.ans.app/hc/en-us/articles/360036410294-Export-results, last updated: 27 March 2025.

[19] Archiving results, URL: https://support.ans.app/hc/en-us/articles/10875494502289-Archiving-results, last updated: 31 October 2025.

[20] Assignment insights, URL: https://support.ans.app/hc/en-us/articles/360027349673-Assignment-insights, last updated: 25 March 2025.

[21] Question insights, URL: https://support.ans.app/hc/en-us/articles/360027234814-Question-insights, last updated: 28 January 2025.

- Grading scheme breakdown: this shows how the grades on the question were obtained, given the grading scheme. Exact information depends on the type of grading scheme.

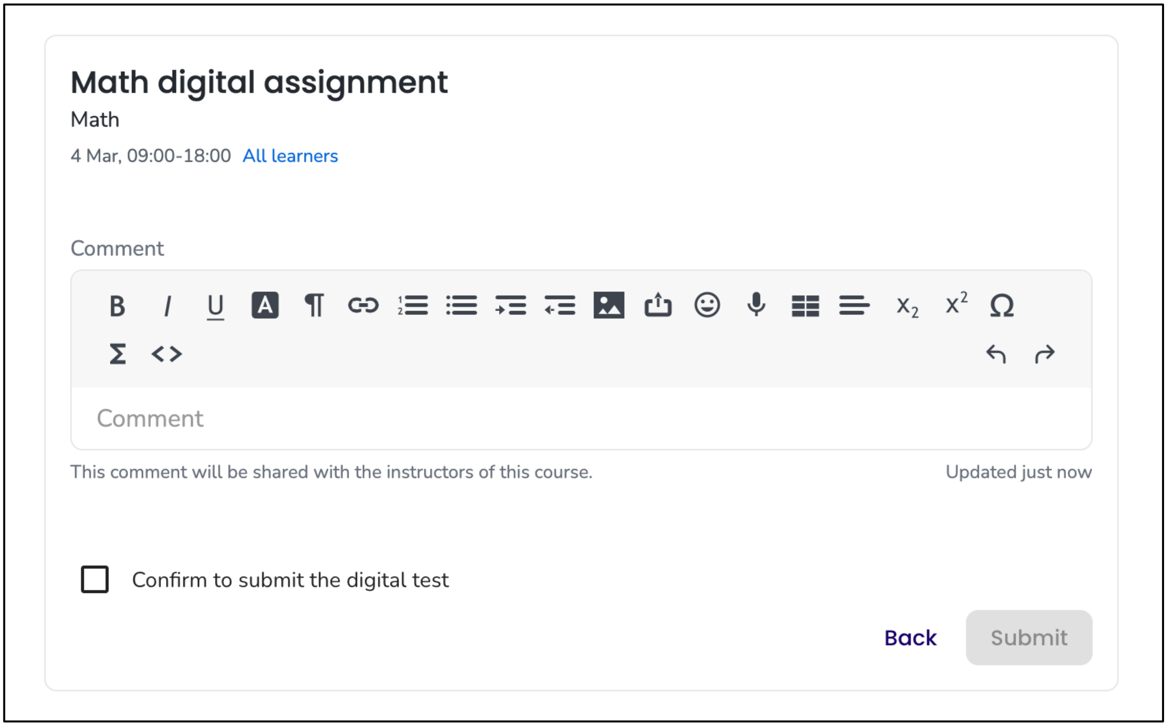
A course can define one or more domains with one of more objectives as learning goals. Questions can be tied to these objectives. If this has been done, the objectives insights will show for each objective the number of students that obtained that objective (in 10% intervals).[22]

Reviewer alignment shows for each question:[23]

- The alignment of grading between different reviewers: good, deviation or needs attention.
- The total number of results, duration of grading and average number of points given.
- A breakdown per reviewing staff member, showing the number of results reviewed, the time spent reviewing, and the average number of points given.

Optionally, students can provide feedback on an assignment at the end of the assignment (see Figure 4). These comments are shown to the staff member, providing a link to the test result of the student, showing student details.

Figure 4: Test submission dialog shown to student, with option to comment on the test



Math digital assignment

Math

4 Mar, 09:00-18:00 All learners

Comment

This comment will be shared with the instructors of this course.

Updated just now

□ Confirm to submit the digital test

On an organisation-level, administrators can see:[24]

[22] Objectives insights, URL: https://support.ans.app/hc/en-us/articles/360027235814-Objectives-insights, last updated: 20 January 2023.

[23] Alignment insights, URL: https://support.ans.app/hc/en-us/articles/360016943257-Alignment-insights, last updated: 29 July 2024.

[24] Insights in the use of Ans on school level, URL: https://support.ans.app/hc/en-us/articles/360018836637-Insights-in-the-use-of-Ans-on-school-level, last updated: 22 November 2024.

- Number of active users per month.
- Daily logins of students and employees and a list of all individual failed login attempts (showing user, date and time, browser, OS and IP-address).
- Amount of (actual or expected) taken assignments per day, optionally filtered by department. Similar information is also available in a calendar view.
- A summary of assignment insights for all assignments, optionally filtered by year or study.

1.1.6 Accessibility

For accessibility purposes, participants in a test can enable a large font mode (font size 13.5 instead of 10.5), dyslexia mode (font set to Arial) or high contrast mode.[25] Ans supports alternative texts for images and can make recommendations when such a text is missing or if text with a low contrast is present.[26] With regards to the Web Content Accessibility Guidelines, Ans states that:[27]

> *"Ans is compliant with WCAG 2.1 A criteria, the majority of AA criteria, and several AAA criteria."*

1.2 User management

1.2.1 User creation and deletion

Users in Ans can be created in several ways:

- Administrators can invite individual users (students or staff) using the Ans web interface.[28]
- Administrators can import students in bulk by uploading a CSV- or Excel-file in the Ans web interface.
- Users can be created through the API (see Section 1.3).[29]
- Users can be automatically created when they login through single sign-on for the first time.[30]
- Users can be automatically created when they login through an LTI link (from an LMS) for the first time.[31]

[25] How to take a digital test, URL: https://support.ans.app/hc/en-us/articles/360010815157-How-to-take-a-digital-test, last updated: 11 April 2025.

[26] Accessibility suggestions in a digital test, URL: https://support.ans.app/hc/en-us/articles/360018497077-Accessibility-suggestions-in-a-digital-test, last updated: 16 July 2024.

[27] Ans WCAG 2.1 Compliance report, URL: https://support.ans.app/hc/en-us/articles/4518991389073-Ans-WCAG-2-1-Compliance-report, last updated: 10 August 2023.

[28] Manage student accounts, URL: https://support.ans.app/hc/en-us/articles/360027344093-Manage-student-accounts, last updated: 15 April 2025.

[29] Use the API to manage users, URL: https://support.ans.app/hc/en-us/articles/4405142363793-Use-the-API-to-manage-users, last updated: 4 September 2024.

[30] Single Sign-On (SSO), URL: https://support.ans.app/hc/en-us/articles/4405556708625-Single-Sign-On-SSO, last updated: 2 March 2025.

[31] General LTI 1.3 documentation: user management, URL: https://support.ans.app/hc/en-us/articles/12232961337105-General-LTI-1-3-documentation-user-management, last updated: 16 July 2024.

- Users can be automatically created by the LMS synchronisation (beta).[32]
- Users can be automatically created when they take a written (paper-based) assignment, and the results of that assignment are uploaded. An administrator can then add the remaining details of these students using the ‘Enrich students’ option.[33]

When students are invited by an administrator, they receive an invitation email to set their password. This invitation email is not sent if the organisation forces the use of single sign-on, as in that case there is no need to set a password.

User accounts contain a name and email address. Students accounts also require a student number. Student numbers have a fixed length configured in the organisation’s settings (shorter student numbers are prefixed with zeros).

Users can be removed by an administrator in the web interface and through the API. In this case, the user attributes (except for the student number) are cleared and for student users the results are also soft deleted. For more information on data retention see Section 10.3.

Students can be marked as alumnus by an administrator, hiding them from the user overview. This does not disable or delete the account. Marking a student as alumnus allows re-use of the user’s email address by another user (in case a new student starts studying and gets assigned the same email address).

Users can be blocked by an administrator. This disallows log in by the user until the account is unblocked but does not remove any information.

Administrators can assume the identity of another user (impersonating them) through a button in the user’s settings. All actions performed from that moment on are performed as if they were done by the impersonated user.

1.2.2 User roles and privileges

By default, Ans offers permissions on three levels: school, course and question bank.[34] Every level has standard roles, pre-defined by Ans. Customers on the ‘Campus’ plan can optionally choose to customise these roles.[35] Custom roles have not been tested as part of this DPIA.

At school level, the following roles are available:

- Administrator: can perform all actions available in the application, including changing school settings, modifying users and viewing all logs.

[32] Synchronise course learners with your LMS (beta), URL: https://support.ans.app/hc/en-us/articles/33611507871377-Synchronise-course-learners-with-your-LMS-beta, last updated: 27 March 2025.

[33] Enrich students, URL: https://support.ans.app/hc/en-us/articles/9640600491921-Enrich-students, last updated: 22 June 2023.

[34] Roles and permissions in Ans, URL: https://support.ans.app/hc/en-us/articles/360015947097-Roles-and-permissions-in-Ans, last updated: 2 March 2025.

[35] Custom roles [Campus], URL: https://support.ans.app/hc/en-us/articles/360020926877-Custom-roles-Campus, last updated: 19 March 2025.

- Department administrator: similar to the administrator level but scoped to a specific department. Only content, users and question banks within that department can be modified by these users.
- Repro: can print and upload scans for paper exams.
- Staff: can create, view, modify and delete content in a course, depending on their role in the course. Specific permissions also depend on the employee privileges configured (see below).
- Student: can view their assigned courses and publications and take and submit their assignments. A student can optionally receive additional permissions in a course, for instance as a teaching assistant. Specific permissions also depend on the student privileges configures (see below).

At course level, the following roles are available:[36]

- Instructor: full access and control over a course. The user can invite colleagues, assign roles, and allocate members to specific questions or groups. This role is assigned by default if a staff member creates a course.
- Invigilator: can monitor the taking-session of a digital test, view the results page, add timeslots and add students to the course or groups. Cannot see the contents of a test, but attachments are visible.
- Reviewer: can review exercises of participants that they have been assigned to. Reviewers can also be assigned to certain groups.
- Learner: can participate in assignments within their courses. A learner sees the courses and assignments that are allocated to them. A learner is able to participate in an assignment once a timeslot has been created. Staff members can also be assigned the role 'learner' for a certain course. Can see their own result of an assignment when published.

At question bank level, the following roles are available:[37]

- Publisher: has all permissions within a question bank. Can create exercises, assignments, domains and objectives. Can add contributors and edit the question bank settings.
- Author: can create and add new exercises to the question bank.

Some additional settings are available to configure employee and student privileges. All these privileges are enabled by default unless otherwise noted. The setting available for employees are:[38]

- Account management: editing profile, editing email.
- Course management: creating courses, removing courses.
- Assignment management: creating assignments, removing assignments.
- Question bank management: creating question banks, removing question banks.

[36] Manage course users, URL: https://support.ans.app/hc/en-us/articles/360012081058-Manage-course-users, last updated: 18 March 2025.

[37] Manage question bank users, URL: https://support.ans.app/hc/en-us/articles/360016142258-Manage-question-bank-users, last updated: 15 April 2025.

[38] Employee privileges, URL: https://support.ans.app/hc/en-us/articles/360027229454-Employee-privileges, last updated: 12 December 2024.

- Repro management: printing exams (disabled by default), uploading scans.

For students the following settings are available:[39]

- Account management: editing profile, editing email.
- Course management: allow students as a reviewer of a course, allow students as an invigilator of a course, allow students as an instructor of a course.
- Question bank management: allow students as an author of a question bank, allow students as a publisher of a question bank.

1.2.3 Authentication and single sign-on

Users can authenticate with an email address and password for locally created Ans accounts. Staff members can enable two-factor authentication on their account (using TOTP) and administrators can require two-factor authentication for all staff members in the organisation.[40]

Ans also supports authenticating with Microsoft and Google accounts. In this case, the user already needs to exist in Ans and is matched on email address. Two-factor authentication is still applied by Ans if the user has this enabled. During testing, Privacy Company found a security issue where these integrations allowed logins by users that did not actually control the corresponding user account. This issue was reported to Ans on 17 April 2025, and a temporary fix was deployed on 20 April 2025. Additional verifications were added on 22 June 2025 after informing users of changes to the login process. Ans informed users they 'had not been made aware of any instances when illegitimate login has taken place'.[41] Ans confirmed that only limited logging information on the issue was available, thus illegitimate login could not be ruled out.[42]

Ans communicated the changes in June as an 'important change', stating that a potential security issue was resolved "if the email is reused by a different user". This did not cover the full scope of the security issue, which allowed for arbitrary user authentication.

Ans supports single sign-on using SURFconext, eduGAIN or a custom SAML authentication provider (beta). It can require a Level of Assurance from SURFconext, requiring two-factor authentication on the SURFconext side through SURFsecureID.

Single sign-on can be enforced, disallowing authentication with local accounts or the standard Microsoft/Google login options. If the education institution sets up a custom domain (e.g., ans.university.com, available in the 'Campus' package), users will be automatically redirected to the SSO-endpoint to authenticate, skipped the Ans sign-in page.[43] This functionality also allows sending emails from the customer's domain.

[39] Student privileges, URL: https://support.ans.app/hc/en-us/articles/360011862858-Student-privileges, last updated: 24 January 2023.

[40] Authentication, URL: https://support.ans.app/hc/en-us/articles/32828302964497-Authentication, last updated: 10 March 2025.

[41] 22nd of June 2025 - Changes to signing into the platform via Microsoft or Google, URL: https://support.ans.app/hc/en-us/articles/35748764619793-22nd-of-June-2025-Changes-to-signing-into-the-platform-via-Microsoft-or-Google, last updated: 30 May 2025.

[42] Confirmed during a meeting between SURF and Ans, 31 October 2025.

[43] Custom domain [Campus], URL: https://support.ans.app/hc/en-us/articles/16632996288913-Custom-domain-Campus, last updated: 3 February 2025.

1.3 API and integrations

Ans offers an API allowing institutions to build integrations, for instance with a student information system (SIS). On top of that, Ans features several standard integrations with software used in the educational sector.

1.3.1 API and webhooks

Ans offers a REST-based API that allows retrieving, creating, updating and deleting all entities available within the data model (see Section 1.6).[44] This integration can be used by institutions to automatically create users, courses, assignments and other information in Ans, based on the data in a student information system or similar applications. API documentation is provided in the OpenAPI format.[45] Various entities in the API provide an 'external_id' field. This field can be set through the API (for instance to keep track of the identifier in the source system) but is not used by Ans or surfaced in the web-interface.

The API is authenticated by a token which can be generated by a user. The token is tied to the user and any actions performed through the API are logged as if the user had performed them through the web-interface. The API also supports the OAuth v2 protocol for authentication, but this is only used for integrations.

Webhooks are also supported.[46] These can send an update to a configured web address when something changes in Ans (create, update or delete). These updates are currently only provided for assignments, results and users.

The API and webhooks are only available to employees and administrators. Access to the API is scoped to the access permissions of the user that created the API-token. Webhooks were sent out without this scoping, which allowed employees to receive (but not update) data for assignments, results and users that do not have access to through the API or web-interface. Privacy Company reported this issue to Ans on 21 April 2025 and a fix was deployed on 18 May 2025.[47] Apart from mentioning the change in the release notes, no communication to customers about this issue was done.

1.3.2 Integrations

Ans offers standard integrations with various software products used in the educational sector.[48] These integrations can be divided in several categories:

- Learning Management Systems: integrations based on LTI version 1.3 with Brightspace, Blackboard, Canvas and Moodle. The integrations make it possible to sign-in students directly from the LMS (a user will be created if necessary). After the test, results can be sent back to the LMS. Synchronising the list of learners to a group in Ans is a newer feature, currently in beta.

[44] What is the API, URL: https://support.ans.app/hc/en-us/articles/4411562026769-What-is-the-API, last updated: 13 December 2024.

[45] API V2, URL: https://ans.app/api/docs/index.html, last viewed: 20 April 2025.

[46] Webhooks, URL: https://support.ans.app/hc/en-us/articles/4411732636561-Webhooks, last updated: 16 January 2024.

[47] 18th of May 2025 (patch release), URL: https://support.ans.app/hc/en-us/articles/35326441661969-18th-of-May-2025-patch-release, last updated: 19 May 2025.

[48] Integrations, URL: https://support.ans.app/hc/en-us/articles/9143558126481-Integrations, last updated: 16 January 2024.

- Lockdown browser software: integrations with Safe Exam Browser, Schoolyear and Secure Test Environment Protocol (STEP). These browsers are 'locked down' to only allow specific actions during test taking. With the integration, it is possible to configure the settings of these browsers from the Ans software.
- Plagiarism detection software: integrations with Turnitin and Ouriginal. Submissions by students in digital or hand-in assignments are automatically submitted to these parties to detect plagiarism. The 'similarity score' is shown in Ans and staff members can click through to the third-party system.
- Print to scan and educational logistics software: integrations with Canon and Rijnja. These integrations allow staff members to order printed versions of the written assignments and have them scanned and delivered to Ans after taking.
- Proctoring software: integrations with ProctorExam and Proctorio. These software solutions are used for remote proctoring of exams. Ans allows to configure the settings of this software for an assignment and offers links to the recordings of the assignments after it has been taken.
- Text-to-speech software: integration with Readspeaker. When enabled, this software is directly included in the webpage the student views. It gives the student the option to read text out loud.

Only administrators can configure integrations, after which employees can enable them for specific assignments (where applicable).

The personal data exchanged when using the integrations differs per platform and is not always visible from the documentation. In most cases, at least basic student data (name and student number) is exchanged. In some cases, exam answers (e.g., in case of plagiarism software) or grades (e.g., in case of LMS integrations), may be exchanged. The assessment of the applications is out of scope of this DPIA.

1.4 Architecture, hosting and security

Ans is a multi-tenant (i.e. one application for all institutions) web application available through the domain https://ans.app. A separate staging environment is available for customers on the 'Campus' plan and on customer request Ans can create an education or sandbox environment for a customer.[49]

The Ans application is primarily hosted on Amazon Web Services and distributed over three availability zones for redundancy.[50] Cloudflare services are used for DDoS mitigation. TransIP (formerly known as CloudVPS) is used for file storage. Passwords are hashed using bcrypt and data is encrypted in transit and at rest using AES-256.

For the main application, the following hosts should (at least) be whitelisted:[51]

- ans.app

[49] Ans – Pricing, URL: https://www.ans.app/pricing, last viewed: 15 April 2025; Implementation process, URL: https://support.ans.app/hc/en-us/articles/4570721838993-Implementation-process, last updated: 15 January 2025.

[50] Ans – Security, URL: https://www.ans.app/security, last viewed: 21 April 2025.

[51] Which URLs should you whitelist, URL: https://support.ans.app/hc/en-us/articles/360039525534-Which-URLs-should-you-whitelist, last updated: 23 July 2024.

- assets.ans.app
- media.ans.app
- files.ans.app (for future use)
- d7e0acfd15964dc2a2412dbfcdebc202.objectstore.eu

Ans regularly sends notification emails to users (e.g., when a test has been submitted or when a grade is available) through Amazon SES. These emails contain a tracking pixel to track when a user views the email (see Section 3.3.12 of the Technical Appendix). This information is then surfaced in the user's email log (see Section 1.5).

Additionally, emails are sent to staff members notifying them of product updates, important changes and to request feedback through Mailerlite. Users can unsubscribe from some of these emails (updates and feedback requests) through a link in the email. These emails contain open and link tracking, tracking when the user views the email or clicks on a link in the email (see Section 3.3.26 of the Technical Appendix). Ans confirmed that this information is used to improve the quality of the emails.[52]

Update after completion of Part A

In response to the draft of Part A of this DPIA, Ans has disabled the tracking features in their service emails by changing the configuration of Mailerlite.

Ans is ISO27001:2017 certified since 2022.[53] All Annex A controls have been implemented except for '11.1.6 Delivery and loading areas' (presumably this is left to the data centre suppliers). Additionally, Ans uses third-party security tools to continuously scan for vulnerabilities and engages third parties for penetration testing of the application and infrastructure.

Database backups are created daily and stored on a hard disk of a different server in a different location.[54] These backups are retained for four weeks. Files uploaded via the platform are stored inside an 'Object Store', which automatically replicates the data in three places of which at least one replica is stored inside another data center at least 5 kilometers away from the original data. Ans tests recovery procedures (restoring data from backup copies) annually to ensure that they can be relied on in an emergency or disaster situation.

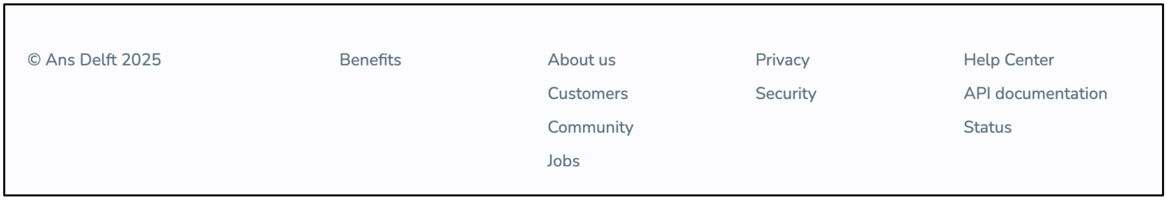
Ans uses several additional tools to deliver their services. These are linked from the footer of the application (see Figure 5).

[52] Feedback Ans 28 May 2025.

[53] Compliance, URL: https://support.ans.app/hc/en-us/articles/17885586401809-Compliance, last updated: 2 January 2024.

[54] Service level agreement (SLA), URL: https://support.ans.app/hc/en-us/articles/12661391857809-Service-level-agreement-SLA, last updated: 19 December 2023.

Figure 5: Footer of the Ans application



© Ans Delft 2025

Benefits

About us
Customers
Community
Jobs

Privacy
Security

Help Center
API documentation
Status

The help center is provided by Zendesk and available at https://support.ans.app. The status website is provided by SorryApp and available at https://status.ans.app. The links to privacy and security information point to Ans' corporate website (hosted by Webflow), available at https://www.ans.app.

Internally, Ans uses Redash[55] to analyse customer data (through the Ans API) for product improvement. Ans self-hosts Redash. The data is only used internally.[56]

1.5 Logging

The Ans application keeps track of changes users make and surfaces these in various log files. The following log files are available:

- School log: contains changes to the school settings (incl. authentication and review defaults), course creations and deletions and question bank creations and deletions.[57]
- User log: contains creation of the user, changes to the user's settings or role and generating a one-time password.[58]
- User email log: contains subjects of emails sent by Ans and the date/time the email was delivered and opened.
- User login history: contains date/time of the logins of the user, including IP-address and browser/OS used. Users can see this information in their own profile as well.
- Course log: contains changes to the course information and settings, creation and changes in assignments, and instructor changes.[59]
- Assignment log: contains changes to the assignment, including changes to the underlying exercises and questions. Some changes can be undone using a 'Restore'-button.[60]
- Result log: contains information on when a student started and submitted an assignment, as well as when they viewed and answered individual questions. Also includes reviewing activity by staff members, and administrative actions performed on the result. For student activity it contains the last two octets of the user's IP-address.[61]

[55] Redash helps you make sense of your data, URL: https://redash.io/, last viewed: 21 April 2025.

[56] Feedback Ans 28 May 2025.

[57] School log, URL: https://support.ans.app/hc/en-us/articles/9912883379089-School-log, last updated: 15 August 2024.

[58] User log, URL: https://support.ans.app/hc/en-us/articles/20756880740241-User-log, last updated: 2 August 2024.

[59] Course log, URL: https://support.ans.app/hc/en-us/articles/12414031959697-Course-log, last updated: 20 August 2024.

[60] Assignment log, URL: https://support.ans.app/hc/en-us/articles/9683336163217-Assignment-log, last updated: 12 February 2025.

[61] Result log, URL: https://support.ans.app/hc/en-us/articles/360015845237-Result-log, last updated: 2 August 2024.

- Question bank log: contains changes to the details of the question bank and added/removed users. Also contains information similar to the assignment log, including logs per individual exercise and question in the question bank.[62]

All the log entries contain the name of the user performing the change, the date/time the change was performed and, where applicable, the old and the new value of the configuration setting. The logs do not link to the individual user profile, which may make it more difficult to locate the exact user if multiple users with the same name exist.

Internally, Ans has some additional logs available (like the IP-address and role of the user, and more actions in the school and course logs), but these are currently not surfaced in the web interface.[63]

When an administrator assumes identity of another user, all actions are logged as being performed by the impersonated user, without mentioning that impersonation was used. The start of assuming the identity of another user is not shown in the interface. Ans has confirmed that impersonating an account is logged, but that the information is not (yet) shown in the interface.[64]

All logs can be viewed by administrators. Department administrators can view logs for entities in their own department. Additionally, instructors can view the user log and user email log of students in their courses. They can also view the course, assignment and result logs if they are an instructor in the course. Invigilators or reviewers cannot view the logs. The question bank log is visible to users with access to the question bank.

The log files cannot be exported (e.g., to a CSV- or PDF-file). Users can opt to print the log file page, but to see all the information in the logs on the print they would first have to click on all changes to show the old and new value.

Amazon Cloudwatch is used for internal application logging, only available to Ans employees. These logs contain the user identifier, IP-address, request URL, content data (exam answers, notes, discussions) and timing information (time it took to answer or grade a question). For more details, see Section 4.2.3 of the Technical Appendix.

AppSignal is used to log internal application warning and errors. These logs mostly contain technical information (e.g., name of script that generated the error and error message) and only limited personal data is sent to AppSignal (the user's IP-address and limited browser information). See Section 3.3.15 of the Technical Appendix for more details.

Cloudflare logged some browser timing information as part of their 'real user monitoring' services. This information consisted of the visited URL and how fast pages were loaded or rendered by the user's browser. Ans indicated that this data was not used and turned off the functionality at the end of May 2025.[65]

[62] Question bank log, URL: https://support.ans.app/hc/en-us/articles/12414069933585-Question-bank-log, last updated: 15 August 2024.

[63] Feedback Ans 28 May 2025.

[64] Feedback Ans 28 May 2025.

[65] Feedback Ans 28 May 2025, verified by Privacy Company on 23 June 2025.

1.6 Data model Ans

Ans offers UML diagrams of their data model on their website, listing all entities and their relationships.[66] In this section a simplified overview of this data model will be given, highlighting the most important entities.

The root entity of an Ans organisation is a school. A school consists of:

- Departments (e.g., a faculty of a university)
- Users (e.g., staff member or student)
- Courses (usually a specific course, like 'Math', in a specific school year)
- Classes (a grouping of students taking part in a set of courses)
- Periods (a school year)

In turn:

- A department has one or more studies, consisting of one or more courses.
- Users can be members of courses and/or classes.
- Users can also be divided into groups within a course.
- Courses belong to a period.

Once this structure has been defined, the tests can be created. These are modelled as assignments, where every assignment:

- Belongs to a specific course.
- Consist of one or more exercises, which contain one or more questions.
- Can be scheduled for taking during one or more timeslots.
- Can be scheduled for publication during one or more timeslots.

When a student takes an assignment, submissions are created for every question. These are grouped into a result which is then reviewed and graded.

The Ans documentation also contains an UML for question banks. As questions banks only process minimal personal data (e.g., only question (bank) author and role), these are not further considered in this section.

[66] Datamodel Ans, URL: https://support.ans.app/hc/en-us/articles/13992142037777-Datamodel-Ans, last updated: 22 June 2023.

2 Personal Data and Data Subjects

When examining the privacy risks of a data processing operation, it is important to consider what types of data of which groups of data subjects are being processed. This chapter provides an overview of all types of data from the various groups of data subjects.

2.1 Categories of data subjects

The categories of data subjects whose personal data is processed through Ans are:

- Students of the institution
  - Regular students (government-funded)
  - Contract students (non-funded)
  - Alumni
- Personnel of the institution
  - Administrators
  - Teachers / Professors
  - Reviewers (teaching assistants)
  - Invigilators (supervisors)

As the scope of this report is limited to universities and universities of applied sciences, it is highly unlikely that personal data of children under 16 would be processed in this context. Such instances would be rare.

2.2 Categories of personal data

The table below lists the personal data that are listed in Schedule 1 of the Ans DPA. *"Personal data of users of the Service are processed. This concerns in particular:"*

Table 3: Overview personal data listed in Schedule 1 of the Ans DPA

Data Subject	Data Item	Source	Remarks
Student	Name	SIS/LTI/LMS (or manual entry by admin)	Source depends per institution
	Email Address	SIS/LTI/LMS (or manual entry by admin)	Source depends per institution
	Student Number	SIS/LTI/LMS (or manual entry by admin)	Source depends per institution
	Role	SIS/LTI/LMS (or manual entry by admin)	Source depends per institution
	Study	SIS/LTI/LMS (or manual entry by admin)	Source depends per institution

	Department (faculty)	SIS/LTI/LMS (or manual entry by admin)	Source depends per institution
	Language Setting	Ans / Student	Default language is set in school settings by an administrator. Users can change the language setting.
	IP Address	Ans	-
	Right to extra time	Ans / SIS	-
	Comments	Student / Teacher	-
	Course enrolment	SIS/LTI/LMS (or manual entry by admin) (depends per institution)	-
	(Preliminary) results	Ans	-
	Files and answers of participants	Student	This includes handwriting of students as well.
Personnel	Name	SIS/LTI/LMS (or manual entry by admin)	Source depends per institution
	Email Address	SIS/LTI/LMS (or manual entry by admin)	Source depends per institution
	Role	SIS/LTI/LMS (or manual entry by admin)	Source depends per institution
	Department (faculty)	SIS/LTI/LMS (or manual entry by admin)	Source depends per institution
	Language Setting	Ans / Teacher	Default language is set in school settings by an administrator. Users can change the language setting.
	IP Address	Ans	

	Comments	Student / Teacher	

Besides the personal data listed above, the following personal data is processed:

Table 4: Other personal data processed in Ans

Data Subject	Data Item	Source	Remarks
Student	Alumni	SIS (or manual entry by admin)	(yes/no) Source depends per institution
	Classes / Groups	SIS/LTI/LMS (or manual entry by admin)	Source depends per institution
	Chat messages[67]	Student / Teacher	-
	Browser information	Ans	-
	Logs of actions taken by the user	Ans	General logs, and logs to generate assessment engagement metrics (including behavioural data (clicks) and timing data (e.g. how long a student works on a question in a digital test)
	Email interaction data	Ans	Open tracking on (notification) emails. This includes the user, email and timestamp when delivered and opened
Personnel	Course	SIS/LTI/LMS (or manual entry by admin)	Source depends per institution
	Chat messages[68]	Student / Teacher	-

[67] Ans considers chat messages to be included in 'comments' which are listed in the DPA.

[68] Ans considers chat messages to be included in 'comments' which are listed in the DPA.

	Browser information	Ans	-
	Logs of actions taken by the user	Ans	General logs, and logs to generate reviewer alignment data
	Email interaction data	Ans	Open tracking on (notification) emails. This includes the user, email and timestamp when delivered and opened

In addition to the data fields listed in Schedule 1 of the Ans DPA, the following personal data is also processed by Ans when the API is used:

Table 5: Data fields when using the API

Data Subject	Data Item	Source	Remarks
Student	Uid	SIS	-
	Name_id	SIS	-
	External_id	SIS	-
Personnel	Uid	SIS	-
	Name_id	SIS	-
	External_id	SIS	-

According to Schedule 1 of the Ans DPA, no special category data, criminal data or Civil Service Numbers (Dutch: BSN) are processed in Ans. *“Controller guarantees that it shall not have the aforementioned type of personal data processed in the Service.”*

Students can be granted extra time to complete an exam, either by configuring this in the overall settings or by importing the information from the student information system. The reason for the extra time is not recorded in Ans, so no special categories of personal data are processed in this way.

2.3 Customer data vs. other information

Ans's privacy policy distinguishes between 'Customer Data' and other types of information it collects. 'Customer Data' refers to content and information submitted by users through the Services. This is typically processed by Ans in its role as a data processor, acting on behalf of the institution.

In addition, Ans collects and receives various other types of information, which are not classified as Customer Data. These include:

- Account creation information: such as the users' email addresses and passwords.
- School setup information: including the email address, school name, domain details, username of the administrator, and password when a school is created.
- Billing information: collected either by Ans or its third-party payment processors, including billing addresses and credit card details for paid Services.
- Service usage data: information on how the Services are accessed and used, such as interactions with courses, students, content, and third-party integrations.
- Contact information: any imported contact data, with user permission.
- Log data: technical data automatically recorded by servers, such as IP addresses, browser details, timestamps, and cookie data.
- Device information: details about the user's device and operating system, depending on device type and settings.

While Ans processes Customer Data strictly under the customer's instructions (as a processor), it appears to process this 'other information' for its own purposes, as a data controller.

2.4 Cookies

The Ans application contains several links to Ans' corporate website in the footer. It is likely that a student may visit the Ans website while using the application. The executed test scenario assumed a student accessing the privacy statement of Ans and several other website pages (such as the 'About us' and 'Contact us' page).

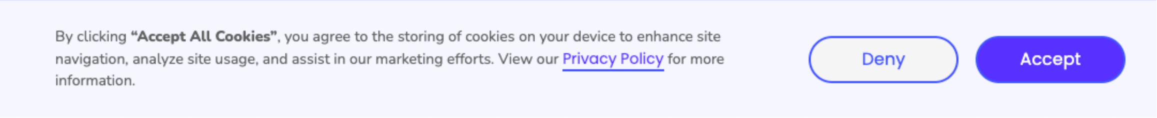
Ans's Cookie Policy is included in its Privacy Policy[69] and aims to give context on the cookies and technologies used by Ans, but fails to provide a comprehensive list of cookies, technologies, and their retention periods.

According to its Cookie Policy, Ans uses third parties like Google Analytics for website analytics for its corporate website. The Cookie Policy states: "*You may opt-in to third party cookies from Google Analytics on our website. If you don't accept the usage of analytical cookies, we will not track you.*".

Below is how Ans's cookie banner appears on the corporate website of Ans:

[69] Ans Privacy Policy, last reviewed 2 September 2024, URL: https://www.ans.app/privacy.

Figure 6: Cookie banner Ans



By clicking **"Accept All Cookies"**, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. View our Privacy Policy for more information.

Initially, it appeared that there were two Google Tag Manager configurations on the Ans webpage(s) that was tested for this DPIA: one that responded to the cookie banner and one that did not. As a result, Google Analytics was triggered twice when you clicked 'Accept' and once even if the user did not click on 'Accept' (see also Section 3.2.13 of the Technical Appendix).[70] Ans resolved this issue at the end of May 2025.[71]

The support site (help center)[72] and the system status site[73] that are both accessible through the Ans application do not have a cookie banner. The help center is provided by Zendesk. On the Zendesk pages as well as the status site, Google Tag Manager and Google Analytics are present, also setting cookies corresponding to those services. See also Section 3.2.11 and 3.2.12 of the Technical Appendix.

Update after completion of Part A

In response to the full draft of this DPIA, Ans has disabled tracking in their Zendesk environment by removing Google Tag Manager and Google Analytics. Google Tag Manager and Google Analytics contained in the status site were removed by Ans at the end of May 2025. [74]

2.5 Access to personal data

Under the GDPR, data subjects have a right of access to their personal data. In this section, the legal framework will be discussed, as well as the features Ans provides in their products to fulfil these legal obligations.

2.5.1 Legal framework

Section 2 of the GDPR gives data subjects information and access rights to their personal data. More specifically, Article 15 GDPR allows data subjects to request a copy of their personal data, together with information on how this personal data is processed and who processes the personal data. Article 28(3)(e) GDPR requires processors to assist controllers when responding to data access rights and this requirement has been incorporated in Article 3 of the SURF Data Processing Agreement.

[70] YouTube cookies are also set on the homepage, as it contains a YouTube embed. Visiting the home page of the Ans corporate website was not part of any of the test scenarios.

[71] Feedback Ans 28 May 2025, verified by Privacy Company on 23 June 2025.

[72] Available at https://support.ans.app.

[73] Available at https://status.ans.app.

[74] Feedback Ans 28 May 2025, verified by Privacy Company on 23 June 2025.

In the Nowak case, the Court of Justice of the European Union has ruled that data subject's access rights extend to the student's exam answers as well as any comments made by an examiner with respect to those answers.[75]

2.5.2 Incorporation of access rights into the product

As part of the technical testing, Privacy Company performed Data Subject Access Requests (DSARs) where a student and an employee requested all their data and information about the processing, pursuant to Article 15 GDPR. This request is discussed in more detail in Chapter 4 of the Technical Appendix.

In the response to the DSARs, Ans referred to Schedule 1 of their Data Processing Agreement, which contains some, but not all the information requested under Article 15 GDPR. For the application data, they referred the user to the Ans platform, and for log data they provided some links to logging available in the Ans application.

Furthermore, Ans provided a copy of Amazon Cloudwatch logs and an extract of a Zendesk support ticket by one of the users. Information on other collected telemetry (e.g., through Cloudflare user monitoring, Google Analytics, Google reCAPTCHA, AppSignal) was not provided and it is unknown if such information would have been available or was already fully anonymised.

The Ans product does not have a feature to request all personal data relating to a specific student or employee. Due to this, users have to manually visit every exam result, discussion, log and chat to retrieve all personal data for a user. In most cases, these pages will not (all) be available to the end-user: students are only able to access exam results during the publication window and the pages with logs on their activities are unavailable to them (except for the login history). Staff members are in a similar position for some of the logs, depending on their role in the course (instructors will be able to see all course information, but reviewers will not). Due to this approach, only an administrator can provide meaningful access to all application data and logs, which will take some effort as the personal data will be spread out over many different web pages.

Administrators do not have access to internal application logs (like the Amazon Cloudwatch logs) and can only request these through the Ans support channel. For this access, the Ans privacy policy also notes that additional costs may be involved:[76]

> *"Ans stores it logs for 365 days, unless legal obligations prescribe that the log files are required, or for research in the context of a (suspected) security incident. During this retention period, customers may request access to this information. Please note that, if a customer requests access to log information beyond what is typically included in our services, an hourly rate may apply for the time spent fulfilling this request."*

[75] CJEU 20 December 2017, C-434/16, ECLI:EU:C:2017:994 (*Nowak*).

[76] Ans Privacy Policy, last reviewed 2 September 2024, URL: https://www.ans.app/privacy.

3 Processing Activities

To assess the lawfulness of data processing activities, it is necessary to map out all data processing operations that fall within the scope of this DPIA.

The term 'processing' is broad:

> *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4(2) GDPR).*

Processing encompasses the entire lifecycle of personal data. Schedule 1 of the Ans DPA essentially repeats the wording of the GDPR when describing the processing operations. If a DPA does not explicitly list the processing operations and instead only refers to the general description of processing in the GDPR, it effectively fails to provide the processor with specific instructions. In practice, the processing activities carried out can be more described as follows:

- Creating and managing user accounts and permissions
- Identifying, authenticating, and authorizing users
- Storing login credentials, contact details, and user roles
- Supporting personnel of institutions in using the platform
- Informing users about new or updated features and methods
- Collecting and storing student data, including personal details, study information, and test results
- Recording completed assignments and student progress
- Logging student activity on the platform
- Capturing and storing communication between students and teachers
- Scanning and processing written assignments submitted by students
- Creating, administering, and reviewing digital assessments
- Storing, analysing, and interpreting test results
- Assessing individual student performance relative to norm groups
- Allowing institutions to retrieve and evaluate assessment data
- Facilitating integration with external systems, including learning tools and student information systems
- Exchanging test results and related data with institutional dashboards and student information systems
- Monitoring the availability, confidentiality, and integrity of all data
- Enforcing data retention and deletion policies
- Preventing unauthorized access, data abuse, and inconsistencies
- Ensuring system reliability
- Recording system error logs and technical events
- Conducting regular system maintenance and performance improvements
- Creating and managing system backups
- Resolving technical issues and applying updates as needed
- Supporting statistical analysis to improve learning outcomes and educational strategies
- Complying with requests from data subjects (e.g., access, rectification, deletion)
- Ensuring adherence to legal requirements regarding the use of digital educational resources

4 Purposes of the Processing

Personal data may only be collected for specified, explicit and legitimate purposes (Article 5 (1) (b) GDPR).

4.1 Purposes institutions

The Higher education and Research Act (WHW) describes the objectives of universities and universities of applied sciences as follows:

> Universities are focused on providing academic education and conducting academic research. In any case, they provide initial training in academic education, conduct academic research, provide training for academic researchers (Article 1.3 (1) WHW).
>
> Universities of applied sciences focus on providing higher professional education. They conduct design and development activities, or research aimed at professional practice. They provide bachelor's degree programmes in higher professional education, associate degree programmes and master's degree programmes in higher professional education where appropriate, and they transfer knowledge to society in all cases. They contribute to the development of professions that are the focus of the education (Article 1.3 (3) WHW).

According to Schedule 1 of the Ans DPA, the purpose for processing personal data under the Agreement is *"to help professors to review written exams, digital exams and all kind of assignments. It enables professors to review more efficient and gives them the opportunity to provide better feedback to the students".*[77] In practice, the purposes extend beyond this and encompass a broader scope. Processing of personal data using digital educational resources such as Ans by universities takes place for the purpose of providing education, including preparing, implementing, evaluating and supporting the education (process) and guiding and monitoring participants (in their learning process).

The GDPR requires the processing purposes for each processing to be specifically designated. To this end, institutions must each have set up their own processing register and inform data subjects about the processing operations through their information materials, such as the privacy statement on the website. The specific purposes of individual institutions are not the subject of this DPIA. However, it is important to note that the purposes for which institutions use Ans must all be directly related to the main purpose.

4.2 Purposes Ans

As a processor, Ans is only allowed to process personal data on behalf of and for the purposes of the institution.

According to its Privacy Policy[78], Ans Exam B.V. processes personal data in accordance with the instructions of the institution (and thus as processor) to *" (a) provide, maintain and improve the Services; (b) to prevent or address service, security, technical issues or at a Customer's request in connection with customer support matters; (c) as required by law or*

[77] Schedule 1 Ans DPA.

[78] Ans Privacy Policy, Last changed 2 September 2024, URL: https://www.ans.app/privacy.

as permitted by the Data Request Policy and (d) as set forth in our agreement with the Customer or as expressly permitted in writing by the Customer."

In addition to this, Ans Exam B.V. processes personal data also for the following (own) purposes:[79]

- To research and analyse trends to improve the services
- To send service and administrative emails and messages (mandatory)
- To send emails about new product features or news (optional, opt-out available)
- To use account data for billing and account management
- To contact users for invoicing, account updates, and similar reasons
- To use contact information for marketing and advertising (optional, opt-out available)
- To investigate and prevent abuse, fraud, and security issues

Finally, the Privacy Policy states: *"This policy is not intended to place any limits on what we do with data that is aggregated and/or de-identified so it is no longer associated with an identifiable user or Customer of the Services."*.

To train the recognition model Ans increased the training data from 50,000 to 240,000 circles taken from written assignments processed between December 2024 and March 2025. An additional purpose of Ans Exam B.V, beyond those outlined above, is to train its recognition model.

[79] Ans Privacy Policy, 'How we use your information'. 2. Other information, Last changed 2 September 2024, URL: https://www.ans.app/privacy.

5 Controller, Processor and Sub-processors

To assess the lawfulness of the data processing, it must be clear which organisations are (functionally) involved in which processing activities and in what capacity.

5.1 Educational institutions

This DPIA assumes that the standard SURF DPA is being used.[80] The institutions are independent data controllers. Each institution signs a (separate) DPA with Ans Exam B.V. for the services related to Ans.

5.2 Ans Exam B.V.

Ans Exam B.V. is a corporation under Dutch law, registered and having its office in The Netherlands. Ans Exam B.V. is the processor for the processing activities that are an integral part of Ans. Ans Exam B.V. is the data controller for the processing activities related to Ans's corporate website, to the research and analysis of trends to improve the services, the personal data used for billing, account management, user communication, and marketing purposes, and the training of its recognition model.

5.3 Other parties involved in the processing

According to Schedule 1 of the Ans DPA, Ans engages the following sub-processors:

Table 6: Overview sub-processors Ans – Ans DPA

Name	Type of data	Subject
AWS	Name Email address Student number Role Study Department (faculty) Language setting IP Address Right on extra time Comments Course enrolment (Preliminary) results Files and answers of participants	Webhosting
Cloudflare	IP-Address	DDos mitigation Encrypted traffic

[80] As a result, the clauses of the standard Ans DPA are not assessed. Only its Schedules are used as a reference (see also the scope description in the Introduction chapter).

TransIP (formerly known as CloudVPS)	Name Student number Files and answers of participants	File storage
Escrow4All	Access to AWS, Cloudflare and TransIP.	SaaS ESCROW
MailerLite	Name Email address	Mails
Zendesk	Name Email address Role	Support tickets

The Technical Appendix summarises the test results of the executed test scenarios per contacted third party, from which an overview of (sub-)processors can be identified (see Table 7 and Section 3.1 of the Technical Appendix).

The table below provides an overview of the observed (sub-)processors involved in the processing. For clarity, these parties can be categorized based on their relevance to different components of the system. Parties listed under Tests 1 to 10 (top row) are related to the processing operations in the main application, while those under Tests 11 to 13 and 15 support other components such as the support portal, status site, website, and support request system. Test 14 focussed on the SSO login process.

Table 7: Overview observed (sub-)processors involved in the processing

	1	2	3	4	5	6	7a	7b	8	9	10	11	12	13	14	15
Cloudflare	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Google Sign-In	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●
Google reCAPTCHA	●			●	●	●	●	●	●	●	●	●	●	●		●
Google Fonts	●			●	●	●	●	●	●	●	●	●	●	●		●
Google Charts	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Google YouTube				●	●				●	●	●					
Google Calendar									●							
Google TM/Analytics												●	●	●		●
Sorry App	●	●		●	●	●	●	●	●	●	●	●	●	●		●
Amazon Cloudfront	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Amazon S3				●												
Twilio Segment	●	●		●			●		●		●					
SatisMeter	●	●		●			●		●		●					
AppSignal				●						●						
UNPKG[81]				●	●	●		●	●	●	●					
TransIP				●	●				●	●	●					
Zendesk												●				●
RSMS													●			
New Relic													●			

[81] Ans removed this party from their product in the release of 22 June 2025, which was verified by Privacy Company on 23 June 2025.

Gravatar													●			●
Webflow														●		
Calendly														●		
Jsdelivr														●		
cdnjs												●				●

The sub-processor list in Ans' DPA (Table 6) is thus not comprehensive as it omits certain sub-processors. It also fails to provide a complete account of the personal data processed by those that are included. For example, Cloudflare also processes content data, which includes most of the data flowing through their system (with the potential exception of uploads and paper exams), while Ans' DPA only mentions IP addresses (see also Section 3.3.1).

Schedule 1 of the Ans DPA acknowledges that more parties are involved in the processing operations and states: *"The Processor uses other applications for the processing of data, such as Appsignal for performance monitoring. These applications do not process any Personal Data and are therefore not included in the overview."* This statement fails to acknowledge that IP addresses are considered personal data under the GDPR and that sending web traffic directly from an end-user device to a third party will cause the third party to process the end-user's IP address. As such, these applications and the parties involved should be included in the overview of sub-processors, as they are processing personal data.

The parties involved in the processing (listed in Table 7) are described below. Each party is accompanied by a description and an indication of its role.

5.3.1 Cloudflare

Cloudflare offers global network services, including content delivery network (CDN) and security services. Cloudflare, Inc is headquartered in San Francisco, United States.

As part of this DPIA, Cloudflare was observed at various parties, including the main application domain ans.app being on Cloudflare. Cloudflare then 'proxies' all the web traffic to the application, sending it on through the backend (at AWS in case of Ans), while providing caching and security services.

Cloudflare is listed in Schedule 1 of the Ans DPA. Ans shared the (undated) standard Cloudflare DPA which forms part of the main agreement (between Ans and Cloudflare) for the purpose of this DPIA.

5.3.2 Google

All Google services listed below are offered by Google LLC, a US-based company. Due to the nature of Google's globally distributed network, it cannot be determined from the outside where the data is processed or stored.

5.3.2.1 Google Sign-In

Google Sign-In is a service that allows websites to offer authentication with a Google account.[82] If a user successfully authenticates, Google profile information may be shared with the application. The Google Sign-In was not tested as part of this DPIA but was present on the login page of the Ans application.

When Google Sign-In is loaded, several unknown data parameters, as well as Google's identifying cookies (if the user was previously authenticated with Google), are exchanged with Google. Additionally, the user's IP-address and browser information (including referring domain) are sent to Google.

Google's privacy policy applies to the use of Google Sign-In.[83]

Update after completion of Part A

The Google Sign-In popup on the login screen has been removed as per the Ans release of 7 December 2025.

5.3.2.2 Google reCAPTCHA

Google reCAPTCHA is a CAPTCHA system which is used by websites and apps to identify and prevent automated access to websites. It is included as JavaScript from www.recaptcha.net or www.google.com.

Google reCAPTCHA is included on Ans' login page. It is also included on the subscription for of the status website.

A _GRECAPTCHA cookie, other Google cookies if the user was previously authenticated on a Google domain, the IP address and browser information of the user (including referring domain) are sent to Google during access.

Google does not publish what other data reCAPTCHA processes (e.g., to detect automated behaviour). It is widely assumed that reCAPTCHA retrieves browser details and tracks user's mouse movements and other actions on the site, to determine if a user is human. In the scope of this DPIA the exact implementation was not further analysed.

Google's privacy policy applies to the use of Google reCAPTCHA.[84]

Update after completion of Part A

[82] Google Identity Overview, URL: https://developers.google.com/identity/gsi/web/guides/overview, last viewed: 10 April 2025.

[83] Security and Privacy in Charts, URL: https://developers.google.com/chart/interactive/docs/security_privacy, last viewed: 6 April 2025.

[84] Security and Privacy in Charts, URL: https://developers.google.com/chart/interactive/docs/security_privacy, last viewed: 6 April 2025.

Google reCAPTCHA on the sign-in page has been replaced with Cloudflare Turnstile as per the Ans release of 17 August 2025.[85] Administrators who manage network restrictions should allow access to https://challenges.cloudflare.com.

Privacy Company has not assessed Cloudflare Turnstile for GDPR compliance, but as a DPA is in place with Cloudflare it is likely that the new situation is more compliant than the old situation.

5.3.2.3 Google Fonts and Google Charts

Google Fonts and Google Charts provide hosting services for fonts files and a graphing library, distributed through a Content Delivery Network. These are delivered through domains that do not contain Google's identifying cookies, meaning only the user's IP-address and browser information (including referring domain) are transmitted to Google. These services are used in the main Ans application to draw graphs in the user interface and to provide fonts needed for Google Sign-In and reCAPTCHA.

Google's privacy policy applies to the use of Google Charts.[86] Which policies apply to Google Fonts is unknown, Google merely states they do not use the collected user data for profiling or targeted advertising.[87]

Update after completion of Part A

Google Fonts was also removed as a consequence of the removal of Google reCAPTCHA and the Google Sign-In popup as it was a dependency of these products.

5.3.2.4 Google YouTube

Google YouTube is an online video hosting provider. The Ans application offers the possibility to embed a YouTube video in an exam question. In this case, the video is included from the www.youtube.com domain. Also, the googleapis.com, play.google.com and doubleclick.net domain are contacted to exchange information.

During access, both for staff members embedding the video and students viewing the video, several YouTube cookies, including advertising cookies[88], Playback information when and how long the video is played, latency, button clicked), other Google cookies if the user was previously authenticated on a Google domain, the IP address and browser information of the user (including referring domain).

Google's privacy policy applies to the use of Google YouTube.[89]

[85] Ans Release Notes: URL: https://support.ans.app/hc/en-us/articles/36388921626513-17th-of-August-2025.

[86] Security and Privacy in Charts, URL: https://developers.google.com/chart/interactive/docs/security_privacy, last viewed: 6 April 2025.

[87] Privacy and Data Collection, URL: https://developers.google.com/fonts/faq/privacy, last viewed: 6 April 2025.

[88] How Google Uses Cookies, URL: https://policies.google.com/technologies/cookies, last viewed: 6 April 2025.

[89] Security and Privacy in Charts, URL: https://developers.google.com/chart/interactive/docs/security_privacy, last viewed: 6 April 2025.

5.3.2.5 Google Calendar

Google Calendar is an online calendar service. Ans provides a link to Google Calendar to staff members at the end of a SatisMeter survey (see Section 5.3.6) to allow for creating an appointment with an Ans researcher. Google Calendar is offered by Google LLC, a US-based company. Due to the nature of Google's globally distributed network, it cannot be determined from the outside where the data is processed or stored. Google's privacy policy applies to the use of Google Calendar.[90]

During access, the following data will be sent to Google:

- Name and email address of the user, if they plan an appointment.
- NID cookie. This cookie remembers preferences, is used for analytics and for advertising.[91]
- Other Google cookies if the user was previously authenticated on a Google domain
- IP address of the user and browser information of the user, including referring domain (e.g., ans.app)

Google's privacy policy applies to the use of Google Calendar.[92]

5.3.2.6 Google Tag Manager / Analytics

Google Tag Manager is a tag management system to include scripts (like analytics scripts) in websites. Google Analytics is web analytics software that tracks website visits and actions visitors undertake on these websites.

Google Tag Manager and Google Analytics are included on the Ans corporate website and Ans support portal. Previously, these services were also enabled on the Ans status page, but they were removed at the end of May 2025.[93]

During access, the following data will be sent to Google:

- Several cookies, not all of which are listed in Google's cookie policy.[94]
- Browser configuration of the user, like screen resolution and language.
- Actions a user takes on the website (for instance: clicks)
- IP address of the user
- Browser information of the user, including referring domain (e.g., ans.app)

Google states they are a processor for the data processing of Google Analytics.[95]

5.3.3 Sorry App

Sorry App is offered by SorryApp Ltd, a UK-based company. Sorry App offers a status website, displaying the current availability of a software application. It also offers

[90] Security and Privacy in Charts, URL: https://developers.google.com/chart/interactive/docs/security_privacy, last viewed: 6 April 2025.

[91] How Google Uses Cookies, URL: https://policies.google.com/technologies/cookies, last viewed: 6 April 2025.

[92] Security and Privacy in Charts, URL: https://developers.google.com/chart/interactive/docs/security_privacy, last viewed: 6 April 2025.

[93] Feedback Ans 28 May 2025, verified by Privacy Company on 23 June 2025.

[94] How Google Uses Cookies, URL: https://policies.google.com/technologies/cookies, last viewed: 6 April 2025.

[95] Safeguarding your data, URL: https://support.google.com/analytics/answer/6004245, last viewed: 10 April 2025.

functionality to subscribe to status updates through email (the latter functionality was not tested during this DPIA).

Ans uses Sorry App to provide the status website available on status.ans.app, linked from the footer of the Ans application. The tool also offers a status bar (to show upcoming maintenance of urgent issues), included from code.sorryapp.com which reads information through an API on ro-api.sorryapp.com.

If a user only visits one of the pages that include the status bar, the user's IP address and browser information is exchanged with Sorry App. If a user also visits the status website, additionally the following data is exchanged: Google Analytics cookies (see Section 3.3.8 of the Technical Appendix, removed at the end of May 2025), Google reCAPTCHA information (see Section 3.3.3. of the Technical Appendix), and New Relic information (see Section 3.3.20 of the Technical Appendix). If the user subscribes to status updates by email, Sorry App also processes the user's email address.

Sorry App primarily hosts on Amazon Web Services. Although their publicly available sample DPA states that international transfers will only be made after written permission by the customer, their privacy policy states their servers are located in the United States.[96]

Ans processes personal data on their status website for their own purposes and therefore acts as a data controller. In this context SorryApp acts as a processor on behalf of Ans Exam B.V.

Section 3.3.20 of the Technical Appendix describes the traffic observed to New Relic. As New Relic is used by the Sorry App status application it is technically a sub-processor of SorryApp. For this reason, New Relic is not further assessed in this DPIA. The same goes for RSMS (Section 3.3.19 of the Technical Appendix).

5.3.4 Amazon

Amazon Web Services, also known as AWS, is a cloud computing services platform offered by Amazon. AWS is headquartered in Seattle, Washington, United States and its services are provided across multiple geographic regions around the world. The following services of Amazon were observed (See Sections 3.3.10 – 3.3.12 of the Technical Appendix):

- Amazon Cloudfront: a content delivery network (CDN), acting as a globally distributed cache for content (videos, images, scripts, et cetera).
- Amazon S3: a cloud object storage service, storing data with high scalability, availability and durability.
- Amazon Simple Email Service (SES): is a transactional email service offered within AWS. It allows applications to send emails.

AWS is included in Schedule 1 of the Ans DPA. According to the information in the Schedule, Ans is hosted on AWS. Ans shared the (undated) standard AWS DPA which forms part of the AWS Customer Agreement for the purposes of this DPIA.

[96] Privacy Notice, URL: https://www.sorryapp.com/privacy-policy/, last updated: 1 February 2021.

5.3.5 Twilio Segment

Twilio Segment is a Customer Data Platform (CDP) which allows companies to collect customer data, including customer actions, from multiple sources (e.g., the application, customer database, invoicing database, et cetera), enrich and transform that data and then send it to other applications. One of the uses of such a tool is to profile customers and send them more targeted marketing messages. Twilio Segment is offered by Segment.io, Inc., a subsidiary of Twilio Inc., both US-based companies.

Segment is included by the Ans main application from domain cdn.segment.com. Segment itself seems to load two other tools: SatisMeter (see Section 3.3.14 of the Technical Appendix) and Amplitude (further traffic by this tool was not observed). The telemetry sent to Segment, to api.segment.io, seems to be limited. The following data was processed:

- Ans User ID of the user
- The URL of the visited page and the full referring URL
- Time zone of the user
- IP address of the user
- Browser information of the user, including referring domain (e.g., ans.app)
- Cookies set by Segment and its plugins (ajs_anonymous_id, ajs_userid, analytics_session_id and analytics_session_id.last_access). One of these cookies contains the Ans User ID (ajs_user_id). The others contain unique session identifiers.

Ans processes personal data to research and analyse trends to improve the services for their own purposes, and thus in the capacity of data controller. Twilio Segment is a processor of Ans Exam B.V.

5.3.6 SatisMeter

SatisMeter is a customer feedback tool that allows integrating a survey into applications. Users can provide a rating and answer one or more questions to provide feedback on the product. SatisMeter is offered by SatisMeter S.r.o., a Czech company, and a subsidiary of Productboard, Inc., a US-based company.

Ans uses SatisMeter to surface surveys to staff members and administrators from time to time (see for an example Figure 2). SatisMeter is not included for student users. At the end of the SatisMeter survey, the user is offered an option to make an appointment with a researcher at Ans using Google Calendar (see 3.3.7).

The Ans User ID of the user and all answers given by the user during the survey (rating, answers to closed and open questions) data is exchanged with SatisMeter (through the app.satismeter.com endpoint).

Ans processes personal data to research and analyse trends to improve the services for their own purposes, and thus in the capacity of data controller. SatisMeter is a processor of Ans Exam B.V.

Surveys can be disabled by users in their profile. In these cases, a survey will not be surfaced in the application. Limited information is still exchanged with SatisMeter in these cases, as the SatisMeter scripts are still included in the web pages. Surveys can also be disabled on a school level, but only through Ans' support department. A self-service setting was available to administrators, but this setting was removed by Ans to *"prevent accidental changes"*.[97]

5.3.7 AppSignal

AppSignal is used by the Ans main application. It offers an application performance monitoring solution, tracking errors and other performance issues within applications. To do this, a script is included in the application which reports errors and warnings to appsignal-endpoint.net. AppSignal is offered by Dutch company AppSignal B.V.

When an error or a warning is reported, the URL of the visited page (including the error), the IP address and browser information (including referring domain) of the user is sent to AppSignal.[98]

AppSignal is not mentioned in Schedule 1 of the Ans DPA. Ans did not share a DPA for AppSignal, but Ans commented that they do have a DPA.

5.3.8 TransIP

TransIP B.V. is a Dutch company with data centres in various locations in the Netherlands.[99] TransIP offers a cloud object storage service. During the tests, TransIP was used by the Ans application when staff members uploaded exam content (e.g., images or sound recordings) and when end-users viewed this content.

In addition to the personal data listed in Schedule 1 of the Ans DPA (see Table 6), TransIP also processes: image or sound data uploaded or viewed by users when creating, making or reviewing an assignment, the IP-address of users, and browser information of the user, including referring domain (e.g., ans.app). During testing, the data items listed in Schedule 1 of the DPA were not observed to be exchanged with TransIP.

TransIP is listed in Schedule 1 of the Ans DPA and Ans shared the sub-processor agreement it has in place with TransIP B.V.

5.3.9 Zendesk

Zendesk provides customer support software. The Ans help centre with knowledge base articles, as well as the Ans support desk (ticket support) are using the Zendesk software. The software is available through the domains support.ans.app and ans.zendesk.com.

Ans works with the ticketing system of Zendesk. It depends per institution if automatic replies are sent. When automatic replies are implemented, the student or staff member (not admins) receive a message with a reference to the contact page of the of the institution. The content of this message is provided by the institution. When automatic

[97] 10th of November 2024, URL: https://support.ans.app/hc/en-us/articles/28797061237265-10th-of-November-2024, last updated: 25 November 2024.

[98] In case of AppSignal, the IP address of the user is not part of the payload sent to AppSignal, but as the payload is sent directly from the end-user's device, AppSignal will receive the end-user's IP address.

[99] What is an availability zone?, URL: https://www.transip.eu/knowledgebase/990-what-is-an-availability-zone, last viewed: 8 April 2025.

replies are not set, students and staff members can contact Ans directly. Depending on the agreement with the institution, Ans will treat the questions directly or forwards the questions to the e-mail address of the admin of the school. Questions of students are almost all forwarded to the institution. Admin can have access to all tickets within their organisation to have an overview of all questions asked by their students and staff members.[100]

According to Schedule 1 of the Ans DPA, Zendesk processes the user's name, email address and role. In addition to this Zendesk also processes a password if it was set when creating a request, the user's support requests including any files added to those requests, search queries done in the help portal, the rating and feedback a user provided to a helpdesk ticket, Google Tag Manager and Google Analytics cookies, Zendesk cookies, Cloudflare security cookies, IP addresses and browser information of the user (including referring domain).

Update after completion of Part A

In response to the full draft of this DPIA, Ans has disabled tracking in their Zendesk environment by removing Google Tag Manager and Google Analytics.

Zendesk is offered by Zendesk, Inc., a US-based company (or possibly by Zendesk Netherlands B.V., a Dutch subsidiary). They offer data hosting locations in the U.S., Ireland, Germany, the U.K., Japan and Australia, but only guarantee a specific data location if a separate add-on is purchased.[101] From the outside, it is not possible to determine the data storage location for the data of Ans.

5.3.10 Gravatar

Gravatar is a service offered by Automattic, a US-based company. Gravatar is a service for providing avatars over multiple websites. Users can register at the website and upload an avatar, which will be shown on other websites using Gravatar. Hosts contacted are secure.gravatar.com and i1.wp.com.

Gravatar avatars are used to display end-user avatars in the Zendesk help center (Section 5.3.9). Additionally, they are used to show the avatars of Ans' employees in the Sorry App application (See Section 5.3.3).

During access, the following data will be sent to Gravatar:

- IP address of the user
- Browser information of the user, including referring domain (e.g., status.ans.app)
- An MD5-hash of the email address of the avatar being requested. In case of the help center, this is an MD5-hash of the end-user's mail address. This hash is outdated

[100] Mail Ans, 7 March 2025.

[101] Data Hosting Locations for Your Zendesk Service Data, URL: https://support.zendesk.com/hc/en-us/articles/4408825765530-Data-Hosting-Locations-for-Your-Zendesk-Service-Data, last updated: 1 July 2024.

and could be reversed into the actual mail address (Gravatar also supports SHA256 hashes, but those are not used by Zendesk).

- Any cookies that were previously set on the .gravatar.com domain (in case the user previously visitor gravatar.com this could include Google Analytics cookies).

Gravatar is a technically a sub-processor of Zendesk and SorryApp. For this reason, Gravatar is not further assessed in this DPIA.

5.3.11 Webflow

Webflow is provided by Webflow, Inc., a US-based company. It provides SaaS services for website building and hosting. Webflow itself seems to use a combination of Amazon AWS (for www.ans.app) and Cloudflare (for cdn.prod.website-files.com) for website hosting.

Webflow is used for the Ans corporate website (www.ans.app). It tries to set a Cloudflare security cookie (_cfuvid), but this is set on the wrong domain (.cdn.webflow.com). This does give an indication that even the traffic to the Amazon AWS endpoint (www.ans.app) also flows through Cloudflare in the backend (another indication is the Cf-Ray HTTP header in the response). It also sets a cookie ‘fs-cc’ for the cookie consent, which carries a unique ID and Google Analytics’ first party cookies will be sent to Webflow as well.

During access, the IP address and browser information of the user (including referring domain) is sent to Webflow. In addition to this a cookie consent cookie with a unique consent ID and Google Analytics cookies are sent to Webflow.

Ans is a data controller for its corporate website. Webflow is therefore a processor of Ans Exam B.V.

5.3.12 Mailerlite

Mailerlite is an email newsletter service which allows to send emails in bulk to a large number of recipients and to send automated emails based on a workflow (e.g., when a new user joins). Mailerlite is offered by MailerLite Limited, an Irish company, with a subsidiary in the United States. Data is stored in the European Union.[102]

During the testing period, several emails were sent to staff members and administrators, not to students. The emails range from overviews of changes to the software, to explanatory emails on how to use the application and a questionnaire to share an opinion on Ans and win a pair of Ans socks. Administrators or staff members were not asked to subscribe or consent to these emails during sign-up. The emails did offer a link to unsubscribe. The emails contained both tracking pixels and tracking URLs.

Besides the personal data listed in Schedule 1 of the DPA, Mailerlite processes also email interaction data (open and link actions, if users show external images in the email and/or click on links in the email) when emails are sent.

Ans shared the standard Mailerlite DPA which supplements the Terms of Use (TOU) for the purposes of this DPIA.

[102] Is my data safe with MailerLite?, URL: https://www.mailerlite.com/help/is-my-data-safe-with-mailerlite, last updated: 18 January 2023.

The role of MailerLite depends on the email and the purpose of the email sent. Emails about changes in the software or about how to work with the application are part of Ans' services in which case MailerLite would be a sub-processor of Ans Exam B.V. For other emails, such as the one in which socks can be won, are for Ans own purposes as a data controller, in which case MailerLite is a processor of Ans Exam B.V.

5.3.13 Escrow4all

Escrow4all B.V. is a Dutch escrow provider. Schedule 1 of the Ans DPA refers to the SaaS Escrow services from Escrow4all. According to the website of Escrow4all, the service model of SaaS Escrow is not universal, and it can cover many scenarios.[103] Schedule 1 of the Ans DPA mentions access to AWS, Cloudflare and TransIP.

Ans is in the process of implementing this service with Escrow4all. At this stage, there is no formal contract with Escrow4all, as Ans needs to obtain customer consent first. While this process is ongoing, Ans is proactively including Escrow4all as a sub-processor for new customers.

Based on the available information, it is unclear whether Escrow4all processes personal data of
the users of Ans, and what that data might include.

[103] Escrow4all, URL: https://www.escrow4all.com/oplossingen/saas-escrow/, last viewed 22 April 2025.

6 Interests in the Data Processing

This chapter outlines the (potential) interests of the institutions, Ans, its (sub-)processors, students and employees of institutions

6.1 Educational institutions

Institutions have an interest in having the capability to administer digital tests and exams, allowing for a reliable assessment of students' knowledge and progress. Furthermore, institutions have an interest in suppliers who comply with the GDPR, so that the institutions, as data controllers, can meet their obligations.

6.2 Ans Exam B.V.

Ans Exam B.V. has an interest in providing reliable and high-quality services in the form of Ans, while also safeguarding its financial and commercial interests.

6.3 Sub-processors

The sub-processors have a commercial interest in providing the services to enable Ans to deliver Ans as a SaaS solution. Additionally, they have an interest in complying with laws and regulations.

6.4 Students

Students have an interest in a well-functioning and reliable examination system, where the institution handles exam-related data with care and accuracy. The institution must implement appropriate technical and organisational measures to prevent unauthorized access or use. Finally, students have a vested interest in ensuring that their personal data is not processed unnecessarily or unlawfully within the examination system.

6.5 Employees of Educational Institutions

Educators and other staff require a well-functioning examination system that contains relevant information about academic progress and allows for the efficient input and retrieval of data such as exams, and grades. Additionally, staff members have an interest in ensuring that their personal data is not processed unnecessarily or unlawfully within the system or by the supplier for their own purposes.

7 Processing Locations

The physical locations where data processing takes place may pose additional risks and therefore be subject to stricter rules and require additional measures. Not only the storage of personal data is relevant to assess, but also, for example, the locations where data is accessed, streamed or temporarily stored.

The GDPR contains specific rules for the transfer of personal data to countries outside the EEA. In principle, personal data may only be transferred to countries outside the EEA if there is adequate protection of the personal data guaranteed. Adequate protection can be achieved in several ways. If the country to which data is transferred had received an adequacy decision from the European Commission, the protection can be considered equivalent to the protection within the EEA. If such an adequacy decision is not present, other mechanisms can be used to ensure protection, such as applying the EU SCCs.

7.1 Ans' factual processing locations

Ans Exam B.V. is headquartered in The Netherlands. Schedule 1 of the Ans DPA includes information on processing locations of some of the sub-processors. The following table lists the information in Schedule 1.[104]

Table 8: Processing locations sub-processors

Name	Subject	Location of processing	Country of establishment	Comments
AWS	Webhosting	EU datacentre (Germany and/or Ireland)	Luxembourg	Amazon Webservices Inc. is headquartered on Seattle, Washington, US.
Cloudflare	DDos mitigation Encrypted traffic	Worldwide (nearest datacentre to user)	United States	
TransIP (formerly known as CloudVPS)	File storage	Netherlands	Netherlands	
Escrow4All	SaaS ESCROW	Netherlands	Netherlands	
MailerLite	Mails	EU datacentre (Germany)	Ireland	

[104] The columns name, subject, location of processing and country of establishment are copied literally from Schedule 1 of the Ans DPA.

Zendesk	Support tickets	EU datacentre (Germany and/or Ireland)	United States	

The other sub-processors that were identified are listed below:

Table 9: Processing locations other identified sub-processors

Name	Subject	Location of processing	Country of establishment	Comments
SorryApp	Status website	US	UK	Sorry App primarily hosts on Amazon Web Services. Although their publicly available sample DPA states that international transfers will only be made after written permission by the customer, their privacy policy states their servers are located in the United States.[105]
AppSignal	Application performance monitoring	Netherlands[106]	Netherlands	

7.2 Transfer mechanisms

7.2.1 Adequacy decision

An adequacy decision means that the country or category of organisations to which data is transferred has a level of protection comparable to that applied within the EEA. Currently, there are adequacy decisions with respect to Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, the United States (commercial organisations participating in the EU-US Data Privacy

[105] Privacy Notice, URL: https://www.sorryapp.com/privacy-policy/, last updated: 1 February 2021.

[106] Privacy Policy, URL: https://www.appsignal.com/privacy-policy, last updated: 10 February 2025.

Framework (DPF)) and Uruguay.[107] With the exception of the United Kingdom, these adequacy decisions do not cover data exchanges in the law enforcement sector which are governed by the Law Enforcement Directive (Article 36 of Directive (EU) 2016/680).

On 10 July 2023, the European Commission issued a renewed adequacy decision for participants to the DPF in the US.[108] As a result, for participants the US is considered to have an adequate level of data protection, and European organisations are allowed to transfer personal data to US based cloud service providers without any additional protective measures.

Cloudflare, Inc., Amazon Web Services, Inc., Zendesk, Inc. have certified their participation in the EU-US Data Privacy Framework. [109]

7.2.2 Standard Contractual Clauses

Personal data may be transferred from the EEA to third countries outside of the EEA using SCCs adopted by the European Commission.[110] These clauses contractually ensure a high level of protection. The publicly available sample DPA of SorryApp includes SCCs.[111]

[107] European Commission, Adequacy decisions, URL: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, Last viewed 31 August 2023.

[108] European Commission, Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows, 10 July 2023, URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721, Last viewed 22 April 2025.

[109] Data Privacy Framework Program, 'Data Privacy Framework List', URL: https://www.dataprivacyframework.gov/list, last viewed22 April 2025.

[110] Based on the Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/6794 June 2021, URL: https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf

[111]

8 Techniques and Methods of the Data Processing

The use of certain data processing techniques and methods may entail additional risks and therefore be subject to stricter rules and additional measures. This is the case, for example, with (semi-)automated decision-making, profiling, and big data processing.

In Ans, no new or potentially invasive technologies are used. There is no processing of big data.

As described in Section 1.1.4, closed-ended questions, like multiple-choice or order questions, can be automatically graded by the software. For these questions, the staff member does not have to review the questions. Optionally, the staff member can however view the answer and change the grading. Leaving comments is not possible on closed-ended questions.

Ans acknowledges in a reflection on a service incident in 2024, that it is not possible to ensure complete accuracy in all response classifications in case of written, paper-based assignments. For this reason, Ans recommends manually reviewing automatically graded responses to help identify any potential errors.[112] Ans estimates that around 6% of multiple-choice questions will require manual review.[113]

With the release on January 5th, 2025, Ans introduced a new recognition model for automatically grading multiple-choice and multiple-response questions in written assignments.

The new recognition model recognises the following four states:

State 0: The circle/box has been left empty.
State 1: The circle/box has a cross inside it.
State 2: The circle/box is fully coloured.
State 3: The circle/box has been corrected because there is a cross outside the fully coloured circle/box.

Ans requires manual review for responses classified as state 3, where a cross is placed fully outside the circle. Student intent in these cases can be ambiguous and determining intent in such situations depends on the context of the entire question. As a result, Ans will no longer automatically grade answers in state 3. This approach also applies to multiple-response questions.[114]

The automated grading does not fall under the prohibition of Article 22 of the GDPR, as it does not involve fully automated decision-making without human involvement and appropriate safeguards.

[112] Ans, ' Service Incident - 6th of May 2024 - Incorrect detection for multiple choice questions when using multiple alternatives and corrections', URL: https://support.ans.app/hc/en-us/articles/24946591856529-Service-Incident-6th-of-May-2024-Incorrect-detection-for-multiple-choice-questions-when-using-multiple-alternatives-and-corrections, last viewed 22 April 2024.

[113] Ans email 31 March 2025.

[114] Ans email 31 March 2025.

To train the recognition model Ans increased the training data from 50,000 to 240,000 circles taken from written assignments processed between December 2024 and March 2025. For this training, Ans used anonymised answers of exams that only included answer circles/boxes and no personal data.[115]

[115] Ans feedback 10 December 2025.

9 Additional legal obligations

In addition to the GDPR, the following laws and regulations may apply to the use of Ans by institutions.

Table 10: Overview additional laws and regulations

Abbreviation	**Law and regulation**	**Relevant articles**
WHW	Higher education and Research Act *(Wet op het Hoger Onderwijs en Wetenschappelijk Onderzoek)*	Several articles
WEB	Adult and Vocational Education Act *(Wet educatie en beroepsonderwijs)*	Several articles
Wgbh/cz	Equal Treatment (Disability and Chronic Illness) Act 2003 *(Wet Gelijke behandeling op grond van handicap of chronische ziekte)*	2, 4, lid f
AW	Archives Act 1995, including the Archives Decree 1995 and the Archives Regulation *(Archiefwet 1995, inclusief het Archief Besluit 1995 en de Archiefregeling)*	5
	Records Retention Schedule for Universities and Universities of Applied Sciences *(Selectielijsten voor Universiteiten en Hogescholen)*	
	Records Retention Schedule for Senior Secondary Vocational Education Institutions *Selectielijst voor onderwijsinstellingen in het middelbaar beroepsonderwijs (mbo)*	
BIHO	Baseline Information Security Higher Education *(Baseline informatiebeveiliging Hoger Onderwijs)*	
Tw	Telecommunications Act *(Telecommunicatiewet)*	11(7a)

9.1 Higher education and Research Act (WHW)

The Higher Education and Research Act (WHW) provides the legal framework for delivering education. Institutions have a quality assurance system that ensures careful management of student records and academic results. Additionally, codes of conduct and integrity standards for both staff and students are actively upheld and implemented.

9.2 Adult and Vocational Education Act (WEB)

The Education and Vocational Training Act (WEB) forms the legal framework for the provision of education. The institutions have a quality assurance system in place, which guarantees, among other things, the careful handling of data in the student administration and study results. In addition, codes of conduct and integrity for staff and students are observed and applied.

9.3 Equal Treatment (Disability and Chronic Illness) Act 2003

Educational institutions are required under the Equal Treatment Act on the Grounds of Disability or Chronic Illness (Wgbh/cz) to make effective adjustments according to individual needs, unless this would place a disproportionate burden on them.

9.4 Archives Act 1995, Records Retention Schedule for Universities and Universities of Applied Sciences

In carrying out their duties, universities of applied sciences and universities perform a public authority task for a limited number of processes. According to Article 5 of the Archives Act (AW), public authority tasks form the basis for a selection list. For the underlying selection list, these tasks are largely related to whether or not a student obtains a degree. These are the tasks for which the information objects fall under the scope of the Archives Act 1995.

The Archives Act forms an exception to the GDPR. This means that personal data may be retained in archives. However, it should be noted that if personal data is not necessary for the context of the case or file, it must still be deleted. The case or file may only contain relevant personal data.[22]

9.5 Records Retention Schedule for Senior Secondary Vocational Education Institutions

In carrying out their work, a vocational institution performs a public authority task for a limited number of processes. According to Article 5 of the 1995 Archives Act (AW), public authority tasks form the basis for a selection list. For the underlying selection list, these tasks largely relate to whether or not a student obtains a degree. These are the tasks for which the information objects fall under the scope of the AW.

Some tasks of vocational institutions can be classified as public authority tasks. In such cases, the decision of the competent authority affects the legal position of a student. The following public authority tasks can be distinguished:
· The issuance of a certificate.
· The granting of exemption on the basis of the Compulsory Education Act (Leerplichtwet)[116].

Documentary structure plan for vocational education

The model documentary structure plan (DSP) is a supplement to the new records retention schedule for vocational education drawn up by the MBO Council (MBO Raad). The MBO Council has drawn up a model documentary structure plan (DSP) to ensure clarity and

[116] Selection list for vocational education institutions in secondary vocational education (MBO). Selection list for the administrative records of the public tasks of the responsible authorities for the period from 1 August 2017.

uniformity in the vocational education sector with regard to the retention of documents. The DSP is a list of the most important and most common documents/information within MBO schools and the statutory retention and destruction periods for those documents. The DSP does not distinguish between digital and physical (paper) documents. The retention and destruction periods apply to both types.[117]

The DSP is not formal in nature and no rights or obligations can be derived from it. Each vocational education institution is responsible at all times for the correct application of relevant legislation and regulations. However, it is strongly recommended that the DSP be used as a basis for the retention and destruction of documents/information.

9.6 Baseline Information Security Higher Education (BIHO)

SURFibo has developed a model information security policy for Higher Education. The policy addresses the relevant information security measures, in accordance with ISO 27002, that need to be implemented within the Higher Education sector.

9.7 Telecommunications Act

The ePrivacy Directive regulates the privacy of users of telecommunications services. The Directive has been implemented in the Netherlands through the Telecommunications Act (Tw).

Article 11(7a) Tw (the "cookie law") states:

> *“Without prejudice to the General Data Protection Regulation, the storing of or gaining access to information in the terminal equipment of a user via an electronic communications network is only permitted on the condition that the user concerned:*
> *a. has been provided with clear and comprehensive information in accordance with the General Data Protection Regulation, at the very least regarding the purposes for which this information is used, and*
> *b. has given consent for this.”*

The law includes three exceptions to this provision in Article 11(7a) (3) Tw. User consent is not required if the information is necessary solely to establish the communication; if access is strictly necessary to provide the information society service requested; or to obtain information about the quality and effectiveness of the information society service, provided this does not or hardly infringe on the user’s privacy.

[117] Introduction to the model Documentary Structure Plan for MBO, available at: https://www.mboraad.nl/publicaties/model-documentair-structuurplan-dsp-mbo .

10 Retention Periods

A data controller may retain personal data only for as long as necessary for the purpose for which it was collected (Article 5 GDPR). After that, the data controller must destroy the data, unless they are required to retain it longer, for example, because this is stipulated by law.

For the public authority tasks of universities and universities of applied sciences, the retention schedule must be established by the boards of the institutions and based on Article 5 of the Archives Act (AW), also approved by the Minister of Education, Culture and Science (OCW). The processes in question must indicate that they involve a public authority task and are therefore subject to the scope of the Archives Act.

The Archives Act forms an exception to the GDPR. This means that personal data may be stored in archives. However, it must be noted that if the personal data are not necessary in the context of the case or file, they must still be removed. A case or file may only contain relevant personal data.

Article 7.3, paragraph 5 of the WHW states:

> *“The examination referred to in paragraph 3 that has been successfully completed, as well as the work produced in preparation for it, shall be retained by the institution’s board for a period of at least seven years.”*

Under the Public Records Act and the selection list, vocational education institutions must retain assessment forms for examinations for up to two years after graduation. The Model DSP Education MBO contains guidelines for retention periods regarding the administration of exams and the exam papers produced. If the assessment form is included in the exam paper, the exam paper must also be retained for two years.

While there may be a requirement to retain certain results, this obligation does not prescribe where the data must be stored. These results may be retained within Ans, or alternatively, in the institution’s student information system. The following sections describe the retention periods as defined in Ans’ legal documentation, as well as how deletion and the configuration of retention periods are handled within Ans.

10.1 Retention periods in legal documentation

Ans’ Privacy Policy includes some information about data retention. It states that the retention of Customer Data is determined by the Customer in a DPA. However, Schedule 1 of the Ans DPA does not include specific retention periods:

> *“The Controller may determine the duration of personal data being processed by Processor. The Processor will store personal data no longer than necessary to provide the services requested by the Controller.”*

For other information than Customer Data, the Privacy Policy specifies that *“Ans stores it logs for 365 days, unless legal obligations prescribe that the log files are required, or for research in the context of a (suspected) security incident. During this retention period, customers may request access to this information. Please note that, if a customer requests* *access to log information beyond what is typically included in our services, an hourly rate may apply for the time spent fulfilling this request."*

Retention periods for insights are not determined.

Ans' Service Level Agreement includes info on retention periods for backups. Backups are created daily and stored on a hard disk of a different server in a different location.[118] Backups are retained for four weeks.

10.2 Data deletion within Ans

Certain data within Ans can only be soft deleted, meaning it is moved to the trash but not immediately removed. This type of data remains recoverable for 180 days, after which it is permanently deleted. In contrast, hard deleted data is permanently removed right away. The list below outlines all data types that are soft deleted. Any data not included in this list is permanently deleted immediately.[119]

Table 11: Overview soft deleted data

Soft deleted data	Comments
Results	
Users	will not be deleted permanently after 180 days
Courses	
Question banks	
Assignments	
Exercises	will not be deleted permanently after 180 days

Deleted courses, question banks, and users can still be accessed via the settings. When a student is deleted, their results are also moved to the trash. According to Ans this is to make the impact of deleting a student more transparent. However, these results can be restored without reinstating the user. This can be done in the assignment settings under "Removed results."
Deleted assignments are in the course settings. The ability to restore an assignment depends on the institution's privilege settings. In some cases, only an administrator has the rights to perform this action.

The Help Page alerts the reader on the following: *"When removing a student: The student number will be retained and the associated results will be anonymised."*

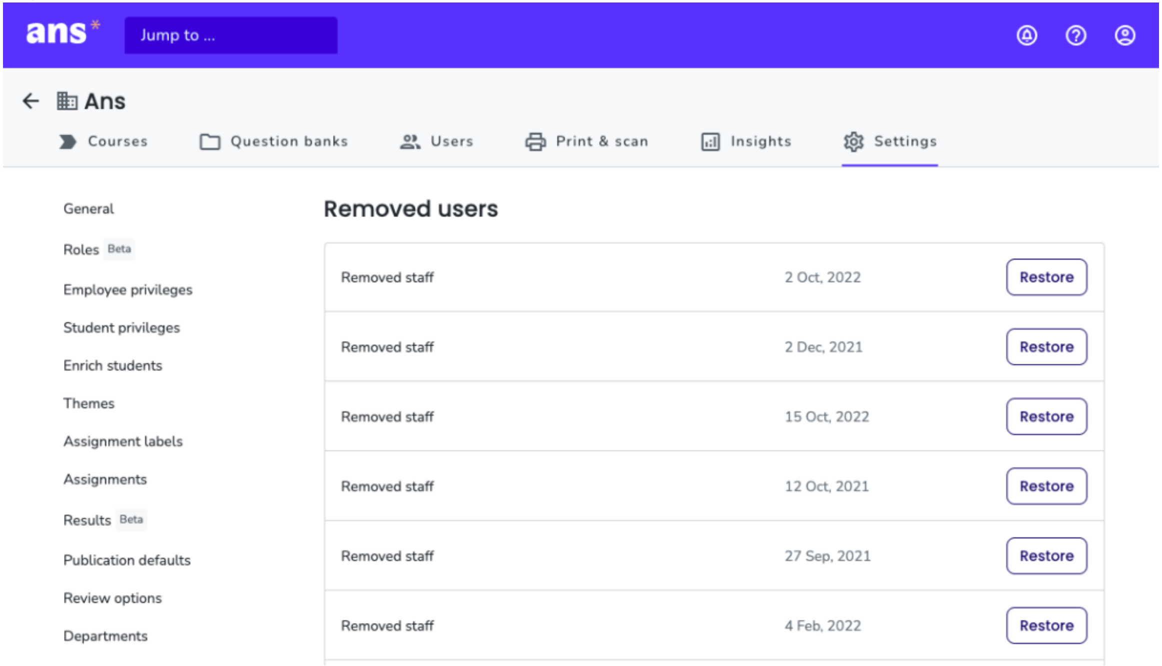
[118] Service level agreement (SLA), URL: https://support.ans.app/hc/en-us/articles/12661391857809-Service-level-agreement-SLA, last updated: 19 December 2023.

[119] Ans, 'Data deletion within Ans', URL: https://support.ans.app/hc/en-us/articles/15049613777809-Data-deletion-within-Ans, last viewed 22 April 2025.

10.3 Removed users

An overview of all deleted users within the institution is visible for the Administrator. According to Ans' web page all information is anonymized. For *"deleted employees"*, there is a list of 'Removed staff' and *"the date in which they were deleted"*.

Figure 7: Removed users



Removed users

Removed staff	2 Oct, 2022	Restore
Removed staff	2 Dec, 2021	Restore
Removed staff	15 Oct, 2022	Restore
Removed staff	12 Oct, 2021	Restore
Removed staff	27 Sep, 2021	Restore
Removed staff	4 Feb, 2022	Restore

For *"deleted students",* the Administrator can see 'Removed student', the student ID and *"the date in which they were deleted"*. Administrators have the rights to restore removed users. Users that are "deleted" will remain in the Removed users tab at the school settings.

When restoring employees, Ans tries to match the email address, which is stored in the database. If the email address can be found, the employee will be restored. This can only be done if the email address is a validated email address of an activated account. For students, Ans checks if the student ID can be found in the removed users. If so, the student is restored, and all courses, assignments, results and other relevant information are restored.[120]

10.4 Results retention period – add-on

In the settings of the institution, the admin has the possibility to define the minimum required retention period of how long assignment results are kept. The admin can set the years until results are anonymised and select the years until results are permanently deleted. This feature is available as an **add-on**, meaning it is not included in the standard software package.

The anonymisation and deletion of results are part of a daily check. During this process, Ans reviews the end date of the timeslot in each assignment to determine whether the

[120] Ans, Instructions for administrators, School settings, 'Removed users', URL: https://support.ans.app/hc/en-us/articles/9891636390161-Removed-users, last viewed 11 December 2024.

configured retention period has been reached, triggering the anonymisation or deletion of the results.

- If there are multiple timeslots in the assignment, the timeslot with the most recent end date is used.
- If the timeslot is deleted after the assignment has been taken, Ans will remember the end time of the deleted timeslot and use that date to anonymise and delete the results.
- If a timeslot is edited or created, then the end time of the assignment is recalculated.

Anonymising results means that all references to a participant are rendered untraceable. Once an assignment has been anonymised, the Taking, Review and Results pages are removed from the assignment. Attempting to access these pages will result in an error, as they no longer exist. This action is irreversible. The metrics in the assignment insights remain after the assignment has been anonymised. This allows users to still see the details regarding the marks, points and other characteristics of the assignment. Once an assignment has been anonymised, this will be shown in the assignment log. The message 'This assignment has been anonymised' will appear.

Additionally, it is possible to permanently delete results via the Results retention period. When the results of an assignment are deleted, they are permanently deleted from the Ans servers. This action also deletes the metrics in the assignment insights. This cannot be reversed.

According to Ans's Support Article, *"Ans has a limit of 100 assignments per school per day that can be anonymised or deleted. This means that if the results retention period gets enabled, and there are more than 100 assignments that can be anonymised or deleted, it can take longer th[a]n the set years to anonymise or delete the results"*

Part B. Lawfulness of the processing

The second part of the DPIA assesses the lawfulness of the data processing. This part contains an assessment of the legal grounds of both the institutions and Ans Exam B.V, the processing of special personal data, the application of purpose limitation, the necessity of the processing, and the application of data subjects' rights.

11 Legal grounds

To be permissible under the GDPR, the processing of personal data must be based on one of the legal grounds mentioned in Article 6 (1) GDPR. This chapter touches upon the legal grounds available to institutions in their role as data controllers. However, the primary focus will be on the legal bases available to Ans, when it processes personal data for its own purposes.

11.1 Legal grounds educational institutions

This (system) DPIA focuses on the data processing that is technically possible or result from how Ans is set up. Institutions must assess for themselves whether there is a sufficient legal basis for each purpose when they use Ans's features (e.g. to conduct exams). An examination tool such as Ans is essential for facilitating education, conducting assessments, and complying with statutory obligations under the Adult and Vocational Education Act (WEB) and the Higher Education and Research Act (WHW). For data processing related to their educational tasks, the legal basis will usually be that it is necessary to perform a task carried out in the public interest.

11.2 Legal grounds Ans

Ans acts as a data processor and processes personal data based on the instructions of the institution, which is the data controller. Because Ans carries out these processing operations on behalf of the institution, the legal grounds used by the education institution also applies to Ans as the processor.

However, Ans also processes personal data for its own purposes. This section focuses on assessing Ans's legal grounds for such processing. To properly evaluate the legal basis, it is important to have a clear understanding of the purpose(s), the personal data processed, and the capacity in which they are processed, as these aspects are not clearly defined in the legal documentation. For this reason, the section begins with clarifying the roles, after which the legal bases of Ans are assessed.

11.2.1 Lack of clarity in data processing roles

According to Schedule 1 of the Ans DPA, the purpose for processing personal data under the Agreement is *"to help professors to review written exams, digital exams and all kind of assignments. It enables professors to review more efficient and gives them the opportunity to provide better feedback to the students".*[121] This description of the purpose in Schedule 1 lacks specificity regarding the purposes for which Ans processes personal data on behalf of the institutions.

Ans's privacy policy provides some further detail, stating that *"Ans may access and use Customer Data*[122] *as reasonably necessary and in accordance with the Customer's instructions in order to: (a) provide, maintain and improve the Services; (b) to prevent or address service, security, technical issues or at a Customer's request in connection with customer support matters; (c) as required by law or as permitted by the Data Request Policy and (d) as set forth in our agreement with the Customer or as expressly permitted in writing*

[121] Schedule 1 Ans DPA.

[122] Content and information submitted by users to the services is referred to in this policy as "Customer Data."

by the Customer." However, the distinction between processing carried out on behalf of the institution and processing for Ans's own purposes remains ambiguous. The privacy policy also includes language that suggests Ans engages in independent data processing, for instance: *"We use other kinds of information in providing the Services. Specifically: To understand and improve our Services. We conduct research and analyze trends to better understand how users are using the Services and improve them. …"* This suggests that when Customer Data is used to improve the services, Ans acts as a processor, whereas when Ans uses "other kinds of information" for service improvement, it does so as a controller.

The vagueness makes it difficult to determine the exact scope of Ans's role as a data processor versus that of an independent data controller. The lack of clarity is also reflected in how personal data is categorized and described in the legal documentation. While the privacy policy draws a distinction between Customer data and 'other information' such as service usage data, account data, and marketing data, there is a noticeable overlap with the personal listed in Schedule 1 of the DPA. For instance, account creation details, school setup information, contact data and certain log data (like IP addresses) appear in both. Common identifiers such as name and email address are mentioned in both the DPA and the 'other information' section of the privacy policy. This overlap between personal data and purposes of the processing blurs the line between the data processed on behalf of the institution and data processed for Ans's own purposes, making it difficult to clearly define the roles and responsibilities.

For some processing activities, however, it seems reasonable to suggest that Ans processes personal data for its own purposes, for example:

- To research and analyse trends to improve the services
- To send emails about new product features or news (optional, opt-out available)
- To use account data for billing and account management
- To contact users for invoicing, account updates, and similar reasons
- To use contact information for marketing and advertising (optional, opt-out available)
- To investigate and prevent abuse, fraud, and security issues

Emails about changes in the software or how to work with the application are part of Ans' services in which Ans Exam B.V. would act as processor. For other emails, such as the one in which socks can be won, are for Ans own purposes as a data controller.

Please note: while the legal grounds of the institutions are out of scope of this DPIA, it is important to highlight that all service (notification) emails that are sent by Ans as processor on behalf of the institution contain open tracking which trigger the applicability of the ePrivacy Directive.

11.2.2 Legal grounds Ans

The legal grounds for Ans are discussed below.

<u>Billing and account management</u>

Ans processes the personal data in connection with the contractual relationship with the institution for their own purposes, in its capacity of data controller. This data includes contact details for invoicing and other information collected during service delivery, which is also used to generate service reports as evidence of the services provided.

This processing is based on Ans's legitimate interests (article 6(1)(f) GDPR):

- The processing is necessary to manage the contractual obligations with the institution.
- The personal data processed are limited to what is essential for invoicing and should be limited to a minimum for the purpose of service verification.
- The impact on data subjects is minimal, as the processing aligns with their reasonable expectations within the contractual context.

The processing of personal data for the purpose of billing and account management is lawfully based on Ans's legitimate interests in accordance with Article 6(1)(f) GDPR.

Marketing Communications.

Ans processes personal data such as email addresses and contact details for its own purposes when sending (optional) marketing communications, including emails about new product features, updates, and promotional materials. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest (recital 47 GDPR). However, as described in Section 3.3.26 of the Technical Appendix, the marketing emails include tracking links and pixels, which trigger the application of the ePrivacy Directive. The use of such tracking technologies requires prior consent under Article 5(3) of the ePrivacy Directive. If consent is not obtained, the processing is considered unlawful under the ePrivacy Directive. Consequently, a legitimate interest assessment would not justify the processing in this context.

In addition to this, Ans possibly uses contact information of staff that were initially processed for another purpose (e.g. providing access to the services). Depending on the context of the mailing, a compatibility assessment (article 6(4) GDPR) can be warranted.

Product improvement

Ans processes both customer data and 'other information' to improve its services and the application. While these purposes are mentioned in Ans's privacy policy, they are not included in Schedule 1 of the Ans DPA. The instruction from the institution is therefore missing. Although product improvement could potentially align with the purposes of the institutions (See also Section 13) it is difficult to assess whether the other legal requirements for such processing are met. There is limited information available regarding the nature of the personal data used for this purpose, the safeguards in place to prevent negative consequences, and what those consequences might be. If the processing does not meet the compatibility test of Article 6(4) GDPR, the processing will not be compatible with the original purpose, and Ans would therefore lack a valid legal basis to carry it out.

Security purposes

Ans uses system logs for security purposes to ensure proper system functioning, detect and prevent errors, and maintain operational continuity. This processing is based on Ans's legitimate interests (article 6(1)(f) GDPR):

- Ans has a legitimate interest ensuring that their product operates securely and reliably.
- While logging is in principle necessary for achieving the stated purposes, the current implementation of application logging goes beyond what is strictly necessary. The application logs capture extensive personal data (including user IDs, IP addresses, content (e.g. exam answers) and timing details) which may be useful for debugging, but routinely logging this volume and details is not proportionate to the legitimate interests.
- Continuous and excessive logging increases the risk of misuse or data breaches.

While Ans has a legitimate interest in using logs to maintain the system secure, the current practice of extensive routine application logging is not proportionate and not in line with the principle of data minimisation. For this reason, the current processing does not meet the requirements of Article 6(1)(f) GDPR.

Cookies

The support site (help center)[123] and the system status site[124] that are both accessible through the Ans application do not have a cookie banner. The help center is provided by Zendesk. On the Zendesk pages, Google Tag Manager and Google Analytics are present, also setting cookies corresponding to those services. If the user instead of the help center visits the status page, also linked in the footer of the Ans application, Google Tag Manager and Google Analytics were also present, including the corresponding cookies. See also Section 3.2.11 and 3.2.12 of the Technical Appendix.

Under the ePrivacy Directive, tracking cookies require the user's prior consent. Since no cookie banner or consent mechanism is presented on the support site, no valid consent is obtained, making this processing of personal data unlawful.

Update after completion of Part A

In response to the full draft of this DPIA, Ans has disabled tracking in their Zendesk environment by removing Google Tag Manager and Google Analytics. Google Tag Manager and Google Analytics contained in the status site were removed by Ans at the end of May 2025.[125]

[123] Available at https://support.ans.app.

[124] Available at https://status.ans.app.

[125] Feedback Ans 28 May 2025, verified by Privacy Company on 23 June 2025.

12 Special category data

Special categories of data are *“personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation”* (Article 9(1) GDPR). With special categories of data, the principle is one of prohibition: these data may not be processed. The law contains specific exceptions to this rule which must be interpreted strictly (article 9(2) GDPR).[126]

According to Schedule 1 of the Ans DPA, no special categories of personal data, criminal data, or national identification numbers (BSN) are processed within the Ans environment. While students may be granted additional time to complete an exam, either by adjusting settings manually or importing this information from the student information system, Ans does not register or process the underlying reason for this accommodation. As such, there is no processing of health data or other special category data within Ans in this context. Consequently, no further assessment under Article 9 GDPR is required.

[126] CJEU 4 July 2023, ECLI: EU:C:2023:537 (Meta vs Bundeskartellamt) paragraph 76. And see, to that effect, judgments of 17 September 2014, Baltic Agro, C 3/13, EU:C:2014:2227, paragraph 24 and the case-law cited, and of 6 June 2019, Weil, C 361/18, EU:C:2019:473, paragraph 43 and the case-law cited.

13 Purpose limitation

The principle of purpose limitation is that data may only be *“collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) GDPR not be considered to be incompatible with the initial purposes”* (Article 5(1)(b) GDPR). In essence, this means that a controller must specify a clear and specific purpose for collecting personal data and ensure that any further processing remains compatible with that original purpose.

Ans processes personal data for the purpose of improving its services. As stated in its privacy policy, this includes efforts *“to understand and improve our Services”* through research and trend analysis. While it is not fully transparent what specific types of information is used for these purposes, it is evident that Ans also uses Customer Data (data originally submitted by users through the platform) for product improvement (see Section 8).

To analyse Customer Data for product improvement, Ans uses Redash.[127] This is self-hosted and the data is used only internally according to Ans. [128] Nevertheless repurposing Customer Data (and ‘other information’) for product development and analytics constitutes a further processing under Article 6(4) GDPR, as the personal data were initially collected for a different purpose: to provide educational services (administering and grading exams). Although it is not entirely clear to what extent Customer Data or other information is used for product improvement, making a full assessment difficult. Any such further use of personal data for product improvement should be assessed in accordance with Article 6(4) GDPR.

[127] Redash helps you make sense of your data, URL: https://redash.io/, last viewed: 21 April 2025.

[128] Feedback Ans 28 May 2025.

14 Necessity and proportionality

14.1 The concept of necessity

The concept of necessity in Data Protection comprises two related principles, namely proportionality and subsidiarity. The personal data may only be processed if it is necessary for the specific purpose pursued by the processing activity. Proportionality requires that any interference with the data subject's privacy is not excessive in relation to the legitimate purpose of the processing. In other words, the scope and intensity of the processing must be proportionate to the objective being pursued. Subsidiarity means that the purposes of the processing cannot reasonably be achieved with other, less invasive means. If there are alternative measures that are less invasive to the data subject's rights, those alternatives must be used instead.

Proportionality demands a balancing exercise between the interests of the data controller and the data subject's rights. Data processing is proportionate only if the amount and type of personal data processed is limited to what is strictly necessary for achieving the stated purpose. If the purpose can be achieved by processing fewer personal data, the controller needs to reduce the amount of personal data accordingly.

Therefore, essentially, the data controller may only process personal data that is strictly necessary to achieve the legitimate purpose. Any processing of data that the controller can do without is not permitted. The application of the principle of proportionality is therefore closely related to core data protection principles set out in Article 5 GDPR, particularly the principles of data minimization, purpose limitation, and lawfulness, fairness and transparency.

14.2 Assessment of the proportionality

The key questions are: are the interests properly balanced? And does the processing not go further than what is necessary?

To assess whether the processing is proportionate to the interest pursued by the data controller(s), the processing must first meet the principles of Article 5 of the GDPR. These principles (such as lawfulness, fairness, transparency, purpose limitation, data minimization, and accuracy) form the legal foundation of all data processing activities. Compliance with these principles is not optional; they are binding legal obligations that must be met for any processing of personal data to be considered lawful and legitimate under the GDPR.

14.2.1 Lawfulness, Fairness, and Transparency

Data must be 'processed lawfully, fairly and in a transparent manner in relation to the data subject' (Article 5(1)(a) GDPR). This means that data subjects must be adequately informed about the processing of their data, that all the legal conditions for lawful data processing must be fully satisfied adhered to, and that the processing must comply with principle of proportionality, meaning it should be necessary and not go beyond what is needed to achieve its purpose.

14.2.1.1 Lawfulness

This subsection examines the legal conditions for the data processing and the lawfulness of international data transfers.

Incomplete description of processing activities in DPA

Schedule 1 of the Ans DPA is incomplete, particularly regarding: (1) the specified purpose of the processing (see also Section 4.1), (2) the description of the processing activities (see Section 3), (3) the categories of personal data being processed (See Section 2.2). While individual institutions may have negotiated more detailed or comprehensive agreements, this version of Schedule 1 serves as the reference point for this assessment. The noted gaps are therefore important to highlight. When the description of processing activities in the DPA is incomplete, it fails to meet the requirements of Article 28 GDPR. Consequently, the necessary instructions from the institution as controller to Ans as processor are effectively missing.

Sub-processer list in Ans' DPA

The sub-processor list in Ans' DPA (Table 6) is not comprehensive as it omits certain sub-processors (Appsignal). It also fails to provide a complete account of the personal data processed by those that are included in the list. For example, Cloudflare also processes content data, which includes most of the data flowing through their system (with the potential exception of uploads and paper exams), while Ans' DPA only mentions IP addresses (see also Section 3.3.1). Besides name, student number and files and answers of participants, TransIP also processes IP address, browser info, and image / sound data uploaded by students. Besides the personal data listed in Schedule 1 of the DPA, Mailerlite processes also email interaction data (open and link actions, if users show external images in the email and/or click on links in the email) when emails are sent, as well as IP addresses and browser info. Also, for Zendesk the listed personal data is incomplete. Next to name, email address and role, Zendesk also processes IP addresses, browser info and support requests.

DPA TransIP

The annexes of the DPA with TransIP B.V. list all possible options (personal data etc.) and states that only the options relevant to the client's specific situation apply. This does not meet the requirement of a clear and specific instruction under Article 28(3) GDPR as it lack sufficient specificity and leaves room for interpretation. As a result, it is not evident which processing activities are actually authorized by Ans as processor.

Processing location SorryApp

SorryApp is a processor for Ans. Sorry App primarily hosts on Amazon Web Services. Although their publicly available sample DPA states that international transfers will only be made after written permission by the customer, their privacy policy states their servers are in the United States. The sample DPA is incomplete or incorrect when it comes to international transfers. If these provisions are not correctly addressed, there is a risk that no valid transfer mechanism is in place. For example, SorryApp is not certified under the EU-U.S. Data Privacy Framework (DPF), meaning that, in the absence of such certification, the transfer would require Standard Contractual Clauses (SCCs) and a documented Data Transfer Impact Assessment (DTIA) to ensure compliance with Chapter V of the GDPR.

14.2.1.2 Fairness

Fairness is an overarching principle which requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected, or misleading to the data subject. There are several circumstances that might be unexpected for the data subject.

Lack of transparency in user impersonation

When an administrator assumes identity of another user, all actions are logged as being performed by the impersonated user, without mentioning that impersonation was used. The start of assuming the identity of another user is not shown in the interface. Ans has confirmed that impersonating an account is logged, but that the information is not (yet) shown in the interface.[129] This information is thus not accessible to administrators or end users.

Users are not informed and most probably do not expect that someone else may act under their account, nor can they distinguish between their own actions and those taken by an administrator impersonating them. As a result, users may be unfairly held accountable for action they did not perform, without any indication that impersonation incurred. This absence of visibility creates an uneven power dynamic and can lead to a loss of confidence in the platform.

Email tracking

Ans regularly sends notification emails to users (e.g., when a test has been submitted or when a grade is available) through Amazon SES. These emails contain a tracking pixel to track when a user views the email (see Section 3.3.12 of the Technical Appendix). This information is then surfaced in the user's email log (see Section 1.5). The fact that staff members can see whether or when a user has read or not read the email (something that is likely not clear to users) raises concerns about fairness, as it might be unexpected, and this information could be potentially used against the users (detrimental).

Insights reviewer alignment

Ans offers staff members further insights into tests on multiple levels. Insights are split between assignments, questions, objectives and reviewer alignment. Reviewer alignment shows for each question:[130] (1) the alignment of grading between different reviewers: good, deviation or needs attention, (2) the total number of results, duration of grading and average number of points given, and (3) a breakdown per reviewing staff member, showing the number of results reviewed, the time spent reviewing, and the average number of points given.

While it may be reasonable to monitor overall grading alignment between different reviewers to ensure consistency, providing a detailed breakdown per individual reviewer (including time spent reviewing) appears disproportionate and could create a chilling effect.

[129] Feedback Ans 28 May 2025.

[130] Alignment insights, URL: https://support.ans.app/hc/en-us/articles/360016943257-Alignment-insights, last updated: 29 July 2024.

Feedback students

At the end of an assignment, students can leave comments or feedback, which are shown to staff along with a link to the student's test result and personal details (see Section 1.1.5). Although the form states that the "comment will be shares with the instructors of this course," it remains unclear whether this also includes the student's name. This is particularly relevant as exams are often reviewed anonymously to promote impartiality (by default, anonymous grading is enabled, see Section 1.1.4). The lack of clarity may lead to misunderstandings about the level of anonymity and could discourage students from providing honest feedback. To ensure fairness, students should either be given the option to submit feedback anonymously or the interface should clearly state that the comment and the student's name (and other details) will be visible to the instructors.

14.2.1.3 Transparency

The principle of transparency not only ensures that consent must be informed but that full transparency of data practices and rights is ensured to users. In the case of children, this means that information relating to data processing must be comprehensible, recognizable and accessible to them (Article 12 GDPR).

Cookie policy Ans

Ans's Cookie Policy is included in its Privacy Policy[131] and aims to give context on the cookies and technologies used by Ans. As outlined in Section 2.4, the Cookie Policy fails to provide a comprehensive list of cookies, technologies, and their retention periods.

14.2.2 Data minimisation and privacy by design

The principles of data minimisation and privacy by design require that the processing of personal data be limited to what is necessary. In accordance with Article 5(1)(c) of the GDPR, the data must be *'adequate, relevant and limited to what is necessary for the purposes for which they are processed'*. This means that the controller may not collect and retain data that are not directly related to a legitimate purpose. According to this principle, the default settings for the data collection should be configured to favour the most privacy-friendly options, thereby minimising data collection.

Application logging

Amazon Cloudwatch is used for internal application logging, only available to authorised Ans employees. These logs include the user identifier, IP-address, request URL, content data (exam answers, notes, discussions) and timing information (e.g. how long it took to answer or grade a question). For more details, see Section 4.2.3 of the Technical Appendix. While capturing full incoming requests can be useful for debugging, routinely logging such a wide volume and variety of personal data raises concerns under the data minimisation principle. A more proportionate approach would be to only enable detailed logging when necessary for troubleshooting. In addition, logging timing data in application logs does not appear strictly necessary.

14.2.3 Accuracy

The principle of accuracy, as set out in Article 5(1)(d) of the GDPR, requires that personal data be accurate and, where necessary, kept up to date. It also requires controllers to take

[131] Ans Privacy Policy, last reviewed 2 September 2024, URL: https://www.ans.app/privacy.

reasonable steps to ensure that inaccurate personal data, in relation to the purposes for which it is processed, is promptly erased or corrected.

In line with the accuracy principle, Ans does not have any technical or functional restrictions that prevent institutions from correcting or updating personal data. The platform also supports both manual and automated account creation, such as through an API. The latter reduces the risk of human error and helps maintain up-to-date and accurate records.

14.2.4 Storage limitation

The principle of storage limitation requires that personal data *'shall not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed*' (Article 5(1)(e), first sentence, GDPR). This principle therefore requires that personal data be deleted as soon as they are no longer necessary to achieve the purpose pursued by the controller. The second sentence of these provisions provides an exception: '*personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')* (Article 5(1)(e), second sentence, GDPR).

Ans' Privacy Policy includes some information about data retention. It states that the retention of Customer Data is determined by the Customer in a DPA. However, Schedule 1 of the Ans DPA does not include specific retention periods:

> *"The Controller may determine the duration of personal data being processed by Processor. The Processor will store personal data no longer than necessary to provide the services requested by the Controller."*

Ans uses soft and hard deletion mechanisms. Soft-deleted is moved to "trash" where it remains recoverable for up to 180 days before permanently deleted. This applies to results, users, question banks, assignments, and exercises. However, not all soft-deleted data is subject to permanent deletion after his period. Users and exercises remain stored indefinitely unless manually removed.

An overview of all deleted users within the institution remains visible to administrators. According to Ans' web page all information in this view is anonymized. For deleted employee accounts, a list of 'removed staff' is available, including the date on which individual was deleted.

For employee accounts, all attributes are deleted except for their role and system logs. For student accounts, the student number is only deleted upon permanent removal, which requires submitting a support request with Ans. When a student is deleted, their results are also soft deleted but can be restored independently of the student account. Similarly, deleted assignment remain accessible in the course settings and may be restorable (depending on the settings).

This retention setup may result in personal data being stored longer than necessary for the purpose it was collected. In addition, while Ans offers functionality that allows institutions to define retention and anonymisation periods for assignment results, this feature is only available as an add-on and not included in the standard software package (see also Section 10.4). As a result, institutions that do not enable this feature may retain personal data longer than necessary, increasing the risk of non-compliance with storage limitation obligations.

14.2.5 Integrity and confidentiality

Personal data must be processed in a way that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. This requirement is set out in Article 5(1)(f) GDPR reinforced by the technical and organisational safeguards required under Article 32(1) and (2) GDPR. These provisions obligate controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Such measures must take into account the nature, scope, context, and purposes of the processing, as well as the risk to the rights and freedoms of data subjects.

Impersonation logging not visible in UI
As described in Sections 1.5 and 14.2.1.2, actions taken during impersonation are logged under the impersonated user's identity, without any indication in the user interface that impersonation took place. Although Ans confirms that impersonation is logged at system level, the absence of visibility in the interface limits the ability of administrators to determine who actually performed the actions. If logs are inaccessible or not clearly linked to the actual actor, the audit trail becomes incomplete and potentially misleading. This increases the risk of undetected misuse and hinders the ability to investigate or respond to unauthorized actions.

One-time passwords
Staff can generate a one-time password for a student, bypassing user's usual account password or SSO to access a test. While this action is logged, the one-time password grants full access to the student's account, not just the relevant test. This means staff or invigilators could create a one-time password and access the student's account and personal data unrelated to the exam, including information outside of their own department or access rights. This setup undermines the integrity of the access controls by allowing broader access than is necessary for the intended purpose. There are valid use cases for allowing staff to generate a one-time password, such as assisting students who have forgotten their credentials at the start of an exam. However, such access should be limited in scope: the one-time password should grant access only to the specific exam it was generate for, rather than to the student's full account, as the latter can lead to unauthorized access to personal data.

Security incidents
During this DPIA, two security incidents were identified. Both were reported to Ans, who took prompt action to resolve them. Ans could not fully rule out that the security issues had been exploited by unauthorised third parties. Given the nature of the security issues, this is not unexpected. The amount of logging required to rule out misuse would probably have breached the principles of data minimisation and storage limitation.

However, Ans did not explicitly notify the institutions (the data controllers) about the security incidents, even though both incidents could meet the criteria for a reportable data breach. The institutions are, as data controllers, ultimately responsible for the data breach reporting obligations. They may also have additional information available (from own log files or reports of abnormal behaviour by third parties), giving them a better position to determine if a data breach took place. The incidents were mentioned in passing in changelogs, but full details on the security incidents were not provided. It was, for example, not communicated that one of the issues allowed full arbitrary user access.

This raises concerns that Ans may lack adequate procedures for identifying security issues that may require notification as a data breach, as well as appropriate protocols for timely reporting such security issues to the relevant parties. In the absence of such protocols, institutions are limited in their ability to meet their own legal obligations regarding breach notifications and response.

14.3 Assessment of the subsidiarity

The key question is whether the same goals can be reached with less intrusive means in accordance with the principles of data minimisation and necessity under Article 5(1)(c) GDPR.

<u>Single-Sign On</u>

When students are invited by an administrator, they receive an invitation email to set their password. All transactional/notification emails contain open tracking (as discussed in Section 1.4). This invitation email is not sent if the organisation forces the use of single sign-on, as in that case there is no need to set a password. Therefore, there are less intrusive means available to provide access to Ans to students. With enforcing the single sign-on authentication with local accounts or the standard Microsoft/Google login options are disallowed. If the education institution sets up a custom domain (e.g., ans.university.com, available in the 'Campus' package), users will be automatically redirected to the SSO-endpoint to authenticate, skipped the Ans sign-in page.[132] This functionality also allows sending emails from the customer's domain.

<u>Alternatives for Google services</u>

Besides the Google SSO integration, Ans incorporates multiple Google services, including Google Charts, YouTube, Google Calendar (used in surveys for teachers) and Google Tag Manager (when users consent to the use of cookies).

Although Google states that it acts as a processor in some contexts (e.g., for Google Analytics), in many cases Google qualifies as a separate data controller, and these services are not always implemented under the control or contractual framework of the institution. As such, there is a risk that personal data is shared with or accessible to a third-party controller without a clear lawful basis or adequate safeguards, resulting in a loss of control for both the user and the institution.

[132] Custom domain [Campus], URL: https://support.ans.app/hc/en-us/articles/16632996288913-Custom-domain-Campus, last updated: 3 February 2025.

The incorporation of the Google services does not meet the subsidiarity principle. The same functionality offered by these services could be achieved through less privacy-invasive alternatives. For example, Ans could use open-source or other tools for data visualization, authentication, or calendar integration, under a clear DPA. By choosing such alternatives, data processing can remain fully within the boundaries of a controllable and auditable environment.

15 Data Subject Rights

The GDPR grants data subjects the right to information, access, rectification and erasure, object to profiling, data portability and file a complaint. It is the data controller's obligation to provide information and to duly and timely address these requests. If the data controller has engaged a data processor, the GDPR requires the DPA to include that the data processor will assist the data controller in complying with data subject rights requests. This chapter assesses whether institutions and Ans meet the GDPR requirements relating to data subjects' rights and whether data subjects can effectively exercise such rights.

15.1 Right to information

Data subjects have a right to information (Articles 12-14 GDPR). This means that data controllers must provide people with easily accessible, comprehensible and concise information in clear language about, inter alia, their identity as data controller, the purposes of the data processing, the intended duration of the storage and the rights of data subjects.

Because Schedule 1 of the DPA is incomplete and lacks sufficient specificity regarding the processing activities, this can undermine the institution's ability to fully meet its transparency and accountability obligations under the GDPR. In addition to this, due to the lack of clarity regarding which personal data is processed for which purpose and the blurred division of roles between the institutions and Ans, it becomes challenging for either party to fully and/or accurately meet their information obligations under the GDPR.

15.2 Right to access

Data subjects have a fundamental right to access personal data concerning them (Article 15 GDPR). Upon request, data controllers must inform data subjects whether they are processing personal data about them (directly, or through a data processor). If this is the case, they must provide data subjects with a copy of the personal data processed, together with information about the purposes of processing, recipients to whom the data have been transmitted, the retention period(s), and information on their further rights as data subjects, such as filing a complaint with the Data Protection Authority.

As part of the technical testing, Privacy Company performed Data Subject Access Requests (DSARs) where a student and an employee requested all their data and information about the processing, pursuant to Article 15 GDPR. This request is discussed in more detail in Chapter 4 of the Technical Appendix.

In the response to the DSARs, Ans referred to Schedule 1 of their Data Processing Agreement, which contains some, but not all the information requested under Article 15 GDPR. For the application data, they referred the user to the Ans platform, and for log data they provided some links to logging available in the Ans application.

Furthermore, Ans provided a copy of Amazon Cloudwatch logs and an extract of a Zendesk support ticket by one of the users. Information on other collected telemetry (e.g., through Cloudflare user monitoring, Google Analytics, Google reCAPTCHA, AppSignal) was not provided and it is unknown if such information would have been available or was already fully anonymised.

The Ans product does not have a feature to request all personal data relating to a specific student or employee. Due to this, users must manually visit every exam result, discussion, log and chat to retrieve all personal data for a user. In most cases, these pages will not (all) be available to the end-user: students are only able to access exam results during the publication window and the pages with logs on their activities are unavailable to them (except for the login history). Staff members are in a similar position for some of the logs, depending on their role in the course (instructors will be able to see all course information, but reviewers will not). Due to this approach, only an administrator can provide meaningful access to all application data and logs, which will take some effort as the personal data will be spread out over many different web pages.

Administrators do not have access to internal application logs (like the Amazon Cloudwatch logs) and can only request these through the Ans support channel. For this access, the Ans privacy policy also notes that additional costs may be involved:[133]

> *"Ans stores it logs for 365 days, unless legal obligations prescribe that the log files are required, or for research in the context of a (suspected) security incident. During this retention period, customers may request access to this information. Please note that, if a customer requests access to log information beyond what is typically included in our services, an hourly rate may apply for the time spent fulfilling this request."*

With support from Ans, the institution is in principle able to comply with access requests. However, retrieving all relevant personal data from the product can be difficult, as the data is spread across various parts of the platform. In practice, this makes the process cumbersome and prone to error, especially in the absence of clear internal procedures or checklists within the institutions. This is further complicated by the fact that Ans's responses lacked clarity regarding the division of responsibilities and did not clearly distinguish between processing carried out as a processor and as a controller.

15.3 Right to object

Data subjects have the right to object to processing based on legitimate interests or public tasks, as well as direct marketing (article 21 GDPR).

As described in Section 1.4, mails are sent to staff members notifying them of product updates, important changes and to request feedback through Mailerlite. Some of these mails can be considered direct marketing. Users can unsubscribe from some of these emails (updates and feedback requests) through a link in the email. Unsubscribing from a mailing list for direct marketing can be understood as an exercise of the right to object under Article 21 GDPR. However, Ans's privacy policy does not explicitly inform users of this right. It merely states that individuals can contact the company with questions about their data, its use, or their rights.

Additionally, Ans processes personal data for training purposes, such as improving recognition models, based on their legitimate interests. Since data subjects have the right to object to processing based on legitimate interests, students should be informed that

[133] Ans Privacy Policy, last reviewed 2 September 2024, URL: https://www.ans.app/privacy.

their exam data may be used for such purposes. Without clear information about this further processing, data subjects cannot effectively exercise their right to object.

15.4 Right to rectification

Data subjects have the right to rectify inaccurate or incomplete personal data (Article 16 GDPR). Ans does not contain any technical or functional restrictions that prevent institutions from complying with requests to rectify or amend personal data.

15.5 Right to erasure

Under Article 17 of the GDPR, data subjects have the right to erasure of their personal data in certain cases, such as when it is no longer needed, consent is withdrawn, or processing is unlawful.

As deletion is currently structured in Ans, it is possible for institutions to comply with its obligations under Article 17 GPDR, but doing so may require additional steps and coordination with Ans. While most data can be soft-deleted and eventually permanently deleted (see Chapter 10 and Section 14.2.4), certain data types (such as users and exercises) are not automatically removed after 180 days. Permanently the student number requires submitting a support request with Ans. This means that to fulfil a data subject's erasure request fully and in a timely manner, the institution needs to have clear internal procedures in place and involve Ans.

Part C. Discussion and Assessment of the Risks

This part concerns the description and assessment of the risks for data subjects. This part starts with an overall identification of the risks to the rights and freedoms of data subjects because of the processing of personal data in Ans. The risks will subsequently be classified according to the likelihood they might occur, and the impact on the rights and freedoms of the data subjects when they do.

16 Risks

In this section, this DPIA lists all privacy risks identified in the context of Ans used by institutions. Each privacy risk will be assessed based on the potential impact it has on the rights and freedoms of the data subjects, and on the likelihood the risk will in fact occur. Some privacy risks will automatically occur to some or all data subjects, others will have a high, medium, or low likelihood of occurring. The severity of the risk and the likelihood are assessed based on the factual description in Part A and the legal assessment in Part B of this DPIA.

Risk Assessment Framework
Risks to the rights and freedoms of the data subject ('privacy risks') occur when processing activities of personal data violate a right or freedom given to the data subject by the GDPR or any other legislation. High risks usually occur when a processing violates a legal protection of one of the fundamental rights as described in the European Charter of Fundamental Rights, but violations of other rights given by Union or Member State law may also constitute a privacy risk.

When assessing data processing activities, the potential risks to the rights and freedoms of individuals are considered. This involves examining:

- The possible negative consequences of the processing.
- The origin of these consequences.
- The likelihood (probability) that these consequences will occur.
- The severity (impact) of the consequences.

The risk analysis follows the methodology described by the British supervisory authority (ICO) for classifying risks. An objective assessment is made of the likelihood (probability) and the impact (severity) of potential negative consequences, such as physical, emotional, or material harm. The combination of the likelihood of harm occurring and the impact of that harm constitutes the resulting risk.

Risk Classification
To visually represent and classify the factors of likelihood and impact, a risk matrix is used.

Table 12: Risk matrix based on the ICO model

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

16.1 Identification of data protection risks

16.1.1 Loss of control – Incomplete description of processing activities in DPA

According to Article 28 (3) GDPR, data processing agreements should define the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the rights and obligations of the controller.

While individual institutions may have negotiated more detailed or comprehensive agreements, Schedule 1 of the Ans DPA serves as the reference point for this assessment. This Schedule 1 is incomplete, particularly regarding: (1) the specified purpose of the processing (see also Section 4.1), (2) the description of the processing activities (see Section 3), (3) the categories of personal data being processed (See Section 2.2). When the description of processing activities in the DPA is incomplete, it fails to meet the requirements of Article 28 GDPR. Consequently, the necessary instructions from the institution as controller to Ans as processor are effectively missing.

The likelihood that this risk materialises is reasonable, particularly because it is plausible (if not likely) that the incomplete Schedule 1 of the DPA is used by institutions as the basis for their data processing agreement with Ans. In such cases, the absence of a complete and specific description of processing activities, purposes, and categories of personal data means that the processor may act without adequate instruction from the controller. The impact for the rights and freedoms of data subjects could be severe, as it can cause misuse or mishandling of their personal data, reduced accountability, and limited ability to exercise their rights. **This constitutes a high risk.**

In response to the full draft of this DPIA, Ans has committed to updating Schedule 1 of the DPA in Q1 2026 and apply this new schedule to all existing and future customer agreements.[134]

16.1.2 Loss of control – Role division

The vagueness in role division between Ans as a data processor and as an independent data controller creates uncertainty around the exact scope of responsibilities. This lack of clarity is evident in overlapping personal data categories described in the DPA and Privacy Policy, blurring the line between data processed on behalf of institutions and data processed for Ans's own purposes.

For example: according to Ans's Privacy Policy, both Customer data and 'other information' may be processed for the purpose of improving and developing the product. While Customer Data is processed on behalf of the institution, and 'other information' is processed for Ans's own purposes, it remains unclear which categories of personal data fall under each, how that data are used, and what safeguards are in place. The current documentation is broadly worded and appears to allow the use of all personal data for product improvement, without clear boundaries or specifications.

There is limited transparency regarding the types of personal data involved in product improvement, the intended use, the duration of processing, and the measures taken to

[134] Feedback Ans 1 December 2025.

prevent adverse effects for data subjects. Without clarity and safeguards, there is a real risk that data is being used beyond its original purpose without a valid legal ground. If the processing does not pass the compatibility test under Article 6(4) GDPR, it would not be considered lawful, and Ans would lack an appropriate legal basis for such further processing.

If roles and responsibilities remain unclear, data subjects may face difficulties exercising their rights effectively. An example of this is the user's right to object to the (further) processing for product improvement by Ans. Data subjects are effectively unable to exercise their right to object under Article 21 GPDR, because they do not have enough information to understand that the processing is taking place in the first place. It is more likely than not that this risk occurs due to the factual situation. Not being able to effectively exercise rights has a high impact. **For that reason, it is a high risk.**

In response to the full draft of this DPIA, Ans has committed to updating their Privacy Statement as well as Schedule 1 of the DPA in Q1 2026 and apply this new schedule to all existing and future customer agreements.[135]

16.1.3 Inability to exercise data subject rights – Right to object direct marketing

As described in Section 1.4, staff members receive emails from Ans about product updates, important changes, and requests for feedback. Some of these mails may qualify as direct marketing. Although users can unsubscribe from some of these emails (updates and feedback requests) through a link in the email, Ans's privacy policy does not explicitly inform them of their right to object to direct marketing under Article 21 GDPR. It merely states that individuals can contact the company with questions about their data, its use, or their rights. This lack of clarity may prevent data subjects from fully understanding or effectively exercising their rights. It may also be unclear which emails serve which purposes and who the relevant controller is (Ans or the institution). The likelihood of this risk occurring is reasonable, but the impact is considered low, as data subjects can still unsubscribe via the unsubscribe link or contact Ans for clarification or to exercise their rights. **This qualifies as a low risk**.

In response to the full draft of this DPIA, Ans has committed to updating their privacy policy to include complete information on the right to object. They will also include additional sender information in their marketing emails. These changes will be completed in Q1 2026.[136]

16.1.4 Lack of transparency – List of sub-processors is incomplete

The sub-processor list in Ans' DPA (Table 4) is not comprehensive as it omits certain sub-processors (Appsignal). It also fails to provide a complete account of the personal data processed by those that are included in the list. For example, Cloudflare also processes content data, which includes most of the data flowing through their system (with the potential exception of uploads and paper exams), while Ans' DPA only mentions IP addresses (see also Section 3.3.1). Besides name, student number and files and answers of participants, TransIP also processes IP address, browser info, and image / sound data

[135] Feedback Ans 1 December 2025.

[136] Feedback Ans 1 December 2025.

uploaded by students. Besides the personal data listed in Schedule 1 of the DPA, Mailerlite processes also email interaction data (open and link actions, if users show external images in the email and/or click on links in the email) when emails are sent, as well as IP addresses and browser info. Also, for Zendesk the listed personal data is incomplete. Next to name, email address and role, Zendesk also processes IP addresses, browser info and support requests.

The likelihood that this risk materialises is reasonable, particularly because it is plausible (if not likely) that the incomplete Schedule 1 of the DPA is used by institutions as the basis for their data processing agreement with Ans. The impact on the rights and freedoms of the data subjects is high as well as the institutions as a controller cannot fully inform the data subjects, cannot control, and may have less control over any further use of the data. **The risk can be qualified as high.**

In response to the full draft of this DPIA, Ans has committed to updating Schedule 1 of the DPA with complete information on sub-processors in Q1 2026 and apply this new schedule to all existing and future customer agreements.[137]

16.1.5 Loss of control – DPA with TransIP lacks clear and specific instructions

The annexes of the DPA with TransIP B.V. list all possible options (personal data etc.) and states that only the options relevant to the client's specific situation apply. This does not meet the requirement of a clear and specific instruction under Article 28 (3) GDPR as it lack sufficient specificity and leaves room for interpretation. As a result, it is not sufficiently clear which processing activities are actually authorised by Ans as processor on behalf of the institution. This creates a risk that personal data may be processed without a clearly defined legal instruction, which undermines accountability and may result in unlawful or excessive processing.

The likelihood of the risk occurring is more likely than not, as the DPA is not tailored to the specific situation. This could have a serious impact on the rights and freedoms of the data subjects, as it may lead to a loss of control over their personal data e.g. due to a lack of purpose limitation. **Therefore, this is a high risk.**

In response to the full draft of this DPIA, Ans has indicated that TransIP is unwilling to amend the DPA. For this reason, Ans has chosen to migrate away from TransIP to Amazon S3.[138] This migration will be completed by the end of Q3 2026 for all files containing personal data (e.g., written exam answers and hand-in assignments). For other files, migration may take up to another year. As only basic visitor information (e.g., IP-address and browser information) is exchanged when retrieving such files, and TransIP's standard DPA mentions these personal data items, this situation seems acceptable.

16.1.6 Loss of control - Processing location SorryApp

SorryApp is a processor for Ans. SorryApp offers a status website, displaying the current availability of a software application. Although their publicly available sample DPA states that international transfers will only be made after written permission by the customer, their

[137] Feedback Ans 1 December 2025.

[138] Feedback Ans 1 December 2025.

privacy policy states their servers are in the United States. The sample DPA is incomplete or incorrect when it comes to international transfers. If these provisions are not correctly addressed, there is a risk that no valid transfer mechanism is in place. For example, SorryApp is not certified under the EU-U.S. Data Privacy Framework (DPF), meaning that, in the absence of such certification, the transfer would require Standard Contractual Clauses (SCCs) and a documented Data Transfer Impact Assessment (DTIA) to ensure compliance with Chapter V of the GDPR.

The likelihood that an insufficient transfer mechanism is in place is reasonable, given the conflicting documentation and the lack of clear contractual safeguards. If no appropriate legal basis governs the transfer, it would constitute an unlawful international data transfer. The impact on data subjects is high, as such transfers result in a loss of control over their personal data and increase the risk of access by third-country authorities without adequate legal remedies. **Therefore, this is a high risk**.

In response to the full draft of this DPIA, Ans has chosen to migrate away from SorryApp to StatusPal.[139] This status page platform offers a solution hosted within the EU. Privacy Company has done a brief assessment of the DPA with StatusPal and identified some shortcomings. Ans has committed to addressing these issues and moving to StatusPal in Q1 2026.[140]

16.1.7 Lack of transparency - User impersonation not visible in UI

Administrators can assume the identity of another user. Users are not informed and most likely do not expect that someone else may act under their account, nor can they distinguish between their own actions and those taken by an administrator impersonating them. As a result, users may be unfairly held accountable for actions they did not perform, without any indication that impersonation occurred. This absence of visibility creates an uneven power dynamic and can lead to a loss of confidence in the platform. Although impersonation events are logged, this information is not visible to either the impersonated users or administrators through the user interface. This lack of transparency limits accountability and undermines trust. In addition, the impersonation logs are inaccessible or not clearly linked to the actual actor, the audit trail becomes incomplete and potentially misleading. This increases the risk of undetected misuse and hinders the ability to investigate or respond to unauthorized actions.

The likelihood of the risk materialising when impersonation is used is certain, as this concerns a missing transparency feature: impersonation is logged but the relevant information is not yet implemented in the interface where users or admins could verify such events. The impact on data subjects is high. Without any way to detect or verify such actions, students may face unfair academic consequences or reputational harm, and their ability to exercise their rights under GDPR is limited. This directly undermines the principles of fairness, transparency, and accountability under Article 5(1)(a) GDPR. **Therefore, this is a high risk.**

[139] Hosted Status Pages & Monitoring | StatusPal, URL: https://www.statuspal.io/, last viewed: 3 December 2025.

[140] Feedback Ans 1 December 2025.

In response to the full draft of this DPIA, Ans has committed to including full information on the start and end of impersonation and the actions taken while impersonating to the user logs. These logs will be surfaced in the user interface and will be available in Q1 2026.[141]

16.1.8 Chilling effect – Email tracking notification emails

The open tracking functionality in service notification emails introduces a risk related to fairness and the potential for a chilling effect. Staff members can see whether and when a student has opened an email (e.g. results availability). This level of monitoring is likely not clearly communicated to the student and may be unexpected.

Although the content of these emails is not personal, the visibility of open status and timing may still create a chilling effect. The ability to view whether a student has read a message could create pressure to engage or respond in a certain way, or lead to negative assumptions being made if the student has not opened a message.

The probability of this risk is reasonable, given that the tracking feature is in active use and the visibility of tracking data to staff is a built-in function. This could have some impact on the rights and freedoms of data subjects, as the emails concern (only) service-related matters rather than personal communication. But the perception of being monitored (without clear notice) can still affect the student's trust and autonomy, especially since this is an educational setting. **This qualifies as a medium risk.**

In response to the full draft of this DPIA, Ans has committed to disabling tracking functionality in notification emails in Q1 2026.[142]

16.1.9 Chilling effect employees – Insights reviewer alignment

Ans offers staff members further insights into tests on multiple levels. Insights are split between assignments, questions, objectives and reviewer alignment. Reviewer alignment shows for each question:[143] (1) the alignment of grading between different reviewers: good, deviation or needs attention, (2) the total number of results, duration of grading and average number of points given, and (3) a breakdown per reviewing staff member, showing the number of results reviewed, the time spent reviewing, and the average number of points given.

While it may be reasonable to monitor overall grading alignment between different reviewers to ensure consistency, providing a detailed breakdown of individual reviewer behaviour, such as time spent per review, goes beyond what is necessary for ensuring grading consistency and constitutes a form of employee monitoring. This level of detail may create a chilling effect, where employees feel pressured or monitored. If the institution intends to work with this type of employee monitoring, prior consultation and approval from the Works Council (OR) must be sought, in accordance with labour law.

The likelihood of the risk occurring is reasonable due to the available functionality, and especially when there is limit transparency or control for the individuals being monitored. It

[141] Feedback Ans 1 December 2025.

[142] Feedback Ans 1 December 2025.

[143] Alignment insights, URL: https://support.ans.app/hc/en-us/articles/360016943257-Alignment-insights, last updated: 29 July 2024.

can undermine trust and affect employee well-being, and the processing most likely would not pass a legitimate interests test. For that reason, the impact to the rights and freedoms is high. **This qualifies as a high risk.**

In response to the full draft of this DPIA, Ans has indicated that their 'new grading experience' no longer offers 'time spent per review' information. This information will be fully removed from Ans in Q1 2026.[144]

16.1.10 Loss of control due to lack of transparency – Feedback students

At the end of an assignment, students can leave comments or feedback, which are shown to staff along with a link to the student's test result and personal details (see Section 1.1.5). Although the form states that the "comment will be shared with the instructors of this course," it remains unclear whether this also includes the student's name. This is particularly relevant as exams are often reviewed anonymously to promote impartiality (by default, anonymous grading is enabled, see Section 1.1.4. The lack of clarity about whether student names are shared alongside feedback may lead to a false expectation of anonymity. This could discourage students from providing honest or critical feedback.

The likelihood of the risk occurring is reasonable, especially if students are unaware their identity is disclosed, and the default is anonymous grading. The impact on the rights and freedoms of the data subjects is moderate, as it may affect the openness of the student (students might avoid providing direct or negative feedback out of fear it could influence how instructors perceive or grade them) compromise perceived fairness in grading and erode confidence in the assessment process. **This qualifies as a medium risk.**

After consulting with several clients, Ans decided to take the following approach to mitigate this risk: the interface will indicate that both the comment and the student's name are visible to instructors. Ans aims to have this implemented by the end of Q2 2026.[145]

16.1.11 Lack of transparency – Incomplete cookie information

Ans's Cookie Policy is included in its Privacy Policy[146] and aims to give context on the cookies and technologies used by Ans, but fails to provide a comprehensive list of cookies, technologies, and their retention periods.

This is a factual situation. The impact on the rights and freedoms of data subjects is high, because the lack of transparency is a violation of a principle of the GDPR, especially when tracking cookies or similar technologies are used. **The risk can be qualified as high**.

In response to the full draft of this DPIA, Ans has committed to updating their cookie policy with the required information in Q1 2026.[147]

[144] Feedback Ans 1 December 2025.

[145] Feedback Ans 1 December 2025.

[146] Ans Privacy Policy, last reviewed 2 July 2025, URL: https://www.ans.app/privacy.

[147] Feedback Ans 1 December 2025.

16.1.12 Lack of data minimisation – Application logging

Amazon Cloudwatch is used for internal application logging, only available to authorised Ans employees. These logs include the user identifier, IP-address, request URL, content data (exam answers, notes, discussions) and timing information (e.g. how long it took to answer or grade a question). For more details, see Section 4.2.3 of the Technical Appendix. While capturing full incoming requests can be useful for debugging, routinely logging such a wide volume and variety of personal data raises concerns under the data minimisation principle. A more proportionate approach would be to only enable detailed logging when necessary for troubleshooting. In addition, logging all content data and timing data in application logs does not appear strictly necessary.

This is a factual situation, so the likelihood of this risk occurring is more likely than not. The consequences for the rights and freedoms of data subjects are severe, as this constitutes processing that violates the principle of data minimisation. **This qualifies as a high risk.**

In response to the full draft of this DPIA, Ans has raised the argument that the current application logging is vital for fraud detection and requested by most institutions in their tender requirements.[148] This is a valid point, also given the main purpose of the Ans application: administering exams. However, this does not mean that unlimited application logging is warranted, and thus Ans has agreed to re-assess the application logging in Q2 2026, together with SURF. A clear overview of the personal data logged, access permissions, retention periods and the purposes and interests for the logging will be created. Where possible, data minimisation will be applied.

16.1.13 Loss of confidentiality – One-time passwords

Staff can generate a one-time password for a student, bypassing user's usual account password or SSO to access a test. While this action is logged, the one-time password grants full access to the student's account, not just the relevant test. This means staff or invigilators could create a one-time password and access the student's account and personal data unrelated to the exam, including information outside of their own department or access rights. This setup undermines the integrity of the access controls by allowing broader access than is necessary for the intended purpose. There are valid use cases for allowing staff to generate a one-time password, such as assisting students who have forgotten their credentials at the start of an exam. However, such access should be limited in scope: the one-time password should grant access only to the specific exam it was generate for, rather than to the student's full account, as the latter can lead to unauthorized access to personal data.

The likelihood of the risk occurring is reasonable, as the functionality exists, and its use is not limited. The potential impact is high, as it may result in unauthorized access to student data. **This qualifies as a high risk**.

In response to the full draft of this DPIA, Ans will ensure that one-time passwords are restricted in scope and grant access only to the specific part of the platform necessary for their intended purpose.[149] This work will be completed before the end of Q2 2026.

[148] Feedback Ans 1 December 2025.

[149] Feedback Ans 1 December 2025.

16.1.14 Loss of control – Personal data processed longer than needed

Ans uses soft- and hard-deletion mechanisms. Soft-deleted is moved to 'trash' where it remains recoverable for up to 180 days before permanently deleted. Not all soft-deleted data is subject to permanent deletion after this period. Users and exercises remain stored indefinitely unless manually removed. An overview of all deleted users within the institution remains visible to administrators. According to Ans' web page all information in this view is anonymized. For deleted employee accounts, a list of 'removed staff' is available, including the date on which individual was deleted.

For employee accounts, all attributes are deleted except for their role and system logs. For student accounts, the student number is only deleted upon permanent removal, which requires submitting a support request with Ans. When a student is deleted, their results are also soft deleted but can be restored independently of the student account.

The retention setup in Ans may result in personal data being stored longer than necessary for the purpose it was collected. In addition, while Ans offers functionality that allows institutions to define retention and anonymisation periods for assignment results, this feature is only available as an add-on and not included in the standard software package (see also Section 10.4). As a result, institutions that do not enable this feature may retain personal data longer than necessary, increasing the risk of non-compliance with storage limitation obligations.

There is a reasonable probability of the occurrence of the risk that personal data will be processed longer than needed. Storing personal data longer than needed leads to a loss of control. This can have a high impact on the rights and freedoms of data subjects. **For that reason, it is a high risk.**

In response to the full draft of this DPIA, Ans has indicated that they will be making several changes to the soft and hard deletion mechanisms.[150] The following changes will be made:

1) Users will also be hard-deleted 180 days after a soft-delete, in line with the other entities.
2) Administrators will have the option to hard-delete entities manually before the 180 days deadline of soft-deletion has passed, using a button in the interface.
3) Soft-deletion will no longer anonymise data immediately, but simply serve as a 'trash can', simplifying the mental model for users.

Similar functionality will also be available through the API, where this is not yet the case. These changes will be available before the end of Q2 2026.

16.1.15 Loss of control – Integrated Google Services

Besides the Google SSO options, Ans incorporates multiple Google services, including Google Charts, YouTube, Google Calendar (used in surveys for teachers), and Google Tag Manager (only when users 'Accept All' cookies). While Google positions itself as a processor for certain services such as Google Analytics, but for most integrations, Google considers itself an independent controller.

Although Google states that it acts as a processor in some contexts (e.g., for Google Analytics), in many cases Google qualifies as a separate data controller, and these services

[150] Feedback Ans 1 December 2025.

are not always implemented under the control or contractual framework of the institution. As such, there is a risk that personal data is shared with or accessible to Google as third-party controller without a clear lawful basis or adequate safeguards, resulting in a loss of control for both the user and the institution.

There is a reasonable probability of the risk occurring due to the integration of the different Google Services. The impact on the data subjects depends per service and can be categorised as 'some impact'. **For that reason, this is a medium risk.** The impact of processing IP addresses and browser information through Google Charts is lower than that of YouTube's processing of personal data, as the latter also processes personal data for advertising purposes.

In response to the full draft of this DPIA, Ans has committed to replacing Google Charts visible to students with a different solution before the end of Q3 2026.[151]

16.1.16 Inability to exercise data subject rights – Administrators not fully able to honour DSARs

The Ans product does not have a feature to request all personal data relating to a specific student or employee. Due to this, users must manually visit every exam result, discussion, log and chat to retrieve all personal data for a user. In most cases, these pages will not (all) be available to the end-user: students are only able to access exam results during the publication window and the pages with logs on their activities are unavailable to them (except for the login history). Staff members are in a similar position for some of the logs, depending on their role in the course (instructors will be able to see all course information, but reviewers will not). Due to this approach, only an administrator can provide meaningful access to all application data and logs, which will take some effort as the personal data will be spread out over many different web pages.

Ans helped to return some log files, but the information returned was not complete. For example, information on some collected telemetry (e.g., through Cloudflare user monitoring, Google Analytics, Google reCAPTCHA, AppSignal) was not provided. It is unknown if such information would have been available or was already fully anonymised.

With support from Ans, the institution is in principle able to comply with access requests, provided that Ans returns also all log files and telemetry. However, retrieving all relevant personal data from the product can be difficult, as the data is spread across various parts of the platform. In practice, this makes the process cumbersome and prone to error, especially in the absence of clear internal procedures or checklists within the institutions. This is further complicated by the fact that Ans's responses lacked clarity regarding the division of responsibilities and did not clearly distinguish between processing carried out as a processor and as a controller.

There is no dedicated tool or guide available for the administrator to easily answer a DSAR from a user. Without a dedicated tool, DSAR responses rely on manual processes, increasing the chance of accidental omissions or inconsistent data retrieval. In addition to this, administrators do not have access to all data. For this data they need the assistance of

[151] Feedback Ans 1 December 2025.

Ans, while Ans supported the request in the test case, not all personal data was returned. There is a reasonable possibility of the occurrence of the risk. The occurrence of the risk can have a severe impact on the data subjects. **The risk can be qualified as high.**

In feedback to the full draft of this DPIA, Ans indicated they never received a data subject access request from a customer.[152] Additionally, any data subject access requests from end-users are, per the DPA, forwarded to the controller. Due to this, it is difficult to determine the best set of requirements for a dedicated DSAR tool. Instead, Ans will create a guide on their support site to assist controllers in complying with DSARs. This guide will also point out that controllers can always ask Ans' support department for additional assistance to comply with a DSAR, in line with the DPA. Where useful, they will provide additional buttons in the user interface to easily export user data. A starting point for this is the dedicated user results page that was recently introduced. These enhancements will be realised before the end of Q3 2026.

16.1.17 Lack of adequate procedures for reporting security incidents

While two security incidents were detected and resolved during the DPIA, Ans did not fully inform the institutions about the scope of the issues, despite the fact that both incidents could qualify as reportable data breaches. Although the incidents were mentioned in passing in changelogs, the institutions were not provided with complete information on the severity of the issues and thus lacked the ability to make their own assessment as to the qualification of the incidents as a reportable data breach. This makes it difficult for institutions as controllers to meet their own legal responsibilities.

The likelihood of the risk occurring in reasonable, as it already occurred during the DPIA process. Without improved internal processes and awareness, similar incidents could go unreported in the future. The potential impact on data subjects is significant. If a data breach is not handled appropriately and reported in a timely manner, affected individuals may be left unaware of potential threats to their personal data. **This qualifies as a high risk.**

In response to the full draft of the DPIA Ans explained that their Incident Response Plan was followed. This process is part of their ISO 27001 certification. Even though this process was followed, controllers are ultimately responsible for assessing data breaches and their impact. For that reason, Ans committed to introducing a section with security advisories in their support portal.[153] The controller can subscribe to updates to this section. The security advisories section will be updated when:

1) An actual security incident and/or data breach occurred.
2) Security vulnerabilities in the Ans product were found that could significantly affect data subjects, where Ans cannot rule out misuse of their application.
3) Security vulnerabilities in third party dependencies (e.g., operating system, software frameworks) were announced that are actively exploited and where Ans cannot rule out misuse of their application.

Advisories will at least contain information on the (potentially) affected users and affected personal data, as well as technical details as far as they help the customer's security officer to judge the applicability of the security advisory to their institution.

[152] Feedback Ans 1 December 2025.

[153] Feedback Ans 1 December 2025.

16.2 Summary of risks

By representing the risks encountered according to their potential impact on the rights and freedoms of data subjects, a picture of the high and low risks associated with processing personal data in Ans emerges. This is displayed in the risk graph developed by the UK regulator ICO, as follows:

Table 13: Risk matrix based on the ICO model

Severity of impact	Serious harm	**Low risk**	**High risk** **1, 4, 6, 9, 13, 14, 16, 17**	**High risk** **2, 5, 7, 11, 12**
	Some impact	**Low risk**	**Medium risk** **8, 10, 15**	**High risk**
	Minimal impact	**Low risk**	**Low risk** **3**	**Low risk**
		Remote possibility	Reasonable possibility	More likely than not
	Likelihood of harm			

Part D. Description of risk mitigating measures

Part D describes the proposed (counter-)measures that are necessary to mitigate the risks found in Part C. This part also contains an analysis of the residual risk after the implementation of the proposed measures, and a recommendation on whether the measures will be sufficient in reducing risk to an acceptable level.

17 Risk mitigating measures

This chapter describes the technical, organizational, and legal measures that institutions and Ans can take to mitigate the risks described above. For each risk, the current risk is described in the upper half of the table and the risk score from section C is shown. The lower half of the table describes the measures that Ans and the institutions can take and assigns a score to the residual risk. In addition, the actions proposed by Ans to implement the measures for each risk are listed in a separate table, together with a timeline for the actions.

17.1 Measures to be taken to mitigate privacy risks

The tables below show the data protection risks for data subjects, with the mitigating measures Ans and the educational institutions can make. The tables below each risk provide an overview of the commitments from Ans.

Loss of control – Incomplete description of processing activities in DPA						
Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.1	Incomplete description of processing activities in DPA	Loss of control	Reasonable possibility	Serious harm	High	
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
	Update the DPA. Ensure the DPA clearly and comprehensively lists all processing activities, types of personal data processed, purposes, retention periods, and sub-processors. Implement procedures to periodically verify	Update the DPA, so that it is up-to-date and clearly specifies all data processing operations carried out on behalf of the institution, including a comprehensive sub-processor list. Proactively inform the institution about any changes to processing activities and assist with	Remote possibility	Serious harm	Low	

	that the actual data processing aligns with what is documented in the DPA and update the agreement as needed.	updating the DPA promptly to reflect these changes.				

Mitigating measures Ans	Timeline
Update Schedule 1 with the correct information (with assistance from SURF)	Q1 2026
Replace Schedule 1 for the existing DPAs with updated versions containing the correct information.	Q1 2026
Update and use the new template for all future DPAs	Q1 2026

Loss of control – Role division						
Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.2	Unclear controller/processor roles Conflicting legal documentation	Loss of control Inability to exercise data subject rights	More likely than not	Serious harm	High	
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
	Together with Ans define and document a clear definition of roles, specifying which data processing operations are performed by Ans as processor and which are undertaken by Ans	Align the descriptions of personal data categories and processing purposes across the DPA, Privacy Policy and other legal documentation to eliminate overlap and clarify the distinction	Remote possibility	Serious harm	Low	

	as independent data controller. Provide clear communication to the data subjects (including where data subjects should direct requests related to their personal data).	between processor and controller roles. Clearly communicate when Ans processes personal data for its own purposes (including legal basis and contacts for exercising data subject rights). Conduct and document a compatibility assessment under Article 6(4) GDPR for any further processing.				

Mitigating measures Ans	Timeline
Update Schedule 1 with the correct information (with assistance from SURF).	Q1 2026
Replace Schedule 1 for the existing DPAs with updated versions containing the correct information.	Q1 2026
Update and use the new template for all future DPAs.	Q1 2026
Update Privacy Policy with the correct information (with assistance from SURF).	Q1 2026

Inability to exercise data subject rights – Right to object direct marketing						
Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.3	Ambiguity about the purpose and sender of emails.	Inability to exercise data subject rights	Reasonable possibility	Minimal impact	Low	

	Lack of clear information in Ans's Privacy Policy.					
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
	Clarify roles and responsibilities in the communication chain. Require Ans to comply with transparency obligations under the GDPR.	Update the privacy policy to explicitly mention the right to object under Article 21 GDPR. Update the privacy policy to inform the data subject what personal data is used for what purpose. Clearly label emails with their purpose (e.g. product update, marketing) and indicate who is the sender (controller), so recipients can make informed decisions and exercise their rights appropriately.	Remote possibility	Minimal impact	Low	

Mitigating measures Ans	Timeline
Update Privacy Policy with the correct information (with assistance from SURF).	Q1 2026

Addition to the emails (short description in the email itself rather than labelling the emails) to indicate the sender (controller).	Q1 2026

Lack of transparency – List of sub-processors is incomplete						
Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.4	The list of sub-processor omits certain sub-processors and fails to provide a complete account of personal data processed by those that are included in the list.	Loss of control due to lack of transparency	Reasonable possibility	Serious harm	High	
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
	Exercise the audit right to regularly audit which sub-processors are used. Ensure all sub-processors are included in the legal framework (including personal data processed by this sub-processor and the processing location).	Provide transparency on the applicable sub-processors and maintain a complete list and ensure that all personal data processed by the sub-processor is listed.	Remote possibility	Serious harm	Low	

Mitigating measures Ans	Timeline
Update Schedule 1 with the correct information (with assistance from SURF).	Q1 2026

Replace Schedule 1 for the existing DPAs with updated versions containing the correct information.	Q1 2026
Update and use the new template for all future DPAs.	Q1 2026

Loss of control – DPA with TransIP lacks clear and specific instructions						
Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.5	The annexes of the DPA with TransIP B.V. list all possible options (personal data etc.) and states that only the options relevant to the client’s specific situation apply.	Loss of control	More likely than not	Serious harm	High	
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
	Implement strong contractual controls and approval processes for (new) sub-processors.	Ensure the DPA and its annexes (e.g., types of personal data, processing purposes, categories of data subjects) are customized and accurately reflect what processing will occur. Or: Use another supplier for file storage.	Remote possibility	Serious harm	Low	

Mitigating measures Ans	Timeline
Migrate all files containing personal data from TransIP to Amazon S3.	Before the end of Q3 2026

Loss of control – Processing location SorryApp						
Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.6	Incomplete or incorrect information on processing locations.	Loss of control – potential unlawful international data transfer	Reasonable possibility	Serious harm	High	
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
	Exercise the audit right to regularly audit which sub-processors are used.	Clarify data processing location(s) and legal transfer mechanism with SorryApp, or alternatively replace processor SorryApp with a different party with a processing location in the EEA or a valid legal transfer mechanism. Or: Remove references to status website from the application, limiting exposure of student and staff to SorryApp.	Remote possibility	Serious harm	Low	

Mitigating measures Ans	Timeline

Address shortcomings in StatusPal DPA and annexes together with StatusPal.	Q1 2026
Migrate status website to StatusPal.	Q1 2026

Lack of transparency – User impersonation not visible in UI						
Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.7	Administrators can assume the identity of another user. Although impersonation events are logged, this information is not visible to either the impersonated users or administrators through the user interface.	Loss of control due to lack of transparency	More likely than not	Serious harm	High	
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
	Disallow the use of user impersonation by administrators, until proper logging is in place.	Make sure start and end of impersonation is logged, and logs are surfaced in user interface. Log the username of the impersonating user with any actions that used impersonation.	Remote possibility	Serious harm	Low	

Mitigating measures Ans	Timeline
Add start and end of user impersonation to the user logs.	Q1 2026

Log the username of the impersonating user with any actions that used impersonation.	Q1 2026
Surface impersonation logs in the user interface.	Q1 2026

Chilling effect – Email tracking notification emails						
Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.8	Staff members can see whether and when users have opened their email (without their knowledge)	Chilling effect	Reasonable possibility	Some impact	Medium	
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
		Disable open tracking of notification emails.	Remote possibility	Some impact	Low	

Mitigating measures Ans	Timeline
Disable open tracking of notification emails.	Q1 2026

Chilling effect employees - Insights reviewer alignment						
Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.9	Reviewer alignment shows for each question a breakdown per reviewing staff member, showing the number of results reviewed, the time spent reviewing, and	Chilling effect employees	Reasonable possibility	Serious harm	High	

	the average number of points given.					
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
	Ensure that there is a legal basis for the insights reviewer alignment. Obtain approval from the Works Council before implementing any form of employee monitoring.	Disable the time spent reviewing insights.	Remote possibility	Serious harm	Low	

Mitigating measures Ans	Timeline
Disable the time spent reviewing insights.	Completed in new grading experience, fully removed from the product in Q1 2026

Loss of control due to lack of transparency - Feedback students						
Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.10	UI of the feedback form and the ability to click through the student file when a student provides feedback after finishing an exam.	Loss of control due to lack of transparency	Reasonable possibility	Some impact	Medium	
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
		Either give students the option to submit feedback anonymously, and/or	Remote possibility	Some impact	Low	

		the interface should clearly state that the comment and the student's name (and other details) will be visible to the instructors.				

Mitigating measures Ans	Timeline
Ans will adjust the interface to clearly state that both the comment and the student's name are visible to instructors.	Before the end of Q2 2026

Lack of transparency – Incomplete cookie information						
Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.11	Incomplete list of used cookies and technologies, and their retention periods	Loss of control due to lack of transparency	More likely than not (certain)	Serious harm	High	
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
	Regularly audit the web traffic for not listed cookies.	Comply with the legal transparency requirements about cookies and similar technologies. Update complete list of cookies.	Remote possibility	Serious harm	Low	

Mitigating measures Ans	Timeline
Comply with the legal transparency requirements about cookies and similar technologies.	Q1 2026

Update complete list of cookies.	Q1 2026

Lack of data minimisation – Application logging						
Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.12	Application logs include content data (exam answers, notes, discussion) and timing information (e.g. how long it took to answer or grade a question)	Lack of data minimisation	More likely than not	Serious harm	High	
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
	Re-assess application logging, access and retention periods, together with Ans (in a joint exercise through SURF).	Re-assess application logging, access and retention periods, together with SURF and institutions.	Remote possibility	Serious harm	Low	

Mitigating measures Ans	Timeline
Re-assess application logging and retention periods, together with SURF and institutions.	Q2 2026

Loss of confidentiality – One-time passwords						
Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.13	One-time password grants full access to the student's account (not just the relevant test) and undermines the	Loss of confidentiality	Reasonable possibility	Serious harm	High	

	integrity of access controls					
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
	Develop and enforce clear internal guidelines on when and how one-time passwords can be generated and used, including who is authorised to issue them, for what purposes, and how their use is documented and monitored.	Ensure that one-time passwords are restricted in scope and grant access only to the specific part of the platform necessary for their intended purpose (e.g., accessing a particular exam), and not to broader student data or full student records.	Remote possibility	Serious harm	Low	

Mitigating measures Ans	Timeline
Ensure that one-time passwords are restricted in scope and grant access only to the specific part of the platform necessary for their intended purpose.	Before the end of Q2 2026

Loss of control – Personal data processed longer than needed						
Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.14	Set up deletion – soft- and hard deletion. Functionality to define retention periods is not standard (add-on)	Loss of control due to not adhering to the principle of storage limitation	Reasonable possibility	Serious harm	High	
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk

	Clearly specify retention periods for different categories of personal data and ensure that staff are instructed to initiate permanent deletion within these timelines, particularly for student accounts and results, or automate deletion using API access.	Allow permanent deletion of all entities, including users. Allow users to permanently delete entities within 180-days soft-deletion period. Simplify the deletion model (clear split between soft-deletion (trash) and hard-deletion).	Remote possibility	Serious harm	Low	

Mitigating measures Ans	Timeline
Allow permanent deletion of all entities, including users.	Before the end of Q2 2026
Allow users to permanently delete entities within 180-days soft-deletion period.	Before the end of Q2 2026
Simplify the deletion model (clear split between soft-deletion (trash) and hard-deletion).	Before the end of Q2 2026

Loss of control – Integrated Google Services						
Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.15	Personal data sharing with third party	Loss of control – not meeting the subsidiarity principle	Reasonable possibility	Some impact	Medium	
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
	Do not implement YouTube videos in the exams.	Replace Google Charts by a different solution, preferably hosted as part of the application.	Remote possibility	Some impact	Low	

Mitigating measures Ans	Timeline
Replace Google Charts by a different solution.	Before the end of Q3 2026

Inability to exercise data subject rights – Administrators not fully able to honour DSARs

Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.16	Personal data not easy to distract from the system. Not all data returned by Ans (data inaccessible for the administrator)	Inability to exercise data subject rights	Reasonable possibility	Serious harm	High	
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
	Create a procedure to handle a data subject requesting its personal data from Ans to ensure all personal data is included in the response.	Create a support page describing how controllers can fulfil a DSAR, assisting controllers through the support channel where necessary. Add additional buttons in the product to more easily export data of users.	Remote possibility	Serious harm	Low	

Mitigating measures Ans	Timeline
Create a support page describing how controllers can fulfil a DSAR.	Before the end of Q3 2026
Add additional buttons in the product to more easily export data of users.	Before the end of Q3 2026

Lack of adequate procedures for reporting security incidents

Reference	Origin	Risk category	Probability	Impact	Risk score	Current risk
16.1.17	Inadequate procedures for identifying and reporting security incidents	Loss of confidentiality	Reasonable possibility	Serious harm	High	
	Measures institution	Measures supplier	Probability	Impact	Risk score	Residual risk
	Ensure that the DPA with Ans includes explicit obligations regarding breach notifications (in line with Article 28 and 33 GDPR). Periodically audit or request evidence from Ans demonstrating compliance with these requirements to verify they have appropriate measures in place. Subscribe applicable staff to security advisories from Ans.	Create security advisories section in Ans' support portal. Establish and document a clear internal procedure for identifying, assessing, and reporting security vulnerabilities (including criteria for escalation, timelines). Train staff on this protocol.	Remote possibility	Serious harm	Low	

Mitigating measures Ans	Timeline
Create security advisories section in support portal.	Q1 2026
Establish and document internal procedures on security advisories and train staff.	Q1 2026

17.2 Assessment of the risks after taking mitigating measures

After implementing the suggested mitigating measures, the risks are:

Table 14: Residual risks after mitigation

Severity of impact	Serious harm	**Low risk** **1, 2, 4, 5, 6, 7, 9, 11, 12, 13, 14, 16, 17**	**High risk**	**High risk**
	Some impact	**Low risk** **8, 10, 15**	**Medium risk**	**High risk**
	Minimal impact	**Low risk** **3**	**Low risk**	**Low risk**
		Remote possibility	Reasonable possibility	More likely than not
	Likelihood of harm			

For Risk 15 (medium risk) Ans committed to transfer the graphs visible to students by the end of Q3 2026. This will resolve the risk for students, not for the teachers.

Conclusion

The DPIA identified 13 high risks, 3 medium risks and 1 low risk for data subjects. The risks arise from contractual factors, the product's functionalities, and the use of subprocessors. If the proposed measures are implemented, all high risks will be reduced to low residual risks. In that case, no prior consultation with the Data Protection Authority is required. Although reducing low risks is not strictly necessary, it is recommended because the measures are easy to implement and help better protect the rights and freedoms of data subjects.

Throughout the DPIA process, Ans has shown a clear commitment to addressing all identified risks and has proactively begun implementing mitigating measures. As a result, many risks have already been resolved ahead of the DPIA's completion (See the textboxes in Part A). For the remaining risks, some measures require additional time. All are planned for implementation over the coming quarters.

Some risks relate to the contractual framework. Ans has committed to updating their templates (including Schedule 1) by the end of Q1 2026 (Ans will work closely with SURF on this). However, Ans expressed concerns about fully resolving these risks, noting that institutions are often reluctant (or slow due to lengthy internal processes) to accept changes and sign updated agreements. Although Ans is in the best position to identify which personal data is processed and for what purpose, it is ultimately the controller's responsibility to ensure that a data processing agreement meeting the requirements of Article 28 (3) GDPR is in place. Institutions should therefore pay close attention to this and proactively ensure that their agreements are updated and compliant. Ans will send out an updated agreement by the end of Q1 2026.

Other risks relate to features institutions themselves requested in their tenders. An example of this is the dashboard features that allow examinators to closely monitor each student's test progress in detail. It is important that institutions take privacy into account when drafting and issuing their tenders or make feature requests.

As a final note, institutions are recommended to use single sign-on (SSO) and enforce SSO, using a dedicated domain for the Ans application. Although this recommendation does not directly relate to an identified personal data risk, certain classes of risks can be avoided by enforcing single sign-on (e.g., one of the vulnerabilities in this DPIA was not applicable to institutions enforcing SSO).